Structure of lexicographic Gröbner bases in three variables of ideals of dimension zero

X. Dahan*

Dep* of Mathematics, Kyūshū university, Japan
dahan@math.kyushu-u.ac.jp

Abstract

We generalize the structural theorem of Lazard in 1985, from 2 variables to 3 variables. We use the Gianni-Kalkbrener result to do this, which implies some restrictions inside which lies the case of a radical ideal.

1 Introduction

Let \( I \) be a zero-dimensional ideal of a polynomial ring \( R[x, y, z] \) over a Noetherian domain \( R \). The lexicographic order \( \prec \) on \( \mathbb{C}^3 \), for which \( x \prec y \prec z \), is put on the monomials of \( k[x, y, z] \) ordered by \( \prec \). Given a polynomial \( p \in k[x, y, z] \), the leading monomial of \( p \), denoted \( \text{lm}(p) \), is the largest monomial for \( \prec \) occurring in \( p \). The coefficient in \( R \) in front of \( \text{lm}(p) \) is called the leading coefficient of \( p \), denoted \( \text{lc}(p) \). It might also be convenient to define the leading term of \( p \) denoted \( \text{lt}(p) \) equal to \( \text{lc}(p)\text{lm}(p) \).

The ideal of leading terms of \( I \) is the ideal of \( R[x, y, z] \) generated by the leading terms of elements of \( I \); it is equal to \( \langle \text{lt}(I) \rangle \). Since \( R \) is Noetherian, there is a finite set of generators of this ideal. A Gröbner basis of \( I \) is a finite set of elements in \( I, g_1, \ldots, g_s \) such that \( \langle \text{lt}(g_1), \ldots, \text{lt}(g_s) \rangle = \langle \text{lt}(I) \rangle \).

In our case, we will take \( R = k \) a field. Note that then \( \langle \text{lt}(I) \rangle \) is equal to \( \langle \text{lm}(I) \rangle \). This last ideal being a monomial ideal, it admits a minimal basis of monomials \( m_1, \ldots, m_s \); then a Gröbner basis \( g_1, \ldots, g_s \) is minimal if \( \text{lm}(g_i) = m_i \) for all \( i \). It is monic if \( \text{lc}(g_i) = 1 \) for all \( i \).

From now on, the monomial order will always be assumed to be \( \text{lex}(x, y, z) \) and the symbol \( \prec \) will be omitted in \( \text{lm}, \text{lc} \) and \( \text{lt} \).

Notation 1 Consider the rings \( R_1 := k[x] \) and \( R_2 := k[x] \). Given \( p \in k[x, y, z] = R_1[y, z] = R_2[z] \), let \( \text{lc}_1(p) \in R_1 \) be the leading coefficient of \( p \) for the lexicographic order \( \prec_{\text{lex}(y, z)} \) on \( R_1[y, z] \) and let \( \text{lc}_2(p) \in R_2 \) be the leading coefficient of \( p \) in \( R_2[z] \).

Furthermore, let \( \text{lm}_1(p) \) and \( \text{lm}_2(p) \) be the monomials such that \( \text{lt}(p) = \text{lc}_1(p)\text{lm}_1(p) = \text{lc}_2(p)\text{lm}_2(p) \).

Moreover, we make the following assumption:

Assumption: The ideal \( I \) will be supposed zero-dimensional, or, equivalently the \( k \)-algebra \( \mathbb{C}^3/I \) is supposed finite. We are given a minimal and monic Gröbner basis \( G := \{ g_1, \ldots, g_s \} \) of \( I \), indexed in a way that \( \text{lm}(g_1) \prec \text{lm}(g_2) \prec \cdots \prec \text{lm}(g_s) \).

We recall some basic facts about the Gröbner basis \( G \):

*Supported by the GCOE program “Math-for-Industry” of Kyūshū University
Theorem 1 (D. Lazard) Let \( J \subset k[x, y] \) be a zero-dimensional ideal, and \( f_1, \ldots, f_s \), a minimal lexicographic Gröbner basis of \( I \) for \( x \prec_{lex(x,y)} y \). Then:

\[
\text{lct}(f_i) \in k[x_1] \text{ divides } \text{lct}(f_j) \text{ for all } i \geq j, \text{ and } \text{lct}(f_i) \text{ divides } f_i \text{ as well.}
\]

It follows easily a factorization property of the polynomials in such a Gröbner basis [5, Theorem 1 (i)]. However, the formulation above is more compact and handy, and is equivalent. The main result of this paper is the following analogue in the case of 3 variables:

Theorem 2 Let \( I, \mathcal{G} := \{g_1, \ldots, g_s\} \) and \( \ell(2) \) be defined as above. Then, for all \( 1 \leq j \leq i \leq s \) such that the variable \( z \) appears in the monomials \( \text{lct}(g_i) \) and \( \text{lct}(g_j) \) with the same exponent, holds:

\[
\text{lct}(g_i) \text{ divides } \text{lct}(g_j), \text{ and if } I \text{ is radical: } \text{lct}(g_i) \text{ divides } g_i \text{ as well.}
\]

Furthermore, in the later case, for all \( i > \ell(2) \), \( g_i \in (\text{lct}(g_i), g_1) \).

The proof will occupy the next section. There is one corollary to this theorem in the context of “stability of Gröbner bases under specialization”, which generalizes the theorem of Gianni-Kalkbrener [2, 3], and improves the theorem of Becker [1] (but holds only with 3 variables).

Corollary 1 Let us assume \( I \) radical. Let \( \alpha \) be a root of \( g_1 \), \( \phi : \overline{k}[x,y,z] \to \overline{k}[y,z], x \mapsto \alpha \), and \( g \neq g_1 \) a polynomial among the Gröbner basis. Then, either \( \phi(g) = g(\alpha,x,z) = 0 \), or \( \phi(\text{lct}(g)) \neq 0 \). This implies that: \( \text{lt}(\phi(g)) = \phi(\text{lt}(g)) \), and in particular, that \( \phi(\mathcal{G}) \) is a Gröbner basis.

Proof: By Theorem 2, we can write \( g = \text{lct}(g)A \) with \( A = \frac{g}{\text{lct}(g)} \in k[x,y,z] \). Hence, if \( \phi(\text{lct}(g)) = 0 \), then \( \phi(g) = 0 \). Else, since \( \text{lt}(A) = y^*z^* \), we get \( \phi(\text{lt}(A)) = \phi(\text{lt}(A)) \). But \( \phi(g) = \text{lct}(g)\phi(A) \), from which follows \( \phi(\text{lt}(g)) = \phi(\text{lct}(g))\phi(\text{lt}(A)) \). On the other hand, \( \phi(g) = \phi(\text{lct}(g))\phi(A) = \phi(\text{lct}(g))\phi(\text{lt}(A)) \).

Gianni-Kalkbrener’s result [2, 3] concerns the easier case where all the variables but the largest one for \( \prec \) are specialized.

Gianni-Kalkbrener. The map \( \phi \) is therein \( \phi : \overline{k}[x,y,z] \to \overline{k}[z], x,y \mapsto \alpha,\beta \) for \( (\alpha, \beta) \) a solution of the system \( g_1, \ldots, g_{\ell(2)} \subset k[x,y] \). For any \( g \) in the Gröbner basis \( \mathcal{G} \) such that \( g \in k[x,y,z] \setminus k[x,y] \), they show that either \( \phi(g) = 0 \) or \( \deg_z(\phi(\text{lt}(g))) = \deg_z(\phi(\text{lt}(g))) \), which implies \( \phi(\text{lt}(g)) = \phi(\text{lt}(g)) \).

Becker [1] has generalized partly this result to the case of a map \( \phi \) that specializes the \( t \) lowest variables for \( \prec \). Taking \( t = 1 \), this covers the case of Corollary 1, but is weaker: it does also say that \( \phi(\mathcal{G}) \) remains a Gröbner basis, while assuming that for \( g \in \mathcal{G} \), \( \phi(\text{lt}(g)) \) may be a term with a monomial strictly smaller for \( \prec \) than the monomial in the term \( \text{lt}(\phi(g)) \) (see the definition of the integer \( r' \) during the proof of Prop. 1 page 4 of [1]. With the notations on the same page of [1] we see \( r' < r \); Corollary 1 above implies \( r = r' \). It can not be said that: \( \phi(\text{lt}(\mathcal{G})) = \text{lt}(\phi(\mathcal{G})) \).

Concerning previous works, let us mention that Kalkbrener [4] has expanded Becker’s result to the more general elimination monomial orders. Still, staying in the purely lexicographic case, it does not enhance the theorem of Becker.
2 Proof of Theorem 2

The main ingredient of the proof consists in generalizing two lemmas of Lazard. These refers to Lemma 2, and Lemma 3 of [5]. We shall explain that a weaker form holds with a larger number of variables. The version of interest here concerns the case of 3 variables. It is nonetheless easy to produce a version with an arbitrary number of variables. Let us first introduce some notations for exponents:

**Notation 2** Let \( f \in k[x, y, z] \) non zero, with leading monomial \( \text{lm}(f) = x^\alpha y^\beta z^\gamma \). The 3 notations \( \alpha_x(f), \alpha_y(f) \) and \( \alpha_z(f) \) will denote \( a, b \) and \( c \) respectively.

If \( g_i \) is among the Gröbner basis \( \mathcal{G} = \{g_1, \ldots, g_s\} \), the shortcuts \( \alpha_x(i), \alpha_y(i), \alpha_z(i) \) will be used instead of \( \alpha_x(g_i), \alpha_y(g_i), \alpha_z(g_i) \)

**Proposition 1** Let \( 1 \leq j < i \leq s \) be such that \( \alpha_y(j) \leq \alpha_y(i) \) and \( \alpha_z(j) \leq \alpha_z(i) \). Then \( \text{lc}_1(g_i) \) divides \( \text{lc}_1(g_j) \).

**Proof:** Let \( a := g_j y^{\alpha_y(i)-\alpha_y(j)} z^{\alpha_z(i)-\alpha_z(j)} \). The multivariate division algorithm with respect to \( \prec \) of \( a \) by \( [g_i] \) gives:

\[
\frac{a}{g_i} = qg_i + r, \quad \text{with } q \neq 0 \Rightarrow \text{lm}(a) \nmid \text{lm}(qg_i),
\]

and \( \text{lm}(g_i) \) does not divide any monomial occurring in \( r \).

By definition of \( a \), \( \text{lm}(g_i) \mid \text{lm}(a) \) so that \( q \neq 0 \), hence \( \text{lm}(qg_i) \nmid \text{lm}(a) \) holds:

\[
\text{lm}(qg_i) = \text{lm}(q) x^{\alpha_x(i)} y^{\alpha_y(i)} z^{\alpha_z(i)} \nmid x^{\alpha_x(j)} y^{\alpha_y(i)} z^{\alpha_z(i)} = \text{lm}(a) \quad \Rightarrow \text{lm}(q) x^{\alpha_x(i)} \nmid x^{\alpha_x(j)}.
\]

By an elementary property of the lexicographic order \( \prec_{\text{lex}(x,y,z)} \), this implies \( \text{lm}(q) \in k[x] \) and therefore \( q \in k[x] \). Next, the equality \( r = a - qg_i \) gives:

\[
\text{lm}(r) = \text{lm}(a - qg_i) \nmid \max\{\text{lm}(a); \text{lm}(qg_i)\} = x^{\max\{\alpha_x(qg_i), \alpha_y(a)\}} y^{\alpha_y(i)} z^{\alpha_z(i)}.
\]

Again, property of lexicographic order implies \( \alpha_z(r) \leq \alpha_z(i) \) and if \( \alpha_z(r) = \alpha_z(i) \) then \( \alpha_y(r) \leq \alpha_y(i) \). We distinguish three cases; in the first two ones the conclusion of the theorem holds, and the third case never happens.

**Case 1:** \( \alpha_z(r) < \alpha_z(i) \). Then \( \text{lc}_1(a) = q \text{lc}_1(g_i) \), and \( \text{lc}_1(a) = \text{lc}_1(g_j) \), this concludes the proof.

**Case 2:** Else \( \alpha_z(r) = \alpha_z(i) \), and \( \alpha_y(r) < \alpha_z(i) \). Similarly, this shows that \( \text{lc}_1(a) = q \text{lc}_1(g_i) \), concluding the proof.

**Case 3:** Else \( \alpha_z(r) = \alpha_z(i) \) and \( \alpha_y(r) = \alpha_y(i) \). Since \( \text{lm}(g_i) \nmid \text{lm}(r) \), necessarily \( \alpha_x(i) > \alpha_x(r) \). On the other hand, \( r \in (g_j, g_i) \subset I \) implies that there exists \( 1 \leq k \leq s \) such that \( \text{lm}(g_k) \mid \text{lm}(r) \). Therefore, \( \alpha_x(k) \leq \alpha_x(r) < \alpha_x(i) \), and in this case \( \alpha_y(k) \leq \alpha_y(r) = \alpha_y(i) \), \( \alpha_z(k) \leq \alpha_z(r) = \alpha_z(i) \). This means \( \text{lm}(g_k) \mid \text{lm}(g_i) \), and \( i \neq k \), which is impossible since the Gröbner basis is minimal. \( \square \)

**Proposition 2** For any \( i > 1 \), the polynomial \( g_i \) of the the Gröbner basis \( \mathcal{G} \) verifies: \( \text{lc}_1(g_i) \) divides \( \text{lc}_2(g_i) \).

**Proof:** Define,

\[
e_i := \max\{\alpha_y(\ell) \text{ s.t } \alpha_y(\ell) < \alpha_y(i), \alpha_z(\ell) \leq \alpha_z(i)\} \quad \text{and} \quad j := \max\{\ell < i \text{ s.t } \alpha_y(\ell) = e_i\}
\]
Note that $e_i$ is well-defined because $i > 1$ and $\alpha_y(1) = \alpha_y(g_1) = 0$. This also shows that $j$ is well-defined. By Proposition 1, $lc_1(g_i)$ divides $lc_1(g_j)$. Let

$$a := \frac{lc_1(g_j)}{lc_1(g_i)}, \quad \text{and} \quad b := a - g_jy^{\alpha_y(i)-\alpha_y(j)}z^{\alpha_z(i)-\alpha_z(j)}.$$  

By construction, $lm(b) < y^{\alpha_y(i)}z^{\alpha_z(i)}$. Furthermore, $b \in \langle g_i, g_j \rangle \subset I$ so its normal form modulo the Gröbner basis of $I$ is 0. The multivariate division equality with respect to $\prec$ of $b$ by $[g_1, \ldots, g_\ell]$ is written: $b = \sum_{1 \leq \ell \leq s} b_\ell g_\ell$. If $b_\ell \neq 0$, then $lm(b_\ell g_\ell) \prec lm(b) < y^{\alpha_y(i)}z^{\alpha_z(i)}$. The inequality $lm(b_\ell) \prec y^{\alpha_y(i)}z^{\alpha_z(i)}$ follows, which is possible only if $\ell \leq i - 1$. Otherly said, $b = \sum_{1 \leq \ell \leq i - 1} b_\ell g_\ell$.

It follows that $a = \sum_{\ell \neq j} b_\ell g_\ell + g_j(b_j + y^{\alpha_y(i)-\alpha_y(j)}z^{\alpha_z(i)-\alpha_z(j)})$, and that:

$$lc_2(a) = \sum_{\alpha_z(b_jb_j') = \alpha_z(i)} lc_2(b_\ell)lc_1(g_\ell) + lc_2(g_j)(clc_2(b_j) + 1),$$

with $\epsilon = 1$ if $\alpha_z(j) + \alpha_z(b_j) = \alpha_z(i)$ and $\epsilon = 0$ if $\alpha_z(j) + \alpha_z(b_j) < \alpha_z(i)$. However $lm(b_\ell g_\ell) \prec y^{\alpha_y(i)}z^{\alpha_z(i)}$ and $\alpha_z(b_\ell g_\ell) = \alpha_z(i)$ imply that $\alpha_y(b_\ell) + \alpha_y(\ell) < \alpha_y(i)$. In particular $\alpha_y(\ell) < \alpha_y(i)$ and consequently $\alpha_y(\ell) \leq e_i$. By definition of $j$, this gives: $\ell \leq j$. Proposition 1 then yields: $lc_1(g_j) \mid lc_1(g_\ell)$.

To conclude, note that Lazard’s Lemma 4 in [5] proves that Prop. 2 is true for $1 \leq i \leq \ell(2)$. So we can proceed by induction on $i$ and assume that $lc_1(g_\ell) \mid lc_2(g_\ell)$ for $2 \leq \ell < i$. Applied in Equation (1):

$$lc_2(a) = \sum_{\alpha_z(b_jb_j') = \alpha_z(i)} lc_2(b_\ell)lc_1(g_\ell)lc_1(g_j) + \frac{lc_2(g_j)}{lc_1(g_j)}lc_1(g_j)(clc_2(b_j) + 1) \in k[x,y]$$

Finally, $\frac{lc_2(a)}{lc_2(g_j)} = \frac{lc_2(g_j)}{lc_1(g_j)} \in k[x,y]$. \(\square\)

This proves the first part of Theorem 2. The second part is based upon the previous proposition and the theorem of Gianni-Kalkbrener. The use of the later requires a restriction:

**Proposition 3** Suppose there is an $1 \leq i < s$ such that: $lc_1(g_i) \neq 1$, there is a root $\alpha$ of $lc_1(g_i)$ which is not a root of $lc_1(g_{i+1})$. Then, $g(\alpha, y, z) = 0$ and $g_{i+1} \in \langle x - \alpha, lc_1(g_{i+1}) \rangle$.

**Proof:** Since $lc_1(g_i)(\alpha) = 0$, by Proposition 2, $lc_2(g_i)(\alpha, y) = 0$ as well. By Gianni-Kalkbrener, this implies $g_1(\alpha, y, z) = 0$. Furthermore, $lc_1(g_{i+1})(\alpha) \neq 0$, implying $p_\alpha(y) := lc_2(g_{i+1})(\alpha, y) \in \overline{k}[y]$ is not zero. Let $\beta \in \overline{k}$ be a root of this polynomial. By Gianni-Kalkbrener, $g_{i+1}(\alpha, \beta, z) = 0$, showing that $g_{i+1} \in \langle x - \alpha, p_\alpha \rangle$. \(\square\)

Note that if $I$ is radical, all elements $g_i$ for which $lc_1(g_i) \neq 1$ verify the assumption on the root $\alpha$ of Proposition 3. By an elementary use of the Chinese remaindering theorem, we get the more general, $g_{i+1} \in \langle g_1, lc_2(g_{i+1}) \rangle$. This proves the last part of Theorem 2.

**Conclusion**

It is likely that Theorem 2 holds without the assumption I radical. This assumption was set to allow the use of Gianni-Kalkbrener’s result. A proof circumventing it must be found. Also, some experiments shown that the results presented here are certainly true in the case of more than 3 variables.
References

[1] T. Becker. Gröbner bases versus $D$-Gröbner bases, and Gröbner bases under specialization. Applicable Algebra in Engineering, Communications and Computing, 5:1–8, 1994.

[2] P. Gianni. Properties of Gröbner bases under specialization. In J.H. Davenport, editor, In Proc. of EUROCAL’87, Lecture Notes in Computer Science (378), pages 293–297. Springer, Berlin, 1987.

[3] M. Kalkbrener. Solving systems of algebraic equations using Gröbner bases. In J.H. Davenport, editor, In Proc. of EUROCAL’87, Lecture Notes in Computer Science (378), pages 282–292. Springer, Berlin, 1987.

[4] M. Kalkbrener. On the stability of Gröbner bases under specialization. J. Symbolic Comput., 24(2):51–58, 1997.

[5] D. Lazard. Ideal bases and primary decomposition: case of two variables. J. Symbolic Comput., 1(3):261–270, 1985.