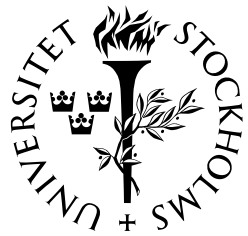
Computational algorithms for algebras

Samuel Lundqvist



Department of Mathematics
Stockholm University
2009

Doctoral Dissertation 2009
Mathematical Department
Stockholm University
SE-106 91 Stockholm

Typeset by LaTeX

ISBN 978-91-7155-974-6 pp. 1–9
Printed by US AB

Till Ilyan och Siri

Abstract

This thesis consists of six papers.

In Paper I, we give an algorithm for merging sorted lists of monomials and together with a projection technique, we obtain a new complexity bound for the Buchberger-Möller algorithm and the FGLM algorithm.

In Paper II, we discuss four different constructions of vector space bases associated to vanishing ideals of points. We show how to compute normal forms with respect to these bases and give complexity bounds. As an application we drastically improve the computational algebra approach to the reverse engineering of gene regulatory networks.

In Paper III, we introduce the concept of multiplication matrices for ideals of projective dimension zero. We discuss various applications and, in particular, we give a new algorithm to compute the variety of an ideal of projective dimension zero.

In Paper IV, we consider a subset of projective space over a finite field and give a geometric description of the minimal degree of a non-vanishing form with respect to this subset. We also give bounds on the minimal degree in terms of the cardinality of the subset.

In Paper V, we study an associative version of an algorithm constructed to compute the Hilbert series for graded Lie algebras. In the commutative case we use Gotzmann's persistence theorem to show that the algorithm terminates in finite time.

In Paper VI, we connect the commutative version of the algorithm in Paper V with the Buchberger algorithm.

Många tack

Först och främst, ett stort tack till min utmärkta handledare Clas Löfwall. Han har gett mig bra problem att arbeta med och har visat ett stort intresse och engagemang för min forskning. Jag ser fram mot ett fördjupat samarbete i framtiden.

Även min biträdande handledare Ralf Fröberg har varit utomordentlig. Jag vill framför allt tacka Ralf för att ha fört in mig på studiet av försvinnandeideal.

Tack till Veronica Crispin Quiñonez för all hjälp med att läsa korrektur och till Jörgen Backelin för många intressanta diskussioner relaterade till min avhandling.

Jag vill tacka mina kollegor för den goda stämning som råder på institutionen, och slutligen, ett varmt tack till alla mina vänner och till min familj för allt stöd.

Stockholm 20 november 2009
Samuel Lundqvist

Contents

List of papers

I S. Lundqvist, *Complexity of comparing monomials and two improvements of the Buchberger-Möller algorithm.* MMISC 2008, Lecture Notes in Comput. Sci. **5393** (2008), 105–125.

II S. Lundqvist, *Vector space bases associated to vanishing ideals of points.* J. Pure Appl. Alg. **214** (2010), no. 4, 309–321.

III S. Lundqvist, *Multiplication matrices and ideals of projective dimension zero.* Submitted (2009).

IV S. Lundqvist, *Non-vanishing forms in projective space over finite fields.* Submitted (2009).

V S. Lundqvist, *An algorithm to determine the Hilbert series for graded associative algebras.* Research Reports in Mathematics, Stockholm University (2005), no. 3, 1–19.

VI S. Lundqvist, *A Buchberger like algorithm without monomial orderings — the graded commutative case.* Manuscript (2009).

1 Introduction and summary of the papers

This thesis concerns computational algorithms for algebras. We present six papers on this subject.

Notation needed to summarize the papers

Let $\Bbbk$ be a field, and denote by $\Bbbk[x_1, \ldots, x_n]$ the polynomial ring in n variables over $\Bbbk$. A monomial in $\Bbbk[x_1, \ldots, x_n]$ is an element of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where each α_i is a non-negative integer. A polynomial in $\Bbbk[x_1, \ldots, x_n]$ is regarded as a $\Bbbk$-linear combination of monomials.

We evaluate a monomial at a point $p = (p_1, \ldots, p_n) \in \Bbbk^n$ by $x_1^{\alpha_1} \cdots x_n^{\alpha_n}(p) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. We extend this evaluation to polynomials by linearity. Suppose that f is a polynomial in $\Bbbk[x_1, \ldots, x_n]$. We say that f is vanishing on p if $f(p) = 0$. When P is a collection of points, we say that f is vanishing on P if $f(p) = 0$ for all $p \in P$.

Example 1.1. Consider $P = \{(1,0,0), (0,1,0), (1,1,1)\}$, a set of three points in $\mathbb{Q}^3$. Then $f = x_1x_2x_3 - x_3$ is vanishing on P.

When P is a collection of points, the vanishing ideal with respect to P consists of all polynomials that vanish on all of the points in P.

While performing computations in the polynomial ring, it is suitable to have an order defined on the set of monomials. A natural ordering is the Lexicographical ordering, denoted by $\prec_{lex}$. It is defined by $x_0^{\alpha_0} \cdots x_n^{\alpha_n} \prec_{lex} x_0^{\beta_0} \cdots x_n^{\beta_n}$ if $\alpha_0 = \beta_0, \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}$ and $\alpha_i < \beta_i$ for some i.

Example 1.2. Consider the monomials $1, x_0, x_2, x_2^2, x_1x_2, x_0x_2, x_0^2, x_1^3x_2$ in the ring $\Bbbk[x_0, x_1, x_2]$. The following holds:

$$1 \prec_{lex} x_2 \prec_{lex} x_2^2 \prec_{lex} x_1x_2 \prec_{lex} x_1^3x_2 \prec_{lex} x_0 \prec_{lex} x_0x_2 \prec_{lex} x_0^2.$$

The Lexicographical ordering is an example of a so-called admissible monomial ordering. An admissible monomial ordering $\prec$ on $\Bbbk[x_0, \ldots, x_n]$ is a total order on the monomials which respects multiplication and has the monomial 1 as the minimal element.

When f is a polynomial in $\Bbbk[x_0, \ldots, x_n]$ and $\prec$ is an admissible monomial ordering, we denote by $\text{in}_\prec(f)$ the greatest monomial occurring in f with respect to $\prec$. When I is an ideal in $\Bbbk[x_0, \ldots, x_n]$ and $\prec$ is an admissible monomial ordering, the initial ideal of I, denoted by $\text{in}_\prec(I)$, is the set of monomials m such that $m = \text{in}_\prec(f)$ for some $f \in I$.

A Gröbner basis for an ideal I with respect to an admissible monomial ordering $\prec$ is a finite set of elements $g_1, \ldots, g_r$ in $\Bbbk[x_0, \ldots, x_n]$ such that $(g_1, \ldots, g_r) = I$ and $(\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_r)) = \text{in}_\prec(I)$.

Example 1.3. Suppose that $x_1^2 + x_2$ and $x_1x_2 + x_3$ are elements in an ideal I, ordered by the Lexicographical ordering. Then x_1^2 and x_1x_2 are elements in $\text{in}(I)$. Since $x_1x_3 - x_2^2 = -x_2(x_1^2 + x_2) + x_1(x_1x_2 + x_3)$, it holds also that x_1x_3 belongs to $\text{in}(I)$.

Example 1.4. If $I = (m_1, \ldots, m_s)$ and all the m_i's are monomials, then $\text{in}(I) = (m_1, \ldots, m_s)$ independently of ordering. Hence $(m_1, \ldots, m_s)$ is a Gröbner basis for I, independently of ordering.

The computation of a Gröbner basis for an ideal I depends on how I is defined.

- If a set of generators for I is given, we can compute a Gröbner basis for I by means of the Buchberger algorithm. The algorithm forms pairs of certain elements in the ideal and computes the so-called S-polynomial of these elements. Each S-polynomial is *reduced* with elements from the ideal. Due to the Noetherian property of the polynomial ring, the algorithm terminates in finite time.

- If I is defined to be the set of polynomials which vanish on a finite set of points, then a Gröbner basis for I can be computed by means of the Buchberger-Möller algorithm. This algorithm is based on linear algebra and has polynomial complexity in the number of variables and the number of points.

Let I be an ideal in $\Bbbk[x_1, \ldots, x_n]$. Then we can form the quotient ring $\Bbbk[x_1, \ldots, x_n]/I$. We write elements in this ring as $[f]$, where $f \in \Bbbk[x_1, \ldots, x_n]$ and where the brackets indicate that we are working modulo I. An important property of the initial ideal $\text{in}_\prec(I)$ with respect to $\prec$ is that

$$\{[e], e \text{ is a monomial outside } \text{in}(I)\}$$

constitute a vector space basis for $\Bbbk[x_1, \ldots, x_n]/I$.

An ideal $I \subseteq \Bbbk[x_1, \ldots, x_n]$ is defined to be zero-dimensional if the quotient ring $\Bbbk[x_1, \ldots, x_n]/I$ is of finite dimension as a vector space over $\Bbbk$. The variety of a zero dimensional ideal is finite.

We conclude with the notation used in the graded setting. The degree of a monomial $m = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, denoted by $|m|$, is $\sum_i \alpha_i$. A polynomial f is said to be homogenous if all the monomials occurring in f have the same degree. When I is generated by homogenous elements, I becomes graded over the natural numbers. By convention, when working on graded ideals, we number the variables starting from zero instead of one. If $I \subseteq \Bbbk[x_0, \ldots, x_n]$ is graded, then the quotient ring $R = \Bbbk[x_0, \ldots, x_n]/I$ can be written as the direct sum $R_0 \oplus R_1 \oplus \cdots$. The Hilbert function of R is the map $\mathbb{N} \to \mathbb{N}, d \mapsto \dim_\Bbbk(R_d)$ and the Hilbert series of R is $\dim_\Bbbk(R_0) + \dim_\Bbbk(R_1)t + \dim_\Bbbk(R_2)t^2 + \cdots$.

1.1 Paper I

In 1982 Buchberger and Möller [1] gave an algorithm, based on linear algebra, to compute a Gröbner basis with respect to a vanishing ideal of points.

Inspired by the Buchberger-Möller algorithm, hereby referred to as the BM algorithm, the so called FGLM algorithm appeared in 1993 [4]. This algorithm transforms a Gröbner basis for a zero-dimensional ideal with respect to any given ordering into a Gröbner basis with respect to any other ordering. The same year another paper related to the subject appeared [9]. Using a higher abstraction level, it was shown that both the BM algorithm and the FGLM algorithm could be seen as algorithms to compute a Gröbner basis from an ideal defined by functionals.

The BM algorithm and the FGLM algorithm both have the same run time complexity. The number of arithmetic operations was reported in [4] and [9] to be proportional to nm^3, where n is the number of variables and m is the number of points. The BM/FGLM algorithm also performs integer comparisons. The integer comparisons were reported to be proportional to n^2m^2.

The BM algorithm appears now in many applications in pure and applied mathematics: statistics, coding theory, interpolation, and computational biology. The FGLM algorithm is the most common tool to solve systems of equations, the defining ideal of which is zero-dimensional.

The application of the BM algorithm in computational biology is the reverse engineering of gene regulatory networks, see [7]. In this application the number of points m is small compared to n — the number of variables. This fact lead to a search of optimized versions of the BM algorithm for the situation $m \ll n$, for instance, see [5] and [6].

In the first paper we show that the optimized versions of the BM algorithm actually performs worse than the original method. Indeed, we show that an upper bound for the arithmetic complexity of the BM/FGLM algorithm is proportional to $\min(m, n)m^3 + nm^2$ instead of the previously reported nm^3.

The paper concerns also the integer comparisons during the BM/FGLM algorithm. The integer comparisons come from merging sorted lists of monomials.

Example 1.5. The lists (x_1x_2, x_3x_4, x_5^2) and (x_2x_3, x_3, x_5^2) are sorted in decreasing order with respect to the Lexicographical ordering. Merging the two lists, we obtain $(x_1x_2, x_2x_3, x_3x_4, x_3, x_5^2, x_5^2)$.

Merging lists of monomials is essentially the same as addition of polynomials. Since addition of polynomials is the most common operation in computer algebra, it is clear that efficient ways to do it is of importance when it comes to performance.

We give a new algorithm for merging sorted lists of monomials and applied to the BM/FGLM algorithm for standard orderings we show that the number of integer comparisons, where the integers are bounded by n, is at most proportional to nm^2.

1.2 Paper II

The second paper is much related to the first one. The aim of it is to argue for that it is vector space bases over the quotient ring $\Bbbk[x_1, \ldots, x_n]/I(P)$, rather than Gröbner bases for $I(P)$, which should be worked with in order to perform computations, such as determining normal forms, over vanishing ideals of points. We show that in the biological applications described in [7], the usage of vector space bases instead of Gröbner bases makes the runtime of the computations decrease from exponential to polynomial.

It holds that the vector space $\Bbbk[x_1, \ldots, x_n]/I(P)$ is of dimension $m = |P|$, and that $\{[e_1], \ldots, [e_m]\}$ is a basis exactly when the matrix (c_{ij}), where $c_{ij} = e_i(p_j)$, has full rank*.

There are several ways to construct a basis. We give four efficient constructions related to the following three bases.

- The basis is the monomial complement of the initial ideal with respect to some monomial ordering.
- The basis separates the points, that is, $e_i(p_i) = 1$ and $e_i(p_j) = 0$ if $i \neq j$.
- The basis is "univariate", that is, $e_i = f^i$, where f is a polynomial of degree one. The polynomial f satisfies $f(p_i) \neq f(p_j)$ whenever $i \neq j$.

Example 1.6. Let $P = \{(1,0,0), (1,1,0), (1,1,1)\}$ in $\mathbb{Q}^3$, so that $I(P) \subset \mathbb{Q}[x_1, x_2, x_3]$.

- A Gröbner basis for $I(P)$ with respect to the Lexicographical ordering with $x_1 \succ x_2 \succ x_3$ is $\{x_1 - 1, x_2^2 - x_2, x_2x_3 - x_3, x_3^2 - x_3\}$. Thus, the initial ideal is equal to $(x_1, x_2^2, x_2x_3, x_3^2)$ and the set of monomials outside the initial ideal is $\{1, x_3, x_2\}$. This means that $\{[1], [x_3], [x_2]\}$ is a $\Bbbk$-basis for $\Bbbk[x_1, \ldots, x_n]/I(P)$.
- An example of a separator basis with respect to P is $\{[x_1(1 - x_2)], [x_2 - x_3], [x_3]\}$.
- An example of a "univariate" basis is $\{[1], [x_1 + x_2 + x_3], [(x_1 + x_2 + x_3)^2]\}$.

1.3 Paper III

Algorithms to compute the variety of a zero-dimensional ideal by means of eigenvalues have been studied in various papers, for instance, see [2] and [10]. An interesting aspect of this approach is that it benefits from using both numerical and symbolic algorithms.

The eigenvalue approach is as follows. If a basis $\{[e_1], \ldots, [e_m]\}$ has been chosen for the quotient ring $\Bbbk[x_1, \ldots, x_n]/I$, then $[x_i][e_j]$ can be expressed as a

*The full rank condition is independent of the representative for each equivalence class.

linear combination of the basis elements for each i and each j. Thus, $[x_i][e_j] = \sum_k c_k^{(i,j)}[e_k]$. The matrix $M_i = (m_{jk}^{(i)})$, where $m_{jk}^{(i)} = c_k^{(i,j)}$, is called the multiplication matrix of x_i with respect to $\{[e_1], \ldots, [e_m]\}$. There is a nice one-to-one correspondence of points in the variety of I and common eigenvectors the multiplication matrices $M_1, \ldots, M_n$ and this correspondence can be used to compute the variety of I from the multiplication matrices.

The aim of the third paper is to generalize this correspondence to quotient rings $R = \Bbbk[x_0, \ldots, x_n]/I$, where I is of projective dimension zero, i.e. graded one-dimensional. Such rings are characterized by the Hilbert function — eventually it attends a constant value $m > 0$. The variety of an ideal of projective dimension zero consists of a finite number of projective points.

When $\Bbbk$ is infinite or contains enough elements, we show that there is a linear form l and an integer r such that the map from R_d to R_{d+1} induced by multiplication by l is surjective for all $d \geq r$. When $\Bbbk$ contains too few elements, it is possible to make a field extension of $\Bbbk$ which guarantees the existence of such a linear form.

For d large enough, this implies that if $\{[e_1], \ldots, [e_m]\}$ is a $\Bbbk$-basis for R_d, then $\{[le_1], \ldots, [le_m]\}$ is a $\Bbbk$-basis for R_{d+1}. This choice of basis is the key to the connection to the eigenvalue method in the zero-dimensional case.

Example 1.7. Let $I = (x_0^2, x_1^2)$. A $\mathbb{Q}$-basis in degree greater than or equal to two for the ring

$$R = \mathbb{Q}[x_0, x_1, x_2]/(x_0^2, x_1^2)$$

is given by

$$\{[x_0 x_2^{d-1}], [x_0 x_1 x_2^{d-2}], [x_1 x_2^{d-1}], [x_2^d]\},$$

so that $\dim_{\mathbb{Q}}(R_d) = 4$ for $d \geq 2$. We have $\dim_{\mathbb{Q}}([x_2]R_d) = \dim_{\mathbb{Q}}(R_{d+1})$ for $d \geq 2$, hence multiplication with $[x_2]$ is surjective for all $d \geq 2$.

As a side effect of our study of ideals of projective dimension zero, we obtain an upper bound of the degree of an element in a reduced Gröbner basis of *any* graded ideal.

1.4 Paper IV

Given a set of points in projective space over a finite field $\Bbbk$, we can pose the following question: Which is the least degree of a non-vanishing form (non-zero on all of the points) with respect to this set of points?

Example 1.8. Consider $\{(1:0:0:0), (0:1:0:0), (0:0:1:0), (0:0:0:1), (1:1:1:0), (1:1:1:1)\} \subseteq \mathbb{P}^3(\mathbb{F}_2)$, where $\mathbb{F}_2$ denotes the field with two elements. The quadratic form

$$(x_0 + x_2 + x_3)^2 + x_1(x_0 + x_2 + x_3) + x_1^2$$

is non-vanishing with respect to the points. Does there exist a linear non-vanishing form? The answer is no and this can be shown by examining all linear forms in $\mathbb{F}_2[x_0, x_1, x_2, x_3]$.

The existence of a linear non-vanishing form is related to the linear form l in Paper III.

In the fourth paper we show that the least degree of a non-vanishing form with respect to a point set is equal to $d+1$, where d is the highest degree such that there is a linear embedding of projective space of degree d into the point set. While it seems hard to check whether there exists a linear embedding or not, it is possible to give a fast algorithm which returns a non-vanishing form, but not necessarily with the lowest possible degree.

1.5 Paper V

In the fifth paper, we give an algorithm to compute the Hilbert function for graded associative algebras. This is the only part of the thesis where we consider non-commutative algebras. By a graded non-commutative algebra we mean the quotient of the free associative algebra in the variables $x_1, \ldots, x_n$, denoted by $\Bbbk\langle x_1, \ldots, x_n\rangle$, with a two-sided ideal generated by homogeneous elements. The algorithm we present does in some sense force algebra axioms on a graded module, turning the latter into an isomorphic copy of a part of $\Bbbk\langle x_1, \ldots, x_n\rangle/I$. Using the presentation

$$\Bbbk\langle X_1, \ldots, X_n\rangle/(\{X_iX_j - X_jX_i\}_{i,j}) \cong \Bbbk[x_1, \ldots, x_n],$$

we can use the algorithm to compute the Hilbert series of graded commutative algebras as well. By using Gotzmann's persistence theorem, we show that in the commutative case, the algorithm computes the Hilbert series in finite time.

The interesting aspect with this approach is that it does not rely on Gröbner bases theory or monomial orders, and that $\Bbbk$-bases can be computed which are not residues of monomials outside the initial ideal.

The ideas of the algorithm came from a paper by Löfwall and Roos [8], where an algorithm to compute the Hilbert series of a graded Lie Algebras was given.

Without going into details, we will illustrate the commutative version of the algorithm with an example.

Example 1.9. Let $I = (x_0^2, x_0x_1 - x_1^2) \subseteq \mathbb{Q}[x_0, x_1]$ and let $R = \mathbb{Q}[x_0, x_1]/I$. We choose [1] as a vector space basis for R_0 and $\{[x_0], [x_1]\}$ as a vector space basis for R_1. We let $V_2 = \text{span}_{\mathbb{Q}}\{x_0 \otimes [x_0], x_1 \otimes [x_0], x_0 \otimes [x_1], x_1 \otimes [x_1]\}$. In the graded $\mathbb{Q}\langle X_0, X_1\rangle$-module $R_0 \oplus R_1 \oplus V_2$ we perform the following computations:

$$X_0^2.1 = x_0 \otimes x_0, (X_0X_1 - X_1^2).1 = x_0 \otimes [x_1] - x_1 \otimes [x_1] \tag{1}$$

and

$$(X_0X_1 - X_1X_0).1 = x_0 \otimes [x_1] - x_1 \otimes [x_0]. \tag{2}$$

Let C_2 be the $\mathbb{Q}$-space spanned by these three expressions. Then $\dim_{\mathbb{Q}} V_2/C_2 = 1$ and we choose $[x_1 \otimes [x_0] + x_1 \otimes [x_1]]$ as a $\mathbb{Q}$-basis of V_2/R_2. Let $e = x_1x_0 + x_1^2$. It holds that $\{[x_1x_0 + x_1^2]\}$ is a $\mathbb{Q}$-basis of R_2. We have $[x_0][x_0] = 0$, $[x_0][x_1] = [e]/2$, and $[x_1][x_1] = [e]/2$.

The equations in (1) force $x_0^2 = 0$ and $x_0x_1 - x_1^2 = 0$ to hold, while (2) forces commutativity.

In degree three, let $V_3 = \text{span}_{\mathbb{Q}}\{x_0 \otimes [e], x_1 \otimes [e]\}$ and let

$$C_3 = \text{span}_{\mathbb{Q}}\{X_0X_1 - X_1X_0).[x_0], (X_0X_1 - X_1X_0).[x_1]\}$$

$$= \text{span}_{\mathbb{Q}}\{x_0 \otimes [e]/2, x_0 \otimes [e]/2 - x_1 \otimes [e]/2\}.$$

Thus $C_3 = V_3$, which implies that $\dim_{\mathbb{Q}}(R_3) = 0$, so the Hilbert series of R is equal to $1 + 2t + t^2$.

The algorithm has been implemented in C, and in the non-commutative case, part of some conjectures by D. Anick and A. Kirillov has been verified.

1.6 Paper VI

The last paper can be seen as a comment on Paper V. It turns out that the axioms we are forcing in the commutative case have an interesting connection to Gröbner bases theory. We show that, during a Gröbner basis computation, each S-polynomial can be replaced by a commutator expression in a graded $\Bbbk\langle X_1, \ldots, X_n\rangle$-module. We also show that the commutator expressions can be used to perform reduction of elements with respect to a Gröbner basis. This gives a homogeneous way to perform the Buchberger algorithm. The reduction of elements in terms of the commutator expressions has much in common with the F4-algorithm [3], which is known to be the fastest existing Gröbner basis algorithm. So, in some sense, the method in Paper V can be seen as a generalization of the Buchberger algorithm, since we can perform it without a monomial ordering. But if we do use a monomial ordering, we are essentially performing the Buchberger algorithm.

The connection to the Buchberger algorithm seems possible to formulate also for non-commutative graded algebras. Indeed, the outline for the graded non-commutative case is already done. Also, the non-graded cases seem possible to attack. Moreover, we have reason to believe that also the Lie Algebra algorithm [8], can be connected to Gröbner basis theory for Lie Algebras. All of this will be joint work with Clas Löfwall.

Another interesting aspect of our approach is that it might give some new insight on the criteria which tells when an S-polynomial does not need to be computed during the Buchberger algorithm. For instance, part of Buchberger's first criteria is implicit in our method.

We give an example of this method below, where, as in Example 1.9, details are omitted.

Example 1.10. We consider the same ideal as in Example 1.9 with respect to the Lexicographical ordering. We now work in the polynomial ring, rather than in the quotient ring, so we omit brackets. It holds that $1, x_0, x_1 \notin \text{in}(I)$. Consider a graded $\mathbb{Q}\langle X_0, X_1\rangle$-module

$$\text{span}_{\mathbb{Q}}\{1\} \oplus \text{span}_{\mathbb{Q}}\{x_0, x_1\} \oplus V_2',$$

where

$$V_2' = \text{span}_{\mathbb{Q}}\{x_0 \otimes x_0, x_0 \otimes x_1, x_1 \otimes x_1\}.$$

In this module, we have $X_0^2.1 = x_0 \otimes x_0$ and $(X_0X_1 - X_1^2).1 = x_0 \otimes x_1 - x_1 \otimes x_1$. Let

$$G_2 = \{X_0^2.1, (X_0X_1 - X_1^2).1\}$$

Notice that, contrary to Example 1.9, $x_1 \otimes x_0 \notin V_2'$ and $(X_0X_1 - X_1X_0).1 \notin G_2$.

It holds that $\text{mult}(G_2) = \{x_0^2, x_0x_1 - x_1^2\}$ is the set of Gröbner basis elements of I of degree two. Hence, the only monomial outside $\text{in}(I)$ of degree two is x_1^2.

In degree three, let

$$V_3' = \{x_0 \otimes x_1^2, x_1 \otimes x_1^2\}$$

and let

$$G_3 = \{(X_0X_1 - X_1X_0).x_0\} \subseteq V_3'.$$

The commutator $(X_0X_1 - X_1X_0).x_0$ corresponds to the S-polynomial $S(x_0^2, x_0x_1 - x_1^2) = x_1(x_0^2) - x_0(x_0x_1 - x_1^2) = x_0x_1^2$.

We have $(X_0X_1 - X_1X_0).x_0 = x_0 \otimes x_1^2$ and since $x_0x_1^2 \in \text{in}(G_2)$, we reduce $x_0 \otimes x_1^2$ by the *reductor* $(X_0X_1 - X_1X_0).x_1 = x_0 \otimes x_1^2 - x_1 \otimes x_1^2$ and get $x_1 \otimes x_1^2$. The element $\text{mult}(x_1 \otimes x_1^2) = x_1^3$ is the only Gröbner basis element of degree three. In the Gröbner basis sense, reducing $(X_0X_1 - X_1X_0).x_0$ by $(X_0X_1 - X_1X_0).x_1$ corresponds to reducing $S(x_0^2, x_0x_1 - x_1^2)$ by $x_0x_1 - x_1^2$ to x_1^3.

References

[1] B. Buchberger and M. Möller, *The construction of multivariate polynomials with preassigned zeroes.* Computer Algebra (Marseille, 1982), Lecture Notes in Comput. Sci., **144** (1982), 24–31.

[2] R.M. Corless, *Editor's Corner: Gröbner bases and Matrix Eigenproblems.* SIGSAM Bull. **30** (1996) no. 4, 26–32.

[3] J.C. Faugère, *A new efficient algorithm for computing Gröbner bases (F4).* J. Pure Appl. Algebra **139** (1999), no. 1, 61–88.

[4] J.C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering.* J. Symb. Comput. **16** (1993), no. 4, 329–344.

[5] W. Just and B. Stigler, *Computing Gröbner bases of ideals of few points in high dimensions.* Communications in Computer Algebra **40** (2006), no. 3, 65–96.

[6] W. Just and B. Stigler, *Efficiently computing Groebner bases of ideals of points.* (2007), arXiv:0711.3475.

[7] R. Laubenbacher, B. Stigler, *A computational algebra approach to the reverse-engineering of gene regulatory networks.* J. Theor. Biol. **229** (2004), 523–537.

[8] C. Löfwall and J.-E. Roos, *A nonnilpotent 1-2-presented graded Hopf algebra whose Hilbert series converges in the unit circle.* Adv. in Math. **130** (1997), no. 2, 161–200.

[9] M. G. Marinari, H.M. Möller, and T. Mora, *Gröbner bases of ideals defined by functionals with an application to ideals of projective points.* Appl. Algebra in Eng. Comm. Comput. **4** (1993), no. 2, 103–145.

[10] H.M. Möller and H. Stetter, *Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems.* Numer. Math. **70** (1995), no. 3, 311–329.