On Groebner Bases and Their Use in Solving Some Practical Problems

Matej Mencinger^{1,2}

¹University of Maribor, Faculty of Civil Engineering, Smetanova 17, 2000, Maribor, Slovenia ²Institute of Mathematics, Physics and Mechanics, Ljubljana, Jadranska 19, 1000, Ljubljana, Slovenia *Corresponding Author: matej.mencinger@um.si

Copyright © 2013 Horizon Research Publishing All rights reserved.

Abstract Groebner basis are an important theoretical building block of modern (polynomial) ring theory. The origin of Groebner basis theory goes back to solving some theoretical problems concerning the ideals in polynomial rings, as well as solving polynomial systems of equations. In this article four practical applications of Groebner basis theory are considered; we use Groebner basis to solve the systems of nonlinear polynomial equations, to solve an integer programming problem, to solve the problem of chromatic number of a graph, and finally we consider an original example from the theory of systems of ordinary (polynomial) differential equations. For computations we use systems »MATHEMATICA« and »SINGULAR«.

Keywords Polynomial system of (differential) equations, integer linear programming, chromatic number of a graph, polynomial rings, Groebner basis, CAS systems

1. Introduction

In his 1965 thesis, Bruno Buchberger[3] developed the theory of what we today call Groebner basis. The theory allows computations in multivariate polynomial rings analogous to those we use in single variable polynomial rings. The theory of Groebner basis can also be seen as a generalization of Gaussian elimination of a linear (polynomial) system, which yields the well-known row echelon form. However, applications of Groebner basis can be found in different fields of (mathematical) science. Roughly speaking, they can be used anywhere where some polynomial(s) (ideals) appear.

The basic idea here was to generalize a step in the classical Gaussian elimination algorithm, when for example the pair of polynomials (obtained from equations) f = 3x + 7y - 5z - 2 and g = 2x + 3y - 8z - 6 is replaced by an (equivalent) pair of polynomials (equations) f = 3x + 7y - 5z - 2 and $S_{f,g} = 5y + 14z + 14$. Recall that the least common multiple of 3 and 2 is 6 and that

$$S_{f,g} = \frac{6}{3}(3x + 7y - 5z - 2) - \frac{6}{2}(2x + 3y - 8z - 6)$$

= 5y + 14z + 14.

In the sequel we provide some definitions from the ring theory which help to understand the origin of Groebner basis (see e.g. [5] or [13] for details). To this end just recall, that the set of *polynomials* $f_1, f_2, ..., f_s$ implies a system of equations

$$f_1(x_1, x_2, \dots, x_n) = 0, f_2(x_1, x_2, \dots, x_n)$$

$$= 0, \dots, f_s(x_1, x_2, \dots, x_n) = 0$$
(1.1)

on one hand, and is naturally associated with the ideal

$$\langle f_1, f_2, \dots, f_s \rangle = \left\{ \sum_{j=1}^s h_j f_j : h_1, \dots, h_s \in k[x_1, x_2, \dots, x_n] \right\}$$

generated by polynomials $f_1, f_2, ..., f_s$ (which is also the *basis* of the ideal $I = \langle f_1, f_2, ..., f_s \rangle$).

The most common *monomial term ordering* is *lexicographic*; though many other are well-known, too (e.g. (graded) reverse lexicographic order, elimination order, etc.).

Recall that as soon as the monomial order is chosen we can speak of *leading monomial* (LM), *leading term*(LT) and *leading coefficient* (LC) of the polynomial.

Recall also, that any vector $\vec{c} \in \mathbb{R}^n$ defines a *weight* (monomial term) *ordering* $<_{\vec{c}}$ in $\mathbb{R}[x_1, x_2, ..., x_n]$ in the following way:

$$x^{\alpha} <_{\vec{c}} x^{\beta} \Leftrightarrow \begin{cases} \vec{c} \cdot \alpha < \vec{c} \cdot \beta & \text{or} \\ \vec{c} \cdot \alpha = \vec{c} \cdot \beta & \text{and } \alpha <_{lex} \beta, \end{cases}$$

where $\vec{c}\alpha$ stands for the standard dot product.

For example, if $\vec{c} = (1,5,10)$, we have $x_1^5 x_2^1 x_3^2 <_{\vec{c}} x_1^1 x_2^0 x_3^3$ since $\vec{c} \cdot \alpha = (1,5,10) \cdot (5,1,2) = 30$ and $\vec{c} \cdot \beta = (1,5,10) \cdot (1,0,3) = 31$. Note, that for $<_{\vec{c}}$ the leading term of $g = 2x_1^5 x_2^1 x_3^2 - 5x_1^1 x_2^0 x_3^3$ is $LT(g) = -5x_1^1 x_3^3$ while for $<_{lex}$ the leading term of (the same) g is $LT(g) = 2x_1^5 x_2^1 x_2^3$.

Once a ring and a monomial order are chosen, one can divide polynomial by another (set of) polynomial(s). The generalization of the Gaussian elimination process for solving system (1.1) requires to »divide a polynomial by a set of polynomials«. The well-known elementary row operations (from Gaussian elimination) are defined by the fact that on every step s (of the Gaussian elimination process for $\vec{f}_0(\vec{x}) = \vec{0}$) the solution of changed system $\vec{f}_s(\vec{x}) = \vec{0}$ remains the same. Let us recall the first example in context of notation $\vec{f}_s(\vec{x}) = \vec{0}$. The initial system: $f_0 =$ 3x + 7y - 5z - 2, $g_0 = 2x + 3y - 8z - 6$ is replaced with $f_1 = f_0$, and $g_1 = S_{f,g} = 5y + 14z + 14$. Note that $g_1 = 2f_0 - 3g_0 + 0$. Note also, that if $f_0(\tilde{x}) = 0$, $g_0(\tilde{x}) = 0$ 0 for some \tilde{x} , then $g_1(\tilde{x}) = 0$, too. The main idea is that one can replace the initial pair f_0 , g_0 with f_1 , g_1 if f_1 and g_1 can be »divided between« the initial polynomials, f_0, g_0 :

$$f_1 = 1f_0 + 0g_0$$
 and $g_1 = 2f_0 - 3g_0$

The division of a polynomial between a set of (other) polynomials is called *the multivariable division* and lead toward the definition of Groebner bases.

 $XY + 2X^3$ and choosing the lexicographic order X > Y, then we can easily verify that $f = -2f_1 + (X + 3Y - Y^2)f_2 + (-3Y^3 + Y^4)$ and on the other hand, when the »importance« of f_1, f_2 is channel to $1. f_2, 2. f_1$, we have:

$$f = (X + 2X^2 + Y - Y^2 - 2XY^2 + 2Y^4)f_2 + 0f_1 + (-3Y^3 + Y^4 - 2Y^6).$$

Considering $f_1 = XY - X^3$, $f_2 = X + Y^2$ and $f = X^2 +$

Obviously, this multivariable division is very sensitive on the order of f_1, f_2 . The order affects the multi-quotients q_1, q_2 , as well as the remainder r. When dividing the polynomial f with the (ordered) set $F = (f_1, f_2)$, one can write: $f = \{\{q_1, q_2\}, r\}$ instead of $f = q_1f_1 + q_2f_2 + r$. Using this notation, in the first case we have $f = \{\{-2, X + 3Y - Y^2\}, -3Y^3 + Y^4\}$ and in the second case we have $f = \{\{X + 2X^2 + Y - Y^2 - 2XY^2 + 2Y4, 0, -3Y3 + Y4 - 2Y6\}$.

Readily, if one chooses the lexicographic term order Y > X the results would be different again, as one can observe from Fig. 1, where system MATHEMATICA is used for the multivariable division. Obviously, Y > X gives "simpler" results than X > Y (concerning the quotients)

2. The Multivariable Division Algorithm

Figure 1. The Mathematica results for multivariable division for different monomial orders.

Concerning the problem of multivariable division we have the following result

Theorem 2.1. Fix a monomial order > and let $F = (f_1, f_2, ..., f_s)$. Then every polynomial $f \in k[x_1, x_2, ..., x_n]$ can be written as

$$f = q_1 f_1 + q_2 f_2 + \dots + q_s f_s + r$$

where $q_i, r \in k[x_1, x_2, ..., x_n]$ and either r = 0 or r is a $k[x_1, x_2, ..., x_n]$ -linear combination of monomials none of which are divisible by the leading terms of any of $f_1, f_2, ..., f_s$, which means that r is reduced with respect to $F = \{f_1, f_2, ..., f_s\}$ (i.e. r has lower degree than any of the divisors $f_1, f_2, ..., f_s$). We can alternatively write:

$$f \stackrel{F}{\longrightarrow} r.$$

The proof of the above theorem is based on the multivariable division algorithm, which can nowadays be found in any textbook of commutative algebra. It is sketched in Fig. 2 (see e.g. [13]).

Multivariable Division Algorithm

Input:
$$f \in k[x_1, x_2, ..., x_n]$$
, ordered set $F = (f_1, f_2, ..., f_s) \in k[x_1, x_2, ..., x_n] \setminus \{0\}$

Output: $q_1, q_2, ..., q_s, r \in k[x_1, x_2, ..., x_n]$ such that $1 \cdot f = q_1 f_1 + q_2 f_2 + \cdots + q_s f_s + r$ 2. r is reduced with respect to $(f_1, f_2, ..., f_s)$ 3. $\max(\operatorname{LM}(q_1)\operatorname{LM}(f_1), ..., \operatorname{LM}(q_s)\operatorname{LM}(f_s)) = \operatorname{LM}(f)$

Procedure: $q_1 := 0, ..., q_s := 0, h := f$

WHILE $h \neq 0$ DO

IF

There exists f such that f LM(f divides f LM(f divides LM(f di

Figure 2. Multivariable Division Algorithm.

Recall that the solutions of (1.1) is actually an *affine variety* defined by the ideal $I = \langle f_1, f_2, ..., f_s \rangle$. We would like to use the division algorithm for the question of ideal membership. If dividing f by $f_1, f_2, ..., f_s$ gives a remainder of zero then we know $f \in I$. But the converse is not true. Even if f has a nonzero remainder there may be some ways to divide it in a different order that gives a remainder of zero, as we will see in the following example. (Note that the example from Fig.1 shows that the remainders are not unique.)

Let us consider for example $f_1 = x^2 - 1$, $f_2 = xy + 2$ and $f = x^2y + xy + 2x + 2$ and choose the lexicographic order x > y, then we obtain

$$f = yf_1 + f_2 + (2x + y).$$

The remainder $r = 2x + y \neq 0$, thus one could conclude that $f \notin \langle f_1, f_2 \rangle$, but if the order of divisors is changed to $F = (f_2, f_1)$, we have f = 0; namely

$$f = 0f_1 + (x + 1)f_2 + 0 = (x + 1)f_2 + 0$$

and $f \in \langle f_1, f_2 \rangle$ after all.

Finally, let us consider $f_1 = x + y$, $f_2 = x - y$ and f = 2y in the ring $\mathbb{R}[x,y]$ and fix the lexicographic term order x > y. Then obviously $f = f_1 - f_2 \in \langle f_1, f_2 \rangle$, but since LT(x + y) = LT(x - y) = x, and because x > y the division algorithm from Fig. 2 returns the remainder r = 2y. As we shall see, Groebner bases are the solution to the above problems.

3. Groebner Bases

The Groebner basis is a special generating set for our ideals $\langle f_1, f_2, ..., f_n \rangle$ for which the multivariable division algorithm for a given f returns the remainder r = 0 if and only if $f \in \langle g_1, g_2, ..., g_t \rangle$.

More precisely, the Groebner basis of an ideal $I \subset k[x_1, x_2, ..., x_n]$ is a finite subset $G = \{g_1, g_2, ..., g_t\}$ of I such that

$$\langle LT(I)\rangle = \langle LT(g_1), LT(g_2), ..., LT(g_t)\rangle.$$

Every nonzero ideal $I \in k[x_1, x_2, ..., x_n]$ has the Groebner basis. Note that $\langle LT(I) \rangle = \langle LT(g) : g \in I \setminus \{0\} \rangle = \langle LM(g) : g \in I \setminus \{0\} \rangle$ is a monomial ideal and by Dickson's lemma (see [5]) $\langle LT(I) \rangle = \langle LM(g_1), LM(g_2), ..., LM(g_t) \rangle = \langle LT(g_1), LT(g_2), ..., LT(g_t) \rangle$ for some finite set $g_i \in I$.

Furthermore, due to the multivariable division algorithm, if $f \in I$ we have $f = q_1g_1 + q_2g_2 + \cdots + q_sg_s + r$ and no term of r is divisible by any of $LT(g_1), LT(g_2), \ldots, LT(g_t)$. Thus,

$$r = f - (q_1g_1 + q_2g_2 + \dots + q_s)$$

so $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), LT(g_2), ..., LT(g_t) \rangle$. But no term of r is divisible by any of the $LT(g_i)$ and so we must have r = 0, which implies:

$$f \in \langle LT(g_1), LT(g_2), ..., LT(g_t) \rangle$$
.

The opposite implication is obvious. Thus, the Groebner basis is a basis.

Obviously, if $G=\{g_1,g_2,...,g_t\}$ is the Groebner basis of I, the remainder of any $f\in I$ (after applying the multidivision algorithm) is unique. If $f=q_1g_1+q_2g_2+\cdots+q_sg_s+r$ and $f=q_1'g_1+q_2'g_2+\cdots+q_s'g_s+r'$ then $r-r'=(q_1-q_1')g_1+\cdots+(q_s-q_s')g_s\in I$. If $r-r'\neq 0$ then $LT(r-r')\in \langle LT(I)\rangle$ which implies that $LT(g_i)$ divides LT(r-r') for some i. But this leads to a contradiction, since no term of r or r' is divisible by any $LT(g_i)$. Thus, we must have r=r' and therefore g=g'.

Testing whether a basis is a Groebner basis is intimately connected with the so called S – polynomial for a given pair of polynomials $f,g \in k[x_1,x_2,...,x_n]$; a generalization of $S_{f,g}$ – polynomial defined in the introduction. The S – polynomial of f and g is defined as follows. Let $f,g \in k[x_1,x_2,...,x_n]$ be nonzero polynomials. Find the least common multiple of their leading monomials: $x^{\gamma} = LCM(LM(f),LM(g))$. Then the S – polynomial of f and g is defined by:

$$S(f,g) = \frac{x^{\gamma}}{LT(f)} \cdot f - \frac{x^{\gamma}}{LT(g)} \cdot g.$$

Note, that the S – polynomials provide cancellacion of leading terms and in fact are the only way that cancelation happens among sums of terms of the same multi-degree.

The *Buchcberger's* basic observation was the following *criterion*. Let I be an ideal. Then $G = \{g_1, g_2, ..., g_t\}$ is a Groebner bases (for I) if and only if for all $i \neq j$ the remainder on division of $S(g_i, g_i)$ by G is zero:

$$S(g_i, g_j) \stackrel{G}{\longrightarrow} 0 \quad \forall i \neq j.$$

This criterion is the basis of the famous *Buchberger's algorithm*, which produces the Groebner bases for the nonzero ideal $I = \langle f_1, f_2, ..., f_s \rangle$. The Buchberger's algorithm is shown in Fig. 3 [13].

Buchberger's Algorithm

Input: A set of polynomials $\{f_1, f_2, ..., f_s\} \in k[x_1, x_2, ..., x_n] \setminus \{0\}$

Output: A Gröbner basis G of the ideal $(f_1, f_2, ..., f_s)$.

Procedure: $G := \{f_1, f_2, ..., f_s\}.$

Step 1. For each pair $g_i, g_j \in G$, $i \neq j$, compute $S(g_i, g_j)$ and apply the multivariable division algorithm to get r_{ij} :

$$S(g_i,g_j) \stackrel{G}{\longrightarrow} r_{ij}$$

IF

All $r_{ij} = 0$, output G

ELSE

Add all nonzero r_{ij} to G and **return** to Step 1.

Figure 3. Buchberger's Algorithm: returns a Groebner basis of $I = \langle f_1, f_2, ..., f_n \rangle$.

Note, that the most efficient computer algebra systems have routines to produce Groebner bases. An example in MATHEMATICA is shown in Fig. 4. Since the Buchberger's Algorithm is based on the Multivariable Division Algorithm, which depends on the monomial term order, the computing of Groebner basis will depend on the monomial term order, as well. In Fig.4 in ν In[1]:=« we want to compute the Groebner basis with respect to the lexicographic term order with ν > ν , whilst in ν In[2]:=« with respect to the lexicographic term order with ν > ν .

Figure 4. Computing Groebner Bases in System MATHEMATICA.

Note, that Buchberger's algorithm produces a lot of »extra« basis elements than needed (i.e. it is not optimal). If we require an extra condition that no term of g_i is divisible by any $LT(g_j)$ and in order to ensure the uniqueness of G (provided the monomial term order is fixed) we also require that each g_i is *monic* (i.e. $LC(g_i) = 1$ for all i = 1, 2, ..., t), then we get the so called *reduced Groebner basis*. The reduced Groebner basis always exists and is unique (see e.g. [13] for the proof). The simple algorithm which produces the reduced Groebner basis beginning with any Groebner basis G is the following: begin with G and make all $g_i \in G$ monic, for any $g \in G$, replace g by its remainder upon division of g by elements if $G \setminus \{g\}$ (in the fixed monomial term order). Of course, the routines in all computer algebra systems already return the reduced Groebner basis. In Fig. 5 and 6 Groebner basis of $\{-x^3 + y, x^2y - y^2\}$ in the lexicographic term order are computed in system MATHEMATICA and SINGULAR. We see that MATHEMATICA returns $\{-y^2 + y^3, -y^2 + xy^2, x^2y - y^2, x^3 - y\}$, while SINGULAR returns $G[1] = y^3 - y^2$, $G[2] = xy^2 - y^2$, $G[3] = x^2y - y^2$, $G[4] = x^3 - y$.

```
\begin{split} & & \text{In[6]:= GroebnerBasis} \left[ \left\{ -\mathbf{x}^3 + \mathbf{y}, \ \mathbf{x}^2 \ \mathbf{y} - \mathbf{y}^2 \right\}, \ \left\{ \mathbf{x}, \ \mathbf{y} \right\} \right] \\ & & \text{Out[6]:= } \left\{ -\mathbf{y}^2 + \mathbf{y}^3, \ -\mathbf{y}^2 + \mathbf{x} \ \mathbf{y}^2, \ \mathbf{x}^2 \ \mathbf{y} - \mathbf{y}^2, \ \mathbf{x}^3 - \mathbf{y} \right\} \end{split}
```

Figure 5. Output of Groebner bases in system MATHEMATICA

Figure 6. Output of Groebner bases in system Singular

One reason to turn to more special systems than MATHEMATICA is to compute the Groebner basis in a special monomial term order or simply to reduce a polynomial (in sense of the multivariable division algorithm) in a special monomial term order. In Fig. 7 we show the Groebner basis of $\{-x^3+y,x^2y-y^2\}$ computed in SINGULAR with respect to the weight order with weight vector (1,3). Note, that the result $G_{<_{(1,3)}} = \{x^3-y,y^2-x^2y\}$ is not the same as the Groebner basis computed in the lexicographic monomial order $G_{<_{lex}(y>x)} = \{-x^5+x^6,-x^3+y\}$.

Figure 7. Groebner basis $G_{\leq (1,3)}$ of $\{x^3-y, -x^2y+y^2\}$ computed in SINGULAR

4. Groebner Bases and Nonlinear Systems of Equations

As mentioned before, we seek solutions $(a_1, a_2, ..., a_n) \in \bar{k}$ of polynomial system

$$f_1(x_1, x_2, ..., x_n) = 0, f_2(x_1, x_2, ..., x_n) = 0, ..., f_s(x_1, x_2, ..., x_n) = 0,$$
 (4.1)

where \bar{k} is the algebraic closure of $k[x_1, x_2, ..., x_n]$. The following theorem gives a criterion on existence of solutions of (4.1). For a proof, see [1]. Let $G = \{g_1, g_2, ..., g_t\}$ be the reduced Groebner basis of $\langle f_1, f_2, ..., f_s \rangle$. There are no solutions to the system (4.1) if and only if $G = \{1\}$. If (4.1) has finitely many solutions, we say that $\langle f_1, f_2, ..., f_s \rangle$ is zero-dimensional. Concerning Groebner basis, $\langle f_1, f_2, ..., f_s \rangle$ (corresponding to (4.1)) is zero-dimensional if and only if for every i = 1, 2, ..., n, there exists $j \in \{1, 2, ..., t\}$ such that $LM(g_i) = x_i^{\alpha}$ for some $\alpha \in \mathbb{N}_0^n$. Note, that if $I = \langle f_1, f_2, ..., f_s \rangle$ is not zero-dimensional, one has to compute the so called *primary decomposition* of I, which is much more complicated then the computations presented in the following example; see [13] for more details.

We want to solve the example from [6]:

$$f_1 = x^2 + yz + x = 0$$
, $f_2 = z^2 + xy + z = 0$, $f_3 = y^2 + xz + y = 0$. (4.2)

To that end, fix the term order to be lexicographic x > y > z. We find Groebner basis of $\langle f_1, f_2, f_3 \rangle$ using system MATHEMATICA (see Fig. 8):

Figure 8. Groebner basis of $\langle f_1, f_2, f_3 \rangle$ associated to (4.1).

Since the first polynomial depends only on z, z is either 0, $-\frac{1}{2}$ or -1. The system has obviously finitely many solutions, since the third polynomial in G contains only z and y and its leading power product is y^2 . And finally, the last polynomial contains x and y and its leading power product is x^2 . If z = 0 the system becomes $y + y^2 =$ $0, xy = 0, x + x^2 = 0$. And the (reduced) set of polynomials is already a reduced Groebner basis of the ideal it generates. The corresponding solutions are y = 0 and x = 0 or x = -1 and y = -1 and x = 0. Our solutions so far are (0,0,0), (-1,0,0) and (0,-1,0). Similar, for z=-1 we get $y^2 = 0, -x + y = 0, xy = 0, x + x^2 - y = 0$. The corresponding reduced Groebner basis is $\{y, x\}$, which yields x = y = 0. So another solution is (0,0,-1). Similar we get for $z = -\frac{1}{2}$ the corresponding reduced Groebner basis: $\{2y + 1, 2x + 1\}$, which yields the final solution $\left(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}\right)$

5. Groebner Bases and Integer Linear Programming

Let $a_{i,j} \in \mathbb{Z}$, $b_i \in \mathbb{Z}$ and $c_j \in \mathbb{R}$ with i = 1,2,...,n and j = 1,2,...,m. We seek a solution $\vec{x} = (x_1, x_2,...,x_n)$ of the system

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \vdots a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m.$$
 (5.1)

which minimizes the cost function $c(x_1, x_2, ..., x_m) =$

 $\sum_{j=1}^{n} c_j x_j$. We call (5.1) an integer (linear) program (IP) and write it in a matrix form:

minimize
$$\vec{c} \cdot \vec{x}$$
 subject to $A\vec{x} = \vec{b}$, where $A \in \mathbb{Z}^{m \times n}$ and $\vec{b} = (b_1, ..., b_m) \in \mathbb{Z}^m$.

We will consider just the main mathematical idea which makes use of Groebner bases when solving IP (5.1). We can associate to (5.1) new variables X_k ; k = 1, 2, ..., m to represent the k —th equation in (5.1) as:

$$X_k^{a_{k1}x_1 + a_{k2}x_2 + \dots + a_{kn}x_n} = X_k^{b_k}.$$

Of course, we can then write the whole system as

$$\begin{split} X_1^{a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n} & \cdots X_m^{a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n} \\ & = X_1^{b_1} & \cdots X_m^{b_m}, \end{split}$$

which is equivalent to

$$\left(X_1^{a_{11}} \cdots X_m^{a_{m1}} \right)^{x_1} \cdot \cdots \cdot \left(X_1^{a_{1n}} \cdots X_m^{a_{mn}} \right)^{x_n} = \vec{X}^{\vec{b}}.$$

Next, to each column of (5.1) or equivalently to each term in the brackets (...) in the above equation we associate a new variable $Y_k = X_1^{a_{1k}} \cdots X_m^{a_{mk}}$; for each k = 1,2,...,n. The first step in solving our problem is to figure out whether a solution exists at all. The theory of Groebner bases helps to characterize the existence and optimality of IP (5.1). The main idea is connected with the following ring homomorphism $\Phi: k[Y_1,...,Y_n] \to k[X_1,...,X_m]$, defined by:

$$\Phi(Y_k) = X_1^{a_{1k}} \cdots X_m^{a_{mk}}, \tag{5.2}$$

yielding $\Phi(Y_1^{x_1} \cdot \dots \cdot Y_n^{x_n}) = \vec{X}^{\vec{b}}$. This implies (see [9] for details) the following: there exist a solution to IP (5.1) (i.e. a vector $\vec{x} = \vec{x}$ such that $A\vec{x} = \vec{b}$) if and only if $\vec{X}^{\vec{b}}$ is in the image of Φ ; yielding $\exists P$ such that $P = \vec{Y}^{\vec{x}}$ for some $\vec{x} \in \mathbb{N}_0^n$.

Next, the basic idea of Conti & Traverso's algorithm[4] is presented. But first we have to consider how to transform (5.1) which can contain some negative integres; recall that $a_{i,j} \in \mathbb{Z}$ and $b_i \in \mathbb{Z}$. This can be generally transformed to an IP with strictly nonnegative (integer) coefficients $a_{i,j}$, b_i by adding an extra indeterminate W defined by

$$X_1 \cdot X_2 \cdot \dots \cdot X_m \cdot W = 1, \tag{5.3}$$

which transforms $X_1^{a_{1j}} \cdot \cdots \cdot X_i^{-a_{ij}} \cdot \cdots \cdot X_m^{a_{mj}}$ to

$$X_1^{a_{1j}+a_{ij}}\cdots X_i^0 \cdots X_m^{a_{mj}+a_{ij}} \cdot W^{a_{ij}} =: \vec{X}^{Aj} W_j.$$

If there are some negative entries in \vec{b} , we transform $\vec{X}^{\vec{b}}$ to $\vec{X}^{\vec{b}}W_{\vec{b}}$ in a similar way.

The optimal solution of IP (5.1) with some negative integers is therefore obtained in the following way:

- Define W by (5.3), if there are some negative entries in \vec{A} , \vec{b}
- Define an ideal $I = \{Y_1 \vec{X}^{A_1}, \dots, Y_n \vec{X}^{A_n}\}$ on the polynomial ring $k[X_1, \dots, X_m, Y_1, \dots, Y_n]$, if there are no negative entries in A, \vec{b}
- Define an ideal $I = \{Y_1 \vec{X}^{A1}W_1, ..., Y_n \vec{X}^{An}W_n, X_1 \cdot X2 \cdot ... \cdot Xm \cdot W 1 \text{ on the polynomial ring } k[X_1, ..., X_m, W, Y_1, ..., Y_n], if there are some negative entries in <math>A, \vec{b}$
- Let G be the reduced Groebner basis of I with respect to a monomial order $<_{\vec{c}}$, where \vec{c} is defined by the cost

function $\vec{c} \cdot \vec{x}$

• Dividing $\vec{X}^{\vec{b}}W_{\vec{b}}$ (i.e. the generalization of $\vec{X}^{\vec{b}}$) by Galways yields a remainder $R \in k[Y_1, ..., Y_n]$, which ensures the optimality of the solution due to its minimality (ensured by the multivariable division algorithm); thus the solution $\vec{x} = (\beta_1, ..., \beta_n)$ to IP (5.1) is obtained by reducing $\vec{X}^{\vec{b}}W_{\vec{b}}$ by G which yields a remainder $R = Y_1^{\beta_1} \cdots Y_n^{\beta_n}$ and thereby the solution $\vec{x} = (\beta_1, ..., \beta_n)$.

Next, we consider the example from [9]. Following (5.1), we have to minimize the cost function

$$\vec{c} \cdot \vec{x} = 1000x_1 + x_2 + x_3 + 100x_4$$

subject to

$$3x_1 - 2x_2 + x_3 - x_4 = -1$$

$$4x_1 + x_2 - x_3 = 5.$$
 (5.4)

The solution to the above example obtained with system SINGULAR is shown in Fig.9. The weighted term order is used with $\vec{C}=(1000002,1000001,1000000,1000,1,1,100)$ to ensure that X1>X2>W>Y1>Y2>Y3>Y4 and to ensure the weight order (1000,1,1,100), corresponding to $\vec{c}=(1000,1,1,100)$. Note, that for example the monomials $\vec{X}^{\vec{b}}W_{\vec{b}}$ and $\vec{X}^{A2}W_2$ are:

$$\vec{X}^{\vec{b}}W_{\vec{b}} = X_1^{-1}X_2^5 = X_1^{-1}X_2^{-1} \cdot X_2^1X_2^5 = W^1X_2^6,$$

$$\vec{X}^{A2}W_2 = X_1^{-2}X_2^1 = X_1^{-2}X_2^{-2} \cdot X_2^2X_2^1 = W^2X_2^3.$$

The optimal solution $\vec{x} = (1,3,2,0)$ is obtained from the result of the multivariable division:

$$W^1X_2^6 \stackrel{G}{\longrightarrow} Y_1^1Y_2^3Y_3^2Y_4^0$$

```
SINGULAR

A Computer Algebra System for Polynomial Computations

by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann

B Mathematik der Universitaet, D-67653 Kaiserslautern

ring r1=0,(X1,X2,W,Y1,Y2,Y3,Y4),Wp(1000002,1000001,10000000,1000,1,1,100);

poly f1=Y1-X13*X24;

poly f1=Y1-X13*X24;

poly f2=Y2-X23*W^2;

poly f3=Y3-X1^2*W;

poly f3=Y3-X1^2*W;

poly f4=Y4-X2*W;

poly f5=X1*X2*W-1;

ideal I=f1,f2,f3,f4,f5;

ideal gI=groebner(I);

reduce(W*X2^6,gI);

Y1*Y2^3*Y3^2

**Oversion 3-1-4

0
```

Figure 9. Computing the optimal solution of IP (5.4) in system SINGULAR.

6. Groebner Bases and Computing the Chromatic Number

One of the most important and applied things in graph theory is the *chromatic number* of a graph. It is defined as the smallest number of colours needed to colour the vertices of graph G = (V, E) so that no two adjacent vertices $k, s \in V$ share the same colour. For many (families) of graphs the chromatic numbers are known (i.e. defined in terms of the number of its vertices and/or edges). Probably the most simple examples are cycle graphs C_n : a cycle graph C_{2k} has chromatic number 2, whilst C_{2k+1} has chromatic number 3, which is usually denoted by $\mathcal{X}(C_{2k+1}) = 3$, $\mathcal{X}(C_{2k}) = 2$. There are many well-known conjectures and open problems concerning the chromatic number of (undirected) graphs (e.g. Hadwiger conjecture, Albertson conjecture, Erdös-Faber-Lovász conjecture). The subject inspired many researchers (e.g. [2,11,15]). The idea of finding a n -colloring and consequently the chromatic number of a given graph using Groebner bases is to associate a variable x[k] to each vertex k of the graph and to reduce the problem to the solution of a system of polynomial equations. The n —th roots of unity is used as ncolours. Since variables x[k] represent the vertices, the condition that a vertex k should have a colour is then associated to roots of

$$x[k]^n - 1 = 0 (6.1)$$

and the polynomial $(x[k]^n - x[s]^n)/(x[k] - x[s])$ is associated to the condition that the vertices k and s (corresponding to x[k] and x[s]) must have different colours (see also [1]). Thus, if vertices k and s are adjacent and the graph has to be coloured by n colours, the polynomial

$$Fn[k,s] = x[k]^{n-1} + x[k]^{n-2}x[s]^{1} + \cdots + x[k]^{1}x[s]^{n-2} + x[s]^{n-1}$$
 (6.2)

must vanish. Thus finding a chromatic number of a given graph G = (V, E) with |V| = N is then obtained by

applying the following algorithm:

- **Input**: Graph G = (V, E) (i.e. vertices x[1], ..., x[N] and the adjacency matrix A(G))
- Output: chromatic number $\mathcal{X}(G)$
- Procedure:
- $n \coloneqq 1$
- WHILE $GIn = \{1\}$ DO $I = \bigcup_{k=1}^{N} \{x[k]^n 1\}$
- For all adjacent vertices k and s compute polynomial Fn[k,s] defined by (6.2) and add it to the ideal I:

$$I := I \cup Fn[k,s]$$

- Compute Groebner basis GIn of I
- IF $GIn = \{1\}$ THEN n := n + 1
- Find a solution (i.e. colouring) of $GIn = \{0, ..., 0\}$; $\mathcal{X}(G) = n$

As an example, the computation of $\mathcal{X}(G)$ (where $G = K_5$ - a complete graph on 5 vertices; see Fig. 10) using the basic system MATHEMATICA is presented in Figs. 11 and 12. In Fig. 11 we see that $GI3 = \{1\}$. Similarly we obtain that $GI4 = \{1\}$. Note that the command

$$Do[Print[Fn[k, s]], \{k, N\}, \{s, k - 1\}]$$

is very useful since it gives a list of all possible edges.

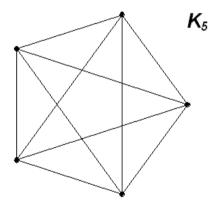


Figure 10. Graph $G = K_5$.

```
 \begin{split} & \ln[1] = \ \mathbf{F3}[k_-, s_-] = \mathbf{x}[\mathbf{k}]^2 + \mathbf{x}[\mathbf{k}] \ \mathbf{x}[\mathbf{s}] + \mathbf{x}[\mathbf{s}]^2; \\ & \ln[2] = \ \mathrm{Do}[\mathrm{Print}[\mathbf{F3}[\mathbf{k}, \mathbf{s}]], \ \{\mathbf{k}, \mathbf{5}\}, \ \{\mathbf{s}, \mathbf{k} - 1\}] \\ & \times [1]^2 + \mathbf{x}[1] \ \mathbf{x}[2] + \mathbf{x}[2]^2, \ \mathbf{x}[1]^2 + \mathbf{x}[1] \ \mathbf{x}[3] + \mathbf{x}[3]^2, \ \mathbf{x}[2]^2 + \mathbf{x}[2] \ \mathbf{x}[3] + \mathbf{x}[3]^2 \\ & \times [1]^2 + \mathbf{x}[1] \ \mathbf{x}[4] + \mathbf{x}[4]^2, \ \mathbf{x}[2]^2 + \mathbf{x}[2] \ \mathbf{x}[4] + \mathbf{x}[4]^2, \ \mathbf{x}[2]^2 + \mathbf{x}[2] \ \mathbf{x}[4] + \mathbf{x}[4]^2, \\ & \times [3]^2 + \mathbf{x}[3] \ \mathbf{x}[4] + \mathbf{x}[4]^2, \ \mathbf{x}[1]^2 + \mathbf{x}[1] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \ \mathbf{x}[2]^2 + \mathbf{x}[2] \ \mathbf{x}[5] + \mathbf{x}[5]^2 \\ & \times [3]^2 + \mathbf{x}[3] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \ \mathbf{x}[4]^2 + \mathbf{x}[4] \ \mathbf{x}[5] + \mathbf{x}[5]^2 \\ & \times [3]^2 + \mathbf{x}[2] \ \mathbf{x}[3] + \mathbf{x}[3]^2, \ \mathbf{x}[4]^2 + \mathbf{x}[4] \ \mathbf{x}[3]^3 - 1, \ \mathbf{x}[4]^3 - 1, \ \mathbf{x}[5]^3 - 1, \ \mathbf{x}[1]^2 + \mathbf{x}[1] \ \mathbf{x}[3] + \mathbf{x}[3]^2, \\ & \times [2]^2 + \mathbf{x}[2] \ \mathbf{x}[3] + \mathbf{x}[3]^2, \ \mathbf{x}[1]^2 + \mathbf{x}[1] \ \mathbf{x}[4] + \mathbf{x}[4]^2, \ \mathbf{x}[2]^2 + \mathbf{x}[2] \ \mathbf{x}[4] + \mathbf{x}[4]^2, \ \mathbf{x}[3]^2 + \mathbf{x}[3] \ \mathbf{x}[4] + \mathbf{x}[4]^2, \\ & \times [1]^2 + \mathbf{x}[1] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \ \mathbf{x}[2]^2 + \mathbf{x}[2] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \ \mathbf{x}[3]^2 + \mathbf{x}[3] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \ \mathbf{x}[4]^2 + \mathbf{x}[4] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \\ & \times [1]^2 + \mathbf{x}[1] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \ \mathbf{x}[2]^2 + \mathbf{x}[2] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \ \mathbf{x}[3]^2 + \mathbf{x}[3] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \ \mathbf{x}[4]^2 + \mathbf{x}[4] \ \mathbf{x}[5] + \mathbf{x}[5]^2, \\ & \times [1]^2 + \mathbf{x}[1] \ \mathbf{x}[3], \ \mathbf{x}[2], \ \mathbf{x}[1]\} \\ & \text{Out}[3] = \{1\} \end{aligned}
```

Figure 11. Computing $GI3 = \{1\}$ for $G = K_5$ and n = 3.

```
\ln[3] = \text{GroebnerBasis} \left[ \left\{ x[1]^5 - 1, x[2]^5 - 1, x[3]^5 - 1, x[4]^5 - 1, x[5]^5 - 1, \right\} \right]
                                x[1]^{4} + x[1]^{3}x[2] + x[1]^{2}x[2]^{2} + x[1]x[2]^{3} + x[2]^{4}, x[1]^{4} + x[1]^{3}x[3] + x[1]^{2}x[3]^{2} + x[1]x[3]^{3} + x[3]^{4},
                                x[2]^4 + x[2]^3 x[3] + x[2]^2 x[3]^2 + x[2] x[3]^3 + x[3]^4, x[1]^4 + x[1]^3 x[4] + x[1]^2 x[4]^2 + x[1] x[4]^3 + x[4]^4,
                                x[2]^4 + x[2]^3 x[4] + x[2]^2 x[4]^2 + x[2] x[4]^3 + x[4]^4, x[3]^4 + x[3]^3 x[4] + x[3]^2 x[4]^2 + x[3] x[4]^3 + x[4]^4,
                                x[1]^4 + x[1]^3 x[5] + x[1]^2 x[5]^2 + x[1] x[5]^3 + x[5]^4, x[2]^4 + x[2]^3 x[5] + x[2]^2 x[5]^2 + x[2] x[5]^3 + x[5]^4, x[2]^4 + x[2]^3 x[5]^4 + x[2]^3 x[2]^4 + x[2]^3 x[
                                x[3]^4 + x[3]^3 x[5] + x[3]^2 x[5]^2 + x[3] x[5]^3 + x[5]^4, x[4]^4 + x[4]^3 x[5] + x[4]^2 x[5]^2 + x[4] x[5]^3 + x[5]^4,
                            \{x[5], x[4], x[3], x[2], x[1]\}
Out[3]= \left\{-1 + x[1]^5, x[1]^4 + x[1]^3 x[2] + x[1]^2 x[2]^2 + x[1] x[2]^3 + x[2]^4, \right\}
                           x[1]^3 + x[1]^2 x[2] + x[1] x[2]^2 + x[2]^3 + x[1]^2 x[3] + x[1] x[2] x[3] + x[2]^2 x[3] + x[1] x[3]^2 + x[2] x[3]^2 + x[3]^3, x[1]^2 + x[1] x[2] + x[1] x[2]^2 + x[1] x[3]^2 + x[3]^3 + x[1]^2 + x[1] x[2]^2 + x[1] x[3]^2 + x[3]^3 + x[
                           x[1] + x[2] + x[3] + x[4] + x[5]
   \ln[4] = GI5 = \{-1 + x[1]^5, x[1]^4 + x[1]^3 x[2] + x[1]^2 x[2]^2 + x[1] x[2]^3 + x[2]^4,
                                    x[1]^3 + x[1]^2 x[2] + x[1] x[2]^2 + x[2]^3 + x[1]^2 x[3] + x[1] x[2] x[3] + x[2]^2 x[3] + x[1] x[3]^2 + x[2] x[3]^2 + x[3]^3
                                    x[1]^2 + x[1] x[2] + x[2]^2 + x[1] x[3] + x[2] x[3] + x[3]^2 + x[1] x[4] + x[2] x[4] + x[3] x[4] + x[4]^2
                                     x[1] + x[2] + x[3] + x[4] + x[5];
   \ln[5] = \mathbf{x}[1] = 1; \mathbf{x}[2] = -(-1)^{1/5}; \mathbf{x}[3] = (-1)^{2/5}; \mathbf{x}[4] = -(-1)^{3/5}; \mathbf{x}[5] = (-1)^{4/5};
   In[6]:= GI5 // FullSimplify
Out[6]= {0, 0, 0, 0, 0}
```

Figure 12. Computing GI5 for $G = K_5$; n = 5 and solving system »GI5=0«.

In Fig. 12 GI5 is computed and the solution to GI5 = 0 is verified. Though it is well-known that $\mathcal{X}(K_n) = n$, yet the example is very practical and instructive (since K_n contains all (simple) edges on n points). In package »Combinatorica« it is possible to compute the chromatic number of a given graph in MATHEMATICA. However, the above procedure may be useful to handle some general (families of) graphs.

7. Groebner Bases and Systems of ODE's

Concerning the qualitative analysis of systems of ODE's (e.g. solving the center-focus problem, cyclicity problems, critical period perturbations, finding linearizability and isochronicity conditions for a given polynomial family), computing of Groebner basis is the first step toward the solution of the problem. Practical problems of this kind are related to questions like: are two polynomial ideals the same, what is the radical of given ideal, etc.

The system $\vec{x}' = A\vec{x} + \vec{X}(\vec{x})$, where A is a matrix and $\vec{X}(\vec{x})$ represents nonlinear terms, is *linearizable* if there is an analytic normalizing transformation $\vec{x} = \vec{y} + \vec{h}(\vec{y})$, where $\vec{h}(\vec{y})$ represents the nonlinear terms, that places $\vec{x}' = A\vec{x} + \vec{X}(\vec{x})$ into the normal form $\vec{y}' = A\vec{y}$.

By the Hilbert Basis Theorem every ideal in the polynomial ring $k[x_1, x_2, ..., x_n]$ over a field k is finitely generated. See [5] for the proof. Moreover, every ascending chain of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ in $k[x_1, x_2, ..., x_n]$ stabilizes, which means that there exists $m \ge 1$ such that for every j > m, $I_j = I_m$ (see [13] for the proof). This is the main idea behind the qualitative investigation of dynamics in polynomial systems of ODE's.

Among many problems we show an original result from [12]. In particular, the problem is arriving from the following 3D system

$$\dot{u} = -v + au^{2} + av^{2} + cuv + dvw,$$

$$\dot{v} = u + bu^{2} + bv^{2} + euv + fvw,$$

$$\dot{w} = -w + Su^{2} + Sv^{2} + Tuv + Uvw,$$
(7.1)

where a, b, c, d, e, f, S, T, U are real coefficients. The system (7.1) was already studied in [7,12] and [8] where planar polynomial systems of ODE's appearing on the center manifold of (7.1) were investigated. Often in order to consider the dynamics on a 2D center manifold of a 3D system like (7.1); i.e. in order to consider a system of the form

$$\dot{u} = -v + (a + dv)(u^2 + v^2),$$

$$\dot{v} = u + (b - du)(u^2 + v^2)$$
(7.2)

one has to introduce the following complex coordinates x = u + iv and y = u - iv. Then (7.2) after substitution $a_{11} = b_{11} = d$, $a_{01} = -b + ia$, $b_{10} = -b - ia$ yields the following complex system:

$$\dot{x} = i(x - a_{11}x^2y - a_{01}xy)$$

$$\dot{y} = -i(a + b_{11}xy^2 + b_{10}xy), \tag{7.3}$$

where a_{kj} , $b_{kj} \in \mathbb{C}$. The following result is based on computing of Groebner basis $G = \{b_{11}^2, a_{01}b_{10} + b_{11}\}$ (with respect to the degree lexicographic order) of the (linearizability) ideal I, which is in this particular case(see (Romanovski et.al., 2013) for details) defined by:

$$I = \langle \frac{a_{11} + 2a_{01}b_{10} + b_{11}}{2}, \frac{a_{11}^2 + 8a_{01}^2b_{10}^2 + 10a_{01}b_{10}b_{11} + b_{11}^2 + 2a_{11}(5a_{01}b_{10} + b_{11})}{4} \rangle.$$

Theorem 6.1. System (7.3) is linearizable if and only if one of the following conditions holds:

- (i) $a_{01}b_{10} + b_{11} = b_{10} = a_{11} b_{11} = 0$;
- (ii) $a_{01}b_{10} + b_{11} = a_{01} = a_{11} b_{11} = 0$.

7. Conclusions

In general, mathematical theories are considered to be more valuable if they turn out to be useful in a broader variety of fields. In order to get an idea of the value of Groebner basis, we have listed some applications. The use of Groebner bases theory in studying systems of ODE's is very wide. See for example [7,8,12,13] and the references therein. The geometrical origin of integer (linear) programming is considered in [14]. System SINGULAR (see [10] is a free computer algebra system for polynomial computations. It can be downloaded at http://www.singular.uni-kl.de/. SINGULAR features one of the fastest implementations of Buchberger's algorithm to compute a Groebner basis. We used system SINGULAR for computing Groebner bases with respect to different monomial order. Among many other applications in science and engineering we emphasize just the use of Groebner bases in coding theory and in robotics.

Acknowledgments

The author acknowledges the support of this work by the Slovenian Research Agency.

REFERENCES

- W.W. Adams, P. Loustaunau. An introduction to Groebner basis, AMS, Providence, RI, 1994.
- [2] S. Akbari, M. Aryapoor, M. Jamaali. Chromatic number and clique number of subgraphs of regular *graph* of matrix algebras. Linear Algebra and its Applications (2012), no. 436, p. 2419–2424.
- [3] B. Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restlasseringes nach einem

- nulldimensionalen Polynomideal. PhD Thesis, Mathematical Institute, University of Innsbruck, Austria, 1965.
- [4] P. Conti, C. Traverso. Buchberger algorithm and integer programming. Proceedings AAECC-9 (new Orleans), Springer LNCS, (1991) 539, p. 130-139.
- [5] D. Cox, J. Little, D. O'Shea. Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geomety and Commutative Algebra. New York: Springer, 2007.
- [6] S.R. Czapor. Groebner basis methods for solving algebraic equations. Ph.D Thesis. University of Waterloo, Canada, 1988.
- [7] V.F. Edneral, A. Mahdi, V.G. Romanovski, D.S. Shafer. The center problem on a center manifold in R3, Nonlinear Anal., (2012) Vol. 75, p. 2614-2622.
- [8] B. Ferčec, M. Mencinger. Isochronicity of centers at a center manifold, AIP conference proceedings, 1468. Melville, N.Y.: American Institute of Physics, (2012), p. 148-157.
- [9] S. Flory, E. Michel. Integer programming with Groebner bases, Online available from: http://www.iwr.uni-heidelberg.de/groups/amj/People/Eberha rd.Michel/Documents/Else/DiscreteOptimization.pdf
- [10] G.M. Greuel, G. Pfister, H. Schönemann. Singular 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005.
- [11] E.L. Lawler. A note on the complexity of the chromatic number problem. Information Processing Lett., (1976), Vol. 5, No. 3, p. 66–67.
- [12] V.G. Romanovski, M. Mencinger, B. Ferčec. Investigation of center manifolds of 3-dimsystems using computer algebra. Program. comput. softw., (2013), Vol. 39, No. 2, p. 67-73.
- [13] V.G. Romanovski, D. Shafer. The center and cyclicity problems: A computational algebra approach. Boston: Birkhauser Verlag, 2009.
- [14] R.R. Thomas. A Geometric Buchberger Algorithm for Integer Programming. Mathematics of Operations Research, (1995), Vol 11, No.1, p. 864-884.
- [15] W. Wang. Total chromatic number of planar graphs with maximum degree ten. Graph Theory, (2007), Vol. 54, p. 91-102.