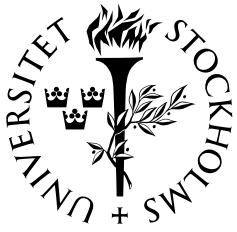


SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Gröbner bases and applications

av

Emma Knutsson

2009 - No 10

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 10691 STOCKHOLM

Gröbner bases and applications

Emma Knutsson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Ralf Fröberg

2009

Abstract

Bruno Buchberger initiated the theory of Gröbner bases and Buchberger's algorithm 1965, since then it has been the key to solve many problems in physics, chemistry and last but not least computational algebra. This essay is a first introduction to Gröbner Bases. We will go through the theoretical background of Gröbner Bases and Buchberger's algorithm and we will look at some applications where we use Gröbner bases to solve systems of polynomial eqution and implicitization problems.

Acknowledgements

I would like to take this opportunity to thank my supervisor Ralf Fröberg for his time, guidance and support. I also like to thank my examiner Christian Gottlieb and my friends Jens Forgård and Erik Melander for their good advices and comments. This essey I dedicate to three people whom has made it possiblie, my mom, my dad, and my beloved husband Jonas.

Contents

Chapter 1

Introduction

The Buchberger algorithm was created to be used on computers. It is formulated in a way which makes it easy to implement and execute on computers. The consequence is that when you just read through the algorithm it's hard to really understand why the algorithm works. I want to know why it works and the direct formulating just makes it even more interesting. Another thing which makes Buchberger's algorithm and Gröbner bases interesting is that it has been found to have many applications both in mathematics and other sciences such as chemistry and physics. It seems to be more or less a rule that with every question answered come ten new ones and you can easily say the theory of Gröbner bases and Buchberger's algorithm has given us many new questions to explore.

1.1 Bruno Buchberger

1965 Bruno Buchberger initiated the theory of Gröbner bases and Buchberger's algorithm in his PhD thesis. Today he is a professor at Johannes Kepler University, Linz, Austria and director of the Software Park Hagenberg, Austria (Buchberger 20090518, internet). Buchberger gave the theory the name Gröbner bases to honour his thesis adviser Wolfgang Gröbner (Fröberg 2005).

1.2 Algebra

I will assume you know some algebra before you read this essay. You should be familiar with basic abstract algebra such as rings, fields and ideals. The Buchberger algorithm is a kind of division algorithm which has the special quailty that it works on polynomial rings so it may be to your advantage to know how normal division algorithms over fields work.

Chapter 2

Introductory Example

We all know how to solve system of linear equations, it's usually not hard and a part of our basic algebra knowledge. The question is what happens when you get system of equations with multiple variables in higher degrees. Are we still able to solve the system and if so, how do we do it? The answer is that if we have a system with a finite number of solution we can use Buchberger's algorithm to calculate a suitable Gröbner basis and thereby solve the system. And before we go through the actual theory of Gröbner bases and Buchberger's algorithm we will start with a small example on this application of Buchberger's algorithm.

Example 2.0.1 *We want to solve the system*

$$\begin{cases} f_1 = x^2y + x = 0 \\ f_2 = x^2 - y^2 = 0 \end{cases}$$

We let
$S(f_1, f_2) = f_3 = f_1 - yf_2 = (x^2y+x) - y(x^2-y^2) = x^2y+x-x^2y+y^3 = x+y^3$
Since $f_1 = f_2 = 0$ *we also have* $f_3 = 0$ *so without changing the solution to the system we extend it with* f_3*. We will get back to the more formal definition of* S *later.*

$$\begin{cases} f_1 = x^2y + x = 0 \\ f_2 = x^2 - y^2 = 0 \\ f_3 = x + y^3 = 0 \end{cases}$$

In this system the same information is stored in more than one place, so we will take away what we don't need. $f_3 \Rightarrow x = -y^3$ *which in* f_1 *gives that* $x^2y + x = x^2y + (-y^3) = x^2y - y^3$*. In* f_2 *we have* $x^2 = y^2$*, applied on* f_1 *this gives* $f_1 = x^2y - y^3 = y^2y - y^3 = 0$*. If we use that* $x = -y^3$ *on* f_2 *we get* $f_2 = x^2 - y^2 = (-y^3)^2 - y^2 = y^6 - y^2$*. The process leaves us with the following system:*

$$\begin{cases} f_2 = y^6 - y^2 = 0 \\ f_3 = x + y^3 = 0 \end{cases}$$

$S(f_2, f_3) = x(y^6 - y^2) - y^6(x + y^3) = xy^6 - xy^2 - xy^6 - y^9 = -xy^2 - y^9$
Using that $y^6 = y^2$ *and* $x = -y^3$ *we have that*
$S(f_2, f_3) = -xy^2 - y^9 = -xy^2 - y^6y^3 = -(-y^3)y^2 - (y^2)y^3 = y^5 - y^5 = 0$

This means that $\{x + y^3, y^6 - y^2\}$ *is a Gröbner basis.*
Now $y^6 - y^2 = y^2(y^4 - 1) = y^2(y - 1)(y + 1)(y^2 + 1) = 0$, *which gives*

$$\begin{cases} y_1 = 0 \\ y_2 = 1 \\ y_3 = -1 \\ y_4 = i \\ y_5 = -i \end{cases}$$

and this gives

$$\begin{cases} x_1 = 0 \\ x_2 = -1 \\ x_3 = 1 \\ x_4 = -i \\ x_5 = i \end{cases}$$

and the system is solved.

Chapter 3

Monomial orderings

The monomial orderings play an important part when we want to calculate Gröbner bases. In Buchberger's algorithm we need to be able to compare monomials and therefore we need to determine an internal order between variables. We have to decide if $x_1 > \cdots > x_n$, $x_n > \cdots > x_1$, or if there are some other ordering between them.

Definition 3.0.1 *A **Monomial** in $x_1, \ldots, x_n$ is a product of the form $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where all of the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers.*

Definition 3.0.2 *A **Polynomial** in $x_1, \ldots, x_n$ with coefficients in k is a linear combination of monomials.*

3.1 Monomial ordering

Definition 3.1.1 *We define $\prec$ to be an admissible ordering on the set of monomials **M** if:*

- For any of monomials $m, n \in \mathbf{M}$ we have $m \prec n$ or $n \prec m$ or $m = n$
- If $m_1 \prec m_2$ and $m_2 \prec m_3$ then $m_1 \prec m_3$, $m_i \in \mathbf{M}$, $i = 1, 2, 3$
- $1 \prec m$ for any monomial $m \in \mathbf{M}$, $m \neq 1$
- If $m_1 \prec m_2$, $m_i \in \mathbf{M}$ then $mm_1 \prec mm_2$ for any monomial $m \in \mathbf{M}$

Different orderings give different Gröbner bases with specific qualities. Which ordering you choose depends mainly on the problem you want to solve and choosing a good ordering can do a lot for the efficiency, both while calulating and using the Gröbner basis. We will start by going through a few examples of the most common monomial orderings and have a short discussion on which one to choose later.

For the **Lexicographic ordering**, denoted Lex, we have that a monomial $x_1^{i_1} \cdots x_n^{i_n} \prec_{Lex} x_1^{j_1} \cdots x_n^{j_n}$ if $i_1 = j_1, \ldots, i_k = j_k$, $i_{k+1} < j_{k+1}$ for some k. The $Lex - ordering$ can in some ways be looked at as a generalization of how words are ordered in a lexcion and the name *Lexicographic* reflects that.

Example 3.1.1 *$x_2^4 x_3^5 \prec_{Lex} x_1 x_2^3$ since for $x_2^4 x_3^5$, x_1^0 which gives $i_1 = 0$ and for $x_1 x_2^2$, $j_1 = 1 \Rightarrow i_1 < j_1$.*

In degree orderings as the **Degree Lexicographical ordering**, $Deglex$, and the **Degree Reverse Lexicographical ordering**, $Degrevlex$, the main comparison is in the degree of the monomial. We have that a monomial $m = x_1^{i_1} \cdots x_n^{i_n} \prec_{deglex} x_1^{j_1} \cdots x_n^{j_n} = n$ if $deg(m) = i_1 + \cdots + i_n < j_1 + \cdots + j_n = deg(n)$ or if $deg(m) = deg(n)$ and $m \prec_{Lex} n$.

Example 3.1.2 *In the degree lexicographical ordering*
$x_1^2 x_2 \prec_{deglex} x_2 x_3^3$ since $deg(x_1^2 x_2) = 3$ which is smaller then $deg(x_2 x_3^3) = 4$.

In the degree reverse lexicographical ordering we have that a monomial $m = x_1^{i_1} \cdots x_n^{i_n} \prec_{degrevlex} x_1^{j_1} \cdots x_n^{j_n} = n$ if $deg(m) < deg(n)$ or if $deg(m) = deg(n)$ and $i_n = j_n, i_{n-1} = j_{n-1}, \ldots, i_k = jk, i_{k-1} > j_{k-1}$ for some k.

Example 3.1.3 *In the degree reversed lexicographical ordering we*
$m = x_1^2 x_2^3 x_3^4 \prec_{degrevlex} x_1^3 x_2^2 x_3^4 = n$ since both m, n have degree 9 and for the last component which is not equal, x_2 we have $i_{k-1} = 3 > 2 = j_{k-1}$.

So which ordering is good for what? There seems to be no easy answer to this question. It depends on the specific problem you want to solve, what kind of problem it is, your input and if you have demands on efficiency. Often the best way to find a good ordering is to experiment. What we can say is that if you have an elimination problem, for example if you want to solve a system of equations, you will always get a useful Gröbner basis if you use the Lexicographical ordering. It has been proved that for a random generated problem the degree reversed lexicographical ordering is the fastest one. The problem is that there is no guarantee that the Gröbner basis you get can be used for elimination problems.

The monomial ordering gives us the possibility to separate and compare different monomials in a polynomial. We want to be able to discuss and use these different monomials and to do so we make the following definition.

Definition 3.1.2 *Let $f \in A = k[x_1, \ldots, x_n], f \neq 0$ and suppose $\prec$ is an admissible ordering of monomials in A. Then f can be uniquely written $f = c_1 m_1 + \cdots + c_N m_N$ with monomials $m_1 \succ m_2 \succ \cdots \succ m_N$ and $c_i \neq 0, i = 1, \ldots, N$. We define the **support** of f to be $supp(f) = \{m_i \mid i = 1, \ldots, N\}$.*
*We define the **leading monomial** of f to be $lm(f) = m_1$, the **leading term** of f to be $lt(f) = c_1 m_1$ and the **leading coefficient** of f to be $lc(f) = c_1$.*

Example 3.1.4 *Let $f = 7x_1^3 x_3 + x_1 x_2^2 - 2x_3$ with the lexicographical ordering we have $supp(f) = \{x_1^3 x_3, x_1 x_2^2, x_3\}$, $lm(f) = x_1^3 x_3$, $lt(f) = 7x_1^3 x_3$, and $lc(f) = 7$.*

Chapter 4

Monomial ideal

4.1 Initial Definitions

One of the basic criteria for an algorithm is that it will in a finite number of steps get you to the desired destination. One of the keystones in making this likely for Buchberger's algorithm is the fact that monomial ideals in a polynomial ring over a field is finitly generated. This is shown in Dickson's lemma.

Definition 4.1.1 *An ideal generated by a set of monomials, elements in* $k[x_1, \ldots, x_n]$ *of the form* $x_1^{i_1} \cdots x_n^{i_n}$*, is called a* ***Monomial Ideal****.*

Theorem 4.1.1 *Let* $\mathfrak{a}$ *be a monomial ideal in* $k[x_1, \ldots, x_n]$*.*
Let $f = \Sigma c_i m_i$*, were* $c_i \in k \setminus \{0\}$ *and* m_i *are different monomials. If* $f \in \mathfrak{a}$ *then* $m_i \in \mathfrak{a}$ *for each* i

Proof We start with defining the concept of **multigrading** of the polynomial ring $k[x_1, \ldots, x_n]$. If $cm = cx_1^{i_1} \cdots x_n^{i_n}, c \in k \setminus \{0\}$, we set $mdeg(cm) = (i_1, \ldots, i_n)$. Let $\mathfrak{a} = \langle n_1, \ldots, n_s \rangle$ be a monomial ideal, and suppose $f = \Sigma c_i m_i \in \mathfrak{a}$. Then $f = g_1 n_1 + \cdots + g_s n_s$ for some $g_i = \Sigma c_i m_i \in k[x_1, \ldots, x_n]$. Let $c_i m_i$ be a nonzero term in f. Then $c_i m_i$ equals the sum if all elements $c_{i,j} m_{i,j} n_i$ which are of the same multidegree as $c_i m_i$. Hence $c_i m_i$ is a linear combination of the $n_i's$, so $c_i m_i \in \mathfrak{a}$.

Definition 4.1.2 *If* $\mathfrak{a}$ *is a nonzero ideal in A, then we define the* ***ideal of leading monomials*** *of* $\mathfrak{a}$ *to be* $l(\mathfrak{a}) = \langle lm(f) : f \in \mathfrak{a} \rangle = \langle lt(f) : f \in \mathfrak{a} \rangle$*.*

4.2 Dickson's Lemma

Lemma 4.2.1 *(Dickson's Lemma) Every monomial ideal in* $k[x_1, \ldots, x_n]$*, a polynomial ring over a field* k*, is finitely generated.*

Proof By induction over n. Since every ideal in $k[x]$ is principal, the lemma is true for $n = 1$. Suppose it is true for $n-1$ variabels, and let $\mathfrak{a}$ be a monomial ideal in $k[x_1, \ldots, x_n]$. Let $\mathfrak{b}_j = (\mathfrak{a} : \langle x_n^j \rangle) \cap k[x_1, \ldots, x_{n-1}] = \langle S_j \rangle$. Since $\mathfrak{b}_j$ is an ideal in $k[x_1, \ldots, x_{n-1}]$, we can choose S_j to be finite. We have $\mathfrak{b}_0 \subseteq \mathfrak{b}_1 \subseteq \cdots$. It follows that $\cup \mathfrak{b}_j$ is an ideal $\mathfrak{b}$ in $k[x_1 \ldots, x_{n-1}]$ and hence finitely generated, $\mathfrak{b} = \langle S \rangle$. If $m \in \mathfrak{a}$ is a monomial then $m = m' x_n^k$ for some monomial $m' \in k[x_1, \ldots, x_{n-1}]$ and some k. Since $m' x_n^k \in \mathfrak{a}$ we get $m' \in \mathfrak{a} : \langle x_n^k \rangle$, so $m \in \langle x_n^k S_k \rangle$. Thus $S' = S_0 \cup x_n S_1 \cup x_n^2 S_2 \cup \cdots$ is a generating set for $\mathfrak{a}$. But for some r we have that $S_k = S_r$ if $k \geq r$, so $S_0 \cup x_n S_1 \cup \cdots \cup x_n^r S_r$ is a finite generating set for $\mathfrak{a}$.

There is an additional, famous result, by the German mathematician David Hilbert, called Hilbert's Basis Theorem. It shows that every ideal in a polynomial ring over a field is finitly generated, but since we only use the monomial ideals we have chosen just to present Dickson's lemma.

Lemma 4.2.2 *Let $\prec$ be an admissible ordering on the monomials in $k[x_1, \ldots, x_n]$. Then any nonempty set S of monomials has a smallest element, in other words there is an $m_0 \in S$ such that $m_0 \prec n$ for any $n \in S, n \neq m_0$.*

Proof Let $\mathfrak{a} = \langle S \rangle$ be the ideal generated by S. By Dickson's Lemma, $\mathfrak{a}$ is finitely generated, $\mathfrak{a} = \langle m_1, \ldots, m_r \rangle$. Since any monomial m in S is a multiple of some $m_i, m = m_i m'$ for some i and som m', we can choose m_0 to be the smallest monomial in $\{m_1, \ldots, m_r\}$ since any multiple of m_i is larger than m_i.

We prefer to use a reformulation of the lemma above and to make referring easy we formulate this in a separate lemma.

Lemma 4.2.3 *Any strictly decreasing sequence of monomials in an admissible ordering $\succ$ is finite.*

Chapter 5

Reduction

We will now get familiar with the reduction process, which we will later use to calculate reduced Gröbner bases. The reduction process works in the same way as the division algorithm for polynomials in $k[x]$. So we will begin with extending the already known division algorithm for $k[x]$ to $k[x_1, ..., x_n]$ and then at the end of the chapter take a closer look on reduction. Our goal in this chapther is to come to a point where we are able to express a polynomial f modulo an ideal $\mathfrak{a} = \langle g_1, \ldots, g_2 \rangle$

For a division algorithm over in $k[x]$ we have the following theorem.

Theorem 5.0.1 *Let k be any field and suppose $f, g \in k[x], g \neq 0$. Then there are uniquely defined polynomials $q, r \in k[x]$ such that $f = qg + r$ with $deg(r) < deg(g)$*

Note that the last part, $deg(r) < deg(g)$ is a way to express that r is "smaller" than g. In one variable we use the degree of the polynomial for comparison, but when we move on to polynomials in several variables we have to make this comparison in some other way.

Example 5.0.1 *$f = x^3 + 2x + 1$ and $g = x + 2$*

$$x^3 + 2x + 1 = x^2(x + 2) + (-2x^2 + 2x + 1)$$
$$x^3 + 2x + 1 = x^2(x + 2) + (-2x)(x + 2) + (6x + 1)$$
$$x^3 + 2x + 1 = x^2(x + 2) + (-2x)(x + 2) + 6(x + 2) + (-11)$$
$$x^3 + 2x + 1 = (x^2 - 2x + 6)(x + 2) + (-11)$$

$\Rightarrow q = x^2 - 2x + 6$, $r = -11$, $f = qg + r$, *where* $deg(-11) < deg(x + 2)$

When we extend the algorithm from $k[x]$ to $k[x_1, \ldots, x_n]$ we will use the monomial orderings introduced in chapter 3 to handle the problem of several variables. Then we will see what to do when g is a sequence of polynomials $g = (g_1, \ldots, g_s)$.

5.1 Division algorithm in $k[x_1, \ldots, x_n]$

First we will make an informal description of the algorithm and then go through it more thoroughly. We want to be able to express a polynomial f as $qg + rem$ where f, g, q, rem are polynomials in $k[x_1, \ldots, x_n]$ and where rem stands for the *remainder* of f with respect to g. So how will we define this remainder? If $f = 0$ we let the remainder of f be 0. Otherwise we look at the monomials in f which are divisible by the leading monomial in g. As an example if we use the Lex order defined in chapter 3 and $f = 2x^2 + x + 3y^2$ and $g = x + y$, the leading monomial of g, $lm(g) = x$ and the monomials if f which are divisible by $lm(g)$ are $\{x^2, x\}$ we call this set S_f. Now let $f_1 = f - \frac{2x^2}{x}(x + y) = 2x^2 + x + 3y^2 - (2x^2 + 2xy) = -2xy + x + 3y^2$. We choose to work with the term $2x^2$ since x^2 is the largest monomial in S_f. In the next step we look at the monomials in f_1 which are divisible by $lm(g)$, $S_{f_1} = \{xy, x\}$. And here comes a crucial part of the algorithm, we claim that the largest monomial in S_{f_1} is smaller then the largest monomial in S_f and next that the largest monomial in S_{f_2} will be smaller than the largest monomial in S_{f_1} and so on. To make it clearer we call these "largest" monomials in S_n, p_n then our claim is that $p_0 \succ p_1 \succ p_2 \succ \ldots$. This is a decreasing sequence under an admissible order and thereby we know from Lemma 4.2.3 that the sequence is finite, in other words, eventually no monomial in f_N will be divisible by $lm(g)$. This f_N we call the *remainder* of f with respect to g. The demand that no monomial in f_N is divisible by $lm(g)$ correspond to $deg(r) < deg(g)$ in the one variable case. For our $f = 2x^2 + x + 3y^2$ and $g = x + y$ we have

$$f_1 = -2xy + x + 3y^2, S_{f_1} = \{xy, x\}$$

which gives

$$f_2 = f_1 - \frac{-2xy}{x}(x + y) = -2xy + x + 3y^2 - (-2xy - 2y^2) = x + 5y^2, S_{f_2} = \{x\}$$

which gives

$$f_3 = f_2 - \frac{x}{x}(x + y) = x + 5y^2 - (x + y) = 5y^2 - y$$

Now no monomial in f_3 is divisible by $lm(g) = x$ and we have come to an end of the algorithm.

$$5y^2 - y \textit{ is the remainder of } 2x^2 + x + 3y^2 \textit{ with respect to } x + y$$

At this piont you might ask yourself if the the *remiander* depends on the monomial ordering. This is not the case, though when we move on to the case where we have a sequence $(g_1, \ldots, g_k)$ we will see that the *reminder* will depend on the order of the sequence. But First we will go through the theory of when g equals a single polynomial in a more formal way. We have

$$f, g \in k[x_1, \ldots x_n], \textit{and } \prec \textit{ an admissible monomial ordering.}$$

If $f = 0$ we let the *remainder* of f to be 0.
Otherwise we let

$$m = lm(g),\ S_f = \{n \in supp(f) \mid m\ divides\ n\}$$

Let p_0 be the largest element in S_f and c_{p_0} be the $p_0 - coefficient\ in\ f$

Then we let

$$f_1 = f - \frac{c_{p_0} p_0}{lc(g)m}\ g$$

And

$$S_{f_1} = \{n \in supp(f_1) \mid m\ divides\ n\}$$

If p_1 is the largest element in S_{f_1} then $p_1 \prec p_0$ since

$$supp(f_1) \subseteq (supp(f) \cup supp(\frac{p_0}{m}\ g) \setminus \{p_0\})$$

If $p_1 \in supp(f) \setminus \{p_0\}$ then obviously $p_1 \prec p_0$.
We have

$$lm(\frac{p_0}{m}\ g) = \frac{p_0}{m}\ lm(g) = \frac{p_0}{m}\ m = p_0$$

Hence we also get $p_1 \prec p_0$ if $p_1 \in supp(\frac{p_0}{m}\ g) \setminus \{p_0\}$.
We continue the process and define

$$f_2 = f_1 - \frac{c_{p_1} p_1}{lc(g)m}\ g\ , S_{f_2} = \{n \in supp(f_2) \mid m\ divides\ n\}\ and\ p_2 = max(S_{f_2})$$

The sequence $p_0 \succ p_1 \succ p_2 \succ \dots$ is finite according to lemma 4.2.3, hence after a finite number of steps no element in $supp(f_N)$ is divisible by m. We have $f_n = f - hg$ for some polynomial h, and we define f_N to be the *remainder* of f with respect to g.

Example 5.1.1 *$f = 5x_1^2 + x_1x_2^2 + x_1x_2 - x_2$, $g = (x_1 + x_2^2)$ and let $\prec$ be Lex Then we have $supp(f) = \{x_1^2, x_1x_2^2, x_1x_2, x_2\}$ and $m = x_1$ which gives $S_f = \{x_1^2, x_1x_2^2, x_1x_2\}$, $p_0 = x_1^2$ and $c_{p_0} = 5$.*

$f_1 = 5x_1^2 + x_1x_2^2 + x_1x_2 - x_2 - (\frac{5x_1^2}{x_1}(x_1 + x_2^2)) = 5x_1^2 + x_1x_2^2 + x_1x_2 - x_2 - 5x_1^2 - 5x_1x_2^2 = -4x_1x_2^2 + x_1x_2 - x_2$

$$S_{f_1} = \{x_1x_2^2, x_1x_2\},\ p_1 = x_1x_2^2,\ c_{p_1} = -4$$

$f_2 = -4x_1x_2^2 + x_1x_2 - x_2 - (\frac{-4x_1x_2^2}{x_1}(x_1x_2)) = -4x_1x_2^2 + x_1x_2 - x_2 + 4x_1x_2^2 + 4x_2^3 = x_1x_2 + 4x_2^3 - x_2$

$$S_{f_2} = \{x_1x_2\},\ p_2 = x_1x_2,\ c_{p_2} = 1$$

$f_3 = x_1x_2 + 4x_2^3 - x_2 - (\frac{x_1x_2}{x_1}(x_1 + x_2^2)) = x_1x_2 + 4x_2^3 - x_2 - x_1x_2 - x_2^3 = 3x_2^3 - x_2$
$f_3 = 3x_2^3 - x_2$ is the remainder of f with respect to g

Now let $g = (g_1, \ldots, g_s)$ be an ordered sequence of nonzero polynomials and f a polynomial.
We recursively define

$$rem(f, (g_1, \ldots, g_s)) = rem(f - ng_k, (g_1, \ldots, g_s))$$

where k is the smallest index such that $lm(g_k)$ divides $lm(f)$ and n is a term chosen so that $lt(f) = lt(ng_k)$. If no $lm(g_i)$ divides $lm(f)$
we define

$$rem(f, (g_1, \ldots, g_s)) = lt(f) + rem(f - lt(f), (g_1, \ldots, g_s))$$

In both cases the process reduce f with the leading monomial and thereby it is finite.

Example 5.1.2 *If we have*

$$f = x^3 + y, g = (x^2 - 1, y - 1) \text{ and the } Lex - ordering$$

Then

$$rem(f, g) = rem(x^3 + y - x(x^2 - 1), (x^2 - 1, y - 1)) =$$
$$= rem(x + y, (x^2 - 1, y - 1))$$

Now no $lm(g_i)$ divides $lm(f)$, so

$$rem(x^3+y, (x^2-1, y-1)) = rem(x+y, (x^2-1, y-1)) = x+rem(y, (x^2-1, y-1)) =$$

$$= x + rem(y - (y - 1), (x^2 - 1, y - 1)) = x + rem(1, (x^2 - 1, y - 1))$$

no $lm(g_i)$ divides 1 so

$$rem(x^3 + y, (x^2 - 1, y - 1)) = x + 1 + rem(0, (x^2 - 1, y - 1)) = x + 1 + 0 = x + 1$$

Thus $x + 1$ is the remainder of $x^3 + y$ with respect to $(x^2 - 1, y - 1)$.

5.2 Reduction

We have defined the remainder $rem(f)$ of a polynomial f when dividing with a sequence $(g_1, \ldots, g_k)$. Now let $\mathfrak{a}$ be an ideal, $\mathfrak{a} = \langle g_1, \ldots, g_k \rangle$ and note that the $rem(f, (g_1, \ldots, g_k)) \equiv f$ modulo $\mathfrak{a}$.

Example 5.2.1 *Given*

$$f = x^2 + x + y \in k[x_1, \ldots, x_n],\ \mathfrak{a} = \langle x^2 - x, y \rangle \text{ and } Lex - ordering$$

We want to write f modulo $\mathfrak{a}$ so we calculate the remainder of f with respect to $\langle g_1 = x^2 - x, g_2 = y \rangle$.

$$rem(f, (g_1, g_2) = rem(f - ng_1, (g_1, g_2))$$

let

$$f_1 = f - ng_k = x^2 + x + y - 1(x^2 - x) = 2x + y$$

Then we have $rem(f, (g_1, g_2) = rem(f_1, (g_1, g_2))$. *Now no leading monomial in* (g_1, g_2) *divides* $lm(f_1)$ *so the*

$$rem(f_1, (g_1, g_2)) = lt(f_1) + (f_1 - lt(f_1), (g_1, g_2))$$

$$f_2 = f_1 - lt(f_1) = 2x + y - 2x = y$$

$$rem(f_2, (g_1, g_2)) = rem(f_2 - ng_2, (g_1, g_2))$$

$f_3 = f_2 - ng_2 = y - 1y = 0$ *and now* $rem(f_3, (g_1, g_2)) = rem(0, (g_1, g_2)) = 0$

and we have come to the end. It's time to look at what we really have.
$rem(f, (g_1, g_2)) = rem(f_1, (g_1, g_2)) =$
$lt(f_1) + rem(f_2, (g_1, g_2)) = lt(f_1) + rem(f_3, (g_1, g_2)) = lt(f_1) + 0 = lt(f_1) = 2x$

$$2x \textit{ is the remiander of } f \textit{ with respect to } (g_1, g_2)$$

$$x^2 + x + y \equiv 2x \textit{ modulo } \mathfrak{a}$$

We could do the same thing in a slightly smoother way. We work in modulo $\mathfrak{a}$ *so the generators of* $\mathfrak{a}, g_1 \equiv \cdots \equiv g_n \equiv 0$ $mod(\mathfrak{a})$ *which in our example gives*

$$\begin{cases} g_1 = x^2 - x \equiv 0 \\ g_2 = y \equiv 0 \end{cases} \quad mod(\mathfrak{a})$$

in other words

$$\begin{cases} x^2 \equiv x \\ y \equiv 0 \end{cases} \quad mod(\mathfrak{a})$$

This can we use to directly reduce f. In our example $f = x^2 + x + y$ *and now we know that from* g_1 *that* $x^2 \equiv x$ $mod(\mathfrak{a})$ *and from* g_2 *that* $y \equiv 0$ $mod(\mathfrak{a})$ *so if we want to express* f $mod(\mathfrak{a})$ *we use that knowledge. First we use* g_1 *and get*

$$f = x^2 + x + y \equiv x + x + y \equiv 2x + y \ mod(\mathfrak{a})$$

then we use g_2 *and get*

$$f = 2x + y \ mod(\mathfrak{a}) \equiv 2x + 0 \equiv 2x \ mod(\mathfrak{a})$$

We call $2x$ for the reduction of $x^2 + x + y$ $modulo(x^2 - x, y)$ it is called reduction since the *remainder* of f usually is "smaller" than f. Note that reduction process works in exactly the same way as the division algorithm though it doesn't present the quotients.

One of the purpose of reduction is to get an unambiguous representation of polynomials in $k[x_1, \ldots, x_n]/\mathfrak{a}$, a *normal form*. The reduction process alone is not enough to give us that, as we will show below, though in the next chapter we will define Gröbner bases and with there aid we will eventually get a unique *normal form*.

Example 5.2.2 *If we want to reduce*

$$x^3y + x^2y^2 + y^2 \text{ modulo the ideal } \mathfrak{a} = (xy, y^2 - 2)$$

we can first use that $g_1 = xy \equiv 0 \ mod(\mathfrak{a})$ *then*

$$x^3y + x^2y^2 + y^2 \equiv x^2(0) + 0 + y^2 \equiv y^2 \text{ modulo } \mathfrak{a}$$

and then use g_2 *in which we have* $y^2 \equiv 2 \ mod(\mathfrak{a})$ *and get*

$$x^3y + x^2y^2 + y^2 \equiv y^2 \ mod(\mathfrak{a}) \equiv 2 \ mod(\mathfrak{a})$$

But we can also switch the order of the g_i *to* $(y^2 - 2, xy)$ *without effecting the ideal* $\mathfrak{a}$*. If we first use* $y^2 \equiv 2 \ mod(\mathfrak{a})$ *we get*

$$x^3y + x^2y^2 + y^2 \equiv x^3y + x^2(2) + (2) \equiv x^3y + 2x^2 + 2 \text{ modulo } \mathfrak{a}$$

and then use $xy \equiv 0 \ mod(\mathfrak{a})$ *and get*

$$x^3y + x^2y^2 + y^2 \equiv x^3y + 2x^2 + 2 \ mod(\mathfrak{a}) \equiv x^2(0) + 2x + 2 \equiv 2x + 2 \ mod(\mathfrak{a})$$

This means that $rem(f, (g_1, \ldots, g_n))$ *depend on the order of* $(g_1, \ldots, g_n)$ *and this is no good. So what will we do? We will of course try to fix it. We will try to find a better set of generators* $\{g_1, \ldots, g_n\}$ *to* $\mathfrak{a}$*, a Gröbner basis, and we will see that we get a remainder which only depends on the ideal* $\mathfrak{a}$ *and not on the generating set.*

Chapter 6

Gröbner bases

Gröbner bases are important since they make it possible to express every polynomial in $k[x_1, \ldots, x_n]$ in a uniqe normal form with respect to the ideal. To start with we will summarize some fact from the previous chapter in a lemma.

Lemma 6.0.1 *Let $f, g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$. Then $f - rem(f, (g_1, \ldots, g_s)) \in \langle g_1, \ldots, g_s \rangle$. In particular, if the $rem(f, (g_1, \ldots, g_s)) = 0$ then $f \in \langle g_1, \ldots, g_s \rangle$.*

Now it's time to answer the big question, what is a Gröbner basis?

Definition 6.0.1 *Let $\mathfrak{a}$ be an ideal in $k[x_1, \ldots, x_n]$. A set $\{g_1, \ldots, g_s\}$ of elements in $\mathfrak{a}$ such that $\langle lm(g_1), \ldots, lm(g_s) \rangle = l(\mathfrak{a})$ is called a **Gröbner basis** for $\mathfrak{a}$.*

Lemma 6.0.2 *If $\{g_1, \ldots, g_s\}$ is a Gröbner basis for $\mathfrak{a}$, then $\langle g_1, \ldots, g_s \rangle = \mathfrak{a}$*

Proof $\langle g_1, \ldots, g_s \rangle \subseteq \mathfrak{a}$ since $g_i \in \mathfrak{a}$ for all i. Let $f \in \mathfrak{a}$. Then $lm(f) \in \langle lm(g_1), \ldots, lm(g_s) \rangle$, hence $lm(f - ng_k) \prec lm(f)$ for some g_k and some term n. Since $f - ng_s \in \mathfrak{a}$, we get by recursiveness that $f \in \langle g_1, \ldots, g_s \rangle$.

6.1 Normal Forms

We will soon define what we mean with a normal form, but first we need some theory to support the definition.

Proposition 6.1.1 *Let $\{g_1, \ldots, g_s\}$ be a Gröbner basis for the ideal $\mathfrak{a} = \langle g_1, \ldots, g_s \rangle$. Then $rem(f_1, (g_1, \ldots, g_s)) = rem(f_2, (g_1, \ldots, g_s))$ if and only if $f_1 - f_2 \in \mathfrak{a}$. In particular $rem(f, (g_1, \ldots, g_s)) = 0$ if and only if $f \in \mathfrak{a}$.*

Proof Suppose $rem(f_1, G) = rem(f_2, G)$, where $G = (g_1, \ldots, g_s)$. Since $f_i - rem(f_i, G) \in \mathfrak{a}, i = 1, 2$,cf Lemma 6.0.1, we get $f_1 - rem(f_1, G) - (f_2 - rem(f_2, G)) = f_1 - f_2 \in \mathfrak{a}$. Now suppose $f_1 - f_2 \in \mathfrak{a}$. Then $rem(f_1, G) - rem(f_2, G) = (f_3 - rem(f_2, G)) - (f_1 - rem(f_1, G)) + (f_1 - f_2) \in \mathfrak{a}$ since $f_i - rem(f_i, G) \in \mathfrak{a}, i = 1, 2$. But $rem(f_1, G), i = 1, 2$ is a linear combination of monomials outside $l(\mathfrak{a})$. If $rem(f_1, G) \neq rem(f_2, G)$ we would have $lm(rem(f_1, G) - rem(f_2, G)) \notin \mathfrak{a}$. But $rem(f_1, G) - rem(f_2, G) \in \mathfrak{a}$ gives $lm(rem(f_1, G) - rem(f_2, G)) \in \mathfrak{a}$, a contradiction.

The $rem(f, G)$ is a linear combination of monomials outside $l(\mathfrak{a})$. We can use this $rem(f, G)$ to represent elements in $k[x_1, \ldots, x_n]/\mathfrak{a}$ since $f - rem(f, G) \in \mathfrak{a}$. We know that the monomials outside $l(\mathfrak{a})$ generate $k[x_1, \ldots, x_n]/\mathfrak{a}$ as a vector space over k and these monomials are linearly independent modulo $\mathfrak{a}$, since if $\lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_n m_n \in \mathfrak{a}$ one of these monomials must be the largest, say m_i which gives that m_i is the leading monomial in $\lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_n m_n \in \mathfrak{a}$ and thereby $m_i \in l(\mathfrak{a})$ a contradiction. Thus we have that the monomials outside $l(\mathfrak{a})$ constitute a k-basis of $k[x_1, \ldots, x_n]/\mathfrak{a}$ and we have found a way to uniquely represent polynomials in $k[x_1, \ldots, x_n]/\mathfrak{a}$. We are now ready to define the *normal form* of a polynomial f in $k[x_1, \ldots, x_n]/\mathfrak{a}$.

Theorem 6.1.1 *Let $f \in k[x_1, \ldots, x_n]$ and let $G = (g_1, \ldots, g_s)$ be a Gröbner basis for the ideal $\mathfrak{a}$. Given a fix monomial ordering we have a that the $rem(f, G)$ is uniquely defined and doesn't depend on the Gröbner bases, G, of $\mathfrak{a}$. We call $rem(f, G)$ for the **normal form** of f and denote it NF(f).*

6.2 Reduced Gröbner bases

Gröbner bases are not unique and since we want unique stuff, we introduce the concept of reduced Gröbner bases which are unique.

Definition 6.2.1 *We define **G** to be a **reduced Gröbner basis** if*

- *$\{lm(g_1), \ldots, lm(g_s)\}$ constitutes a minimal set of generators for $l(\mathfrak{a})$*
- *g_i are monic*
- *no $lm(g_i)$ divides any monomial in $supp(g_j), i \neq j$*

Proposition 6.2.1 *A reduced Gröbner basis exists and is unique.*

Proof Given a Gröbner basis, G you can construct a reduced Gröbner basis. You start with picking a subset $G' = \{g_{i_1}, \ldots, g_{i_k}\}$ of G so that the first condition in the definition is fulfilled. Then multiply each g_{i_t} with $lc(g_{i_t}^{-1})$ so we get monic elements. Last, take the remainder of each g_{i_t} with respect to $G' \setminus \{g_{i_t}\}$. Thus the reduced Gröbner basis exists. This reduced Gröbner basis is unique since if $\{g_1, \ldots, g_s\}$ and $\{h_1, \ldots, h_s\}$ are two reduced Gröbner bases for an ideal

$\mathfrak{a}$ with $lm(g_i) = lm(h_i)$ we get that $g_i - h_i \in \mathfrak{a}$. If $g_i - h_i \neq 0$ we would have $lm(g_i - h_i) \in lm(\mathfrak{a})$, but the leading terms in g_i and h_i are equal, hence cancel in, $g_i - h_i$. But $g_i - h_i$ is a linear combination of monomials outside $l(\mathfrak{a})$, which gives a contradiction.

The proof might be a little bit hard to follow, but there are two main points which we want to observe.

- A minimal set of monomial generators in an monomial ideal is unique.
- Every monomial in a monomial ideal is divisible by one of the generators.

Chapter 7

S-polynomials

7.1 Initial Definition

Starting with one generating set for an ideal you want to calculate a new generating set, a Gröbner basis, for the ideal. To do this we use the S-polynomial. The definition might look a bit complicated but it's not as hard as it lookes as you will see when we reflect back to the introductory example. First we need a definition.

Definition 7.1.1 *Let f and g be nonzero polynomials.*
Then h is a least common multiple of f and g, $lcm(f,g)$, if both f and g divide h and if any other polynomial which is a multiple of both f and g is a multiple of h.

Example 7.1.1 *Let $f = xy$ and $g = x^2$ then we have*
$lcm(f,g) = lcm(xy, x^2) = x^2y$

7.2 S-polynomial

Definition 7.2.1 *Let (f_i, f_j) be a fixed pair of monic elements in a set of generators of an ideal with an given ordering $\prec$. The **S-polynomial** of (f_i, f_j) in $\prec$ is*

$$S_{i,j} = S(f_i, f_j) = \frac{lcm(lm(f_i), lm(f_j))}{lm(f_i)} f_i - \frac{lcm(lm(f_i), lm(f_j))}{lm(f_j)} f_j$$

The S-polynomials are used in the construction of and as a criterion for Gröbner bases. Say that we have an ideal generated by $\mathbf{a} = \langle f_1, \ldots, f_k \rangle$ to this set we calculate the reduced S-polynomials $S(f_i, f_j)$ were $i, j = 1, \ldots, k$. If $S_{i,j} \neq 0$ we are to extend the generating set $(f_1, \ldots, f_k)$ with the
$rem(S_{i,j}, (f_1, \ldots, f_k))$ and calculate all new S-polynomials and so on. If we add an S-polynomial f_{k+1} to the generators $(f_1, ..., f_{k,})$ then
$lm(f_{k+1}) \notin (lm(f_1), ..., lm(f_k))$. Since the monomial ideal $l(f_1, ..., f_k)$ is finitely

generated, we reach it after a finite number of steps, so eventually all S-polynomials reduce to 0 and this gives us the Gröbner bases, $\{f_1, \ldots, f_n\}$. Thus we have the criterion for Gröbner basis formulated in the theorem after the example.

Example 7.2.1 *If we recall the Introductory Example in chapter 2*

$$\begin{cases} f_1 = x^2y + x \\ f_2 = x^2 - y^2 \end{cases}$$

and want to calculate the S-polynomial of f_1 and f_2, $S(f_1, f_2)$, we have

$$\frac{lcm(lm(f_1), lm(f_2))}{lm(f_1)} = \frac{lcm(x^2y, x^2)}{x^2y} = 1$$

and

$$\frac{lcm(lm(f_1), lm(f_2))}{lm(f_2)} = \frac{lcm(x^2y, x^2)}{x^2} = y$$

So when we calculate the S-polynomial, $S(f_1, f_2)$ we get
$S(f_1, f_2) = f_3 = \frac{lcm(lm(f_1), lm(f_2))}{lm(f_1)} f_1 - \frac{lcm(lm(f_1), lm(f_2))}{lm(f_2)} f_2 = f_1 - yf_2 = (x^2y + x) - y(x^2 - y^2) = x^2y + x - x^2y + y^3 = x + y^3$

Theorem 7.2.1 *Let $(f_1, \ldots, f_k)$ be a sequence of monic elements in $k[x_1, \ldots, x_n]$ and let $S_{i,j} = S(f_i, f_j)$ be the S-polynomials. Then $\{f_1, \ldots, f_k\}$ is a Gröbner basis of $\langle f_1, \ldots, f_k \rangle$ if and only if $rem(S_{i,j}, (f_1, \ldots, f_k)) = 0$ for all i, j.*

The proof of the theorem is rather tricky and technical so we have chosen to exclude it here, but we warmly recommend futher reading in "An Introduction to Gröbner bases" by Fröberg.

Chapter 8

Buchberger's algorithm

8.1 Buchberger's algoritm for calculating Gröbner bases

If we start with an ideal

$$\mathfrak{a} = \langle f_1, \ldots, f_k \rangle$$

Calculate all S-polynomials, S_{f_i,f_j} and reduce them with respect to $(f_1, \ldots, f_k)$, we denote the reduced S-polynomial with $\overline{S}_{i,j}$. If $\overline{S}_{i,j} = 0$ we move on and calculate the next S-polynomial. If $\overline{S}_{i,j} \neq 0$, we extend $(f_1, \ldots, f_n)$ with $\overline{S}_{i,j}$ and get $(f_1, \ldots, f_k, f_{k+1})$. This will not change the ideal since the S-polynomial already lies in the ideal and we stay within the ideal while we reduce. Then we start over and calculate all new S-polynomials, $S_{i,k+1},\ i = 1, \ldots, k$, and reduce them. Continue until all S-polynomials reduce to zero.
If the $\overline{S}_{i,j} \neq 0$ we have $lm(\overline{S}_{i,j}, (f_1, \ldots, f_n)) \notin \langle lm(f_1), \ldots, lm(f_n) \rangle$ so each time we extend the generating set, we also extend the monomial ideal generated by the leading monomials of the generators. Since we know that the monomial ideal is finitely generated, by Dickson's Lemma, all S-polynomials will eventually be reduced to zero. Thus the final result will be a Gröbner basis, by Theorem 7.2.1.

Example 8.1.1 *Calculate a Gröbner basis for the ideal* $\mathfrak{a}$ *using Lex.*

$$\mathfrak{a} = \langle x_1^2 + x_2, x_1x_2 - x_2^2 \rangle$$

$$\begin{cases} f_1 = x_1^2 + x_2 \\ f_2 = x_1x_2 - x_2^2 \end{cases}$$

$S(f_1, f_2) = \frac{x_1^2x_2}{x_1^2}(x_1^2 + x_2) - \frac{x_1^2x_2}{x_1x_2}(x_1x_2 - x_2^2) = x_1^2x_2 + x_2^2 - x_1^2x_2 + x_1x_2^2 = x_2^2 + x_1x_2^2$

Then we reduce $S(f_1, f_2)$ *and use that* $f_2 = x_1x_2 - x_2^2 \equiv 0 \ mod(\mathfrak{a}) \Rightarrow x_1x_2 \equiv x^2 \ mod(\mathfrak{a})$

$$S(f_1, f_2) = x_1x_2^2 + x_2^2 \equiv x_2^2x_2 + x_2^2 \equiv x_2^3 + x_2^2 \ mod(\mathfrak{a})$$

$$\overline{S}(f_1, f_2) = x_2^3 + x_2^2$$

$$\begin{cases} f_1 = x_1^2 + x_2 \\ f_2 = x_1x_2 - x_2^2 \\ f_3 = x_2^3 + x_2^2 \end{cases}$$

$S(f_1, f_3) = \frac{x_1^2x_2^3}{x_1^2}(x_1^2+x_2)-\frac{x_1^2x_2^3}{x_2^3}(x_2^3+x_2^2) = x_1^2x_2^3+x_2^4-x_1^2x_2^3-x_1^2x_2^2 = x_2^4-x_1^2x_2^2$
We reduce with the aid of f_1 *and* f_3*we get*

$$S(f_1, f_3) = x_2^4 - x_1^2x_2^2 \equiv x_2^4 + x_2^3 \equiv -x_2^3 + x_2^3 \equiv 0 \ mod(\mathfrak{a})$$

$$\overline{S}(f_1, f_3) = 0$$

$S(f_2, f_3) = \frac{x_1x_2^3}{x_1x_2}(x_1x_2 - x_2^2) - \frac{x_1x_2^3}{x_2^3}(x_2^3 + x_2^2) = x_1x_2^3 - x_2^4 - x_1x_2^3 - x_1x_2^2 = -x_2^4 - x_1x_2^2$
we reduce with the aid of f_2 *and* f_3 *and get*

$$S(f_2, f_3) = -x_2^4 - x_1x_2^2 \equiv -x_2^4 - x_2^3 \equiv -x_2(-x_2^2) - x_2^3 \equiv x_2^3 - x_2^3 \equiv 0 \ mod(\mathfrak{a})$$

$$\overline{S}(f_2, f_3) = 0$$

And thereby all the S-polynomials are reduced to zero and the criterion for a Gröbner basis is fulfilled. $\langle x_1^2 + x_2, x_1x_2 - x_2^2, x_2^3 + x_2^2\rangle$ *is a Gröbner basis for the ideal* $\mathfrak{a}$

Chapter 9

Applications

In this chapter we will look at two applications of Gröbner bases. We will use the software maple12 to do the calculation which is not suitable to do by hand and plots. The maple-code is available in the appendix.

9.1 To solve systems of polynomial equations

First we will note that if we have a homogeneous system of polynomial equations, the polynomials in the system will generate an ideal. The solutions to the system are exactly the zeros to all the polynomials in the ideal.

Theorem 9.1.1 *If $f_1 = \cdots = f_k = 0$ has a finite number of solutions then the number of solutions, counted with multiplicity equals*

$$dim_C \frac{C[x_1, \ldots, x_n]}{l(\mathfrak{a})}$$

We will use the theorem in our applications, but we have chosen not to prove it here.

Since the monomials outside $l(\mathfrak{a})$ constitutes a base for the factor ring then, if the system has a finite number of solutions, there is for every variable x_i an element $x_i^{a_i}$ for some positive a_i otherwise there would be infinitely many x_i^n outside $l(\mathfrak{a})$. If we use the Lex order then there will be a $x_n^{a_n}$ in $l(\mathfrak{a})$. In other words there is a Gröbner basis element with $x_n^{a_n}$ as leading monomial, but the only monomials that are smaller than $x_n^{a_n}$ is lower order of x_n which gives an equation in only one variable. This equation we have to solve in some good way, then we can substitute the solutions in to the system of equations and get a system of equations with $n-1$ unknown variables. For the same reasons as above we will have an equation which only depends on the variable x_{n-1} and so on. In the end we have solved all equations in the system. As an example we can look at the Gröbner basis in the introductory exampel, $\{x+y^3, y^6-y^2\}$ were we solve the equation $y^6 - y^2$, then substitute y in the second equation

$x+y^3$ and get an equation which only depends on x. When we have solved that equation we have solved the whole system of equations.

Example 9.1.1 *We want to solve the system:*

$$\begin{cases} x^3+xy+y^2-z^2=0 \\ x^2-xz+y+2z-2=0 \\ x^4+xyz+yz+z^2-2=0 \\ x^2-y-2z+1=0 \end{cases}$$

we use maple to calculate the Gröbner basis $\mathfrak{G}$

$$\mathfrak{G}=[z-1,y,x-1]$$

which gives

$$\begin{cases} z-1=0 \\ y=0 \\ x-1=0 \end{cases} \quad \Rightarrow \quad \begin{cases} z=1 \\ y=0 \\ x=1 \end{cases}$$

Example 9.1.2 *We want to decide maximum and minimum of* $f=x^3+2xyz-z^2$ *under the condition* $g=x^2+y^2+z^2=1$. *We use Lagrange multipliers and then solve the system with the aid of Gröbner basis. Lagrange's multipliers give*

$$\begin{cases} \frac{\partial f}{\partial x}=\lambda\frac{\partial g}{\partial x} \\ \frac{\partial f}{\partial y}=\lambda\frac{\partial g}{\partial y} \\ \frac{\partial f}{\partial z}=\lambda\frac{\partial g}{\partial z} \\ g=1 \end{cases} \Rightarrow \begin{cases} 3x^2+2yz-2\lambda x=0 \\ 2xz-2\lambda y=0 \\ 2xy-2z-2\lambda z=0 \\ x^2+y^2+z^2-1=0 \end{cases}$$

We calculate the Gröbner basis $\mathfrak{G}$ *using the lex order with* $\lambda \prec z \prec y \prec x$ *to get an equation which only depends on* x
$\mathfrak{G}=-6x^2-25x^3-18x^4+25x^5+24x^6, 6xy+25yx^2+24yx^3, 51x^2+72x^3-51x^4-72x^5+10y^2x, 14x^2-5y^2+18x^3-14x^4-18x^5+5y^4, 6xy+11yx^2+2y-2y^3+2xz, 51x^2+67x^3-51x^4-72x^5+5x+5yz, x^2+y^2+z^2-1, -88x^2-10y^2+10-159x^3+78x^4+144x^5+10\lambda$

$$\begin{cases} -6x^2-25x^3-18x^4+25x^5+24x^6=0 \\ 6xy+25yx^2+24yx^3=0 \\ 51x^2+72x^3-51x^4-72x^5+10y^2x=0 \\ 14x^2-5y^2+18x^3-14x^4-18x^5+5y^4=0 \\ 6xy+11yx^2+2y-2y^3+2xz=0 \\ 51x^2+67x^3-51x^4-72x^5+5x+5yz=0 \\ x^2+y^2+z^2-1=0 \\ -88x^2-10y^2+10-159x^3+78x^4+144x^5+10\lambda=0 \end{cases}$$

$$\begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \\ x_5 = -\frac{3}{8} \\ x_6 = -\frac{3}{8} \\ x_7 = -\frac{2}{3} \\ x_8 = -\frac{2}{3} \\ x_9 = 1 \\ x_{10} = -1 \end{cases} \Rightarrow \begin{cases} y_1 = 0 \\ y_2 = 0 \\ y_3 = 1 \\ y_4 = -1 \\ y_5 = \frac{3}{16}\sqrt{22} \\ y_6 = -\frac{3}{8}\sqrt{22} \\ y_7 = \frac{1}{3} \\ y_8 = -\frac{1}{3} \\ y_9 = 0 \\ y_{10} = 0 \end{cases} \Rightarrow \begin{cases} z_1 = 1 \\ z_2 = -1 \\ z_3 = 0 \\ z_4 = 0 \\ z_5 = -\frac{1}{16}\sqrt{22} \\ z_6 = \frac{1}{16}\sqrt{22} \\ z_7 = \frac{2}{3} \\ z_8 = -\frac{2}{3} \\ z_9 = 0 \\ z_{10} = 0 \end{cases}$$

and now it is easy to decide maximum and minimum for f under the condtition g=1

$$maximum = 1, minimum = -\frac{28}{27}$$

Some times it is enough to calculate the number of solutions of a system. This can also be done with the aid of Gröbner bases.

Example 9.1.3 *Determine the number of solutions to*

$$\begin{cases} xy - 1 = 0 \\ yz - x = 0 \\ z^2 - y = 0 \end{cases}$$

We calculate the Gröbner basis with the Degrevlex order

$\mathfrak{G} = [z^2 - y - 1, yz - x, y^2 - xz + y, xy - 1, x^2 - z]$ *and* $l(\mathfrak{a}) = [z^2, yz, y^2, xy, x^2]$

which gives that the set of monomials outside $l(\mathfrak{a})$ *is* $\{1, x, y, z, xz, yz, x, y, z\}$

$$dim_{\boldsymbol{C}} \frac{\boldsymbol{C}[x, y, z]}{l(\mathfrak{a})} = 7$$

The system has 7 solution counted with multiplicity.

Example 9.1.4 *Calculate the number of solutions to the following system:*

$$\begin{cases} a + b + c + d + e = 0 \\ ab + bc + cd + de + ea = 0 \\ abc + bcd + cde + dea + eab = 0 \\ abcd + bcde + cdea + deab + eabc = 0 \\ abcde - 1 = 0 \end{cases}$$

We calculate the Gröbner basis, $\mathfrak{G}$ *with the lex-ordering.*
$\mathfrak{G} = [-1 - 122e^5 + 122e^{10} + e^{15}, -55d^2 + 987e^2 - 979e^7 + 233de - 231de^6 - 8e^{12} - 2de^{11} + 55d^2e^5, 128103e^2 - 127116e^7 + 48787de - 48554de^6 - 55d^2 - 1042e^{12} - 398de^{11} + 55d^5e^2 + 165d^6e + 55d^7, -55c - 144e + 143e^6 + e^{11} + 55ce^5, -275ec + 136674e^2 - 136763e^7 + 53913de - 53911de^6 + 275d^2 - 1121e^{12} - 442de^{11} - 275d^3e^4 + 1210d^5e^2 + 440d^6e + 275cd, 69307e^3 + 28018de^2 + 550d^2e - 550ce^2 - 69289e^8 - 568e^{13} - 28336de^7 -$

$232de^{12}+550d^5e^3+275d^6e^2-550d^4e^4+550c^2e+275c^3, -144e+143e^6+e^{11}-55b+55be^5, -42124e^2+42218e^7-15106de+15092de^6+346e^{12}+124de^{11}+275d^3e^4-440d^5e^2-110d^6e-275d^4e^3-275eb+275bd, 550ec-105873e^2+105776e^7-40726de+40722de^6-550d^2+867e^{12}+334de^{11}+275d^3e^4-1045d^5e^2-330d^6e+275c^2-275d^4e^3-275eb+275bc, 179073e^2-178981e^7+69019de-69003de^6+275d^2-1467e^{12}-566de^{11}-550d^3e^4+1650d^5e^2+550d^6e+275d^4e^3+825eb+275b^2, a+b+c+d+e]$ *we get*

$$l(\mathfrak{a}) = \{e^{15}, d^2e^5, d^7, e^5c, cd, c^3, e^5b, bd, bc, b^2, a\}$$

And get the number of solutions to 70

9.2 Implicitization

We want to rewrite a function on parametric form to implicit form. This is a form of elimination since we eliminate the parameters and get an equation with the variables we are interested in. We will make an informal description of what happens. Suppose that we have

$$f = \begin{cases} x_1 = h_1(t_1, \ldots, t_m) \\ \quad \vdots \\ x_n = h_n(t_1, \ldots, t_m) \end{cases}$$

and we want to find the polynomial equations in the x_i which define f. We now look at the equations

$$\begin{aligned} x_1 - h_1(t_1, \ldots, t_m) &= 0 \\ &\vdots \\ x_n - h_n(t_1, \ldots, t_m) &= 0 \end{aligned}$$

and the idea is to eliminate the variables $t_1, \ldots, t_m$ from these equations. We calculate the Gröbner basis with the lex order and let $t_1 \succ \cdots \succ t_m \succ x_1 \succ \cdots \succ x_n$ which will give us a Gröbner basis which contains polynomials that only involve $x_1, \ldots, x_n$ since $t_1, \ldots, t_m$ will be eliminated first. The equations when the polynomials that only involve $x_1, \ldots, x_n$ equal zero will be the implicit form of the function f.

Example 9.2.1 *We want to write f on implicit form*

$$f(t) = \begin{cases} x = \frac{t}{1+t} \\ y = 1 - \frac{1}{t^2} \end{cases}$$

We calculate the Gröbner basis of using a special elimination ordering in which you divide the parameters you want to eliminate and the variables you want to keep in two blocks. The order uses the lex−ordering between the blocks, in other words $t_1 \succ \ldots, \succ t_m \succ x_1 \succ \cdots \succ x_n$ and the degrevlex − ordering within the blocks. In this example we want to eliminate t so we use $lexdeg([t],[x,y])$ and get the following Gröbner basis:

$$\mathfrak{G} = [1 - 2x + yx^2, -yx + 1 + yt - t, x + xt - t]$$

In the Gröbner basis above we have one polynomial which only depends on x, y as a consequence of the $lexdeg-ordering$ and the equation we get when we let this polynomial equal zero is in fact the implicit form of the function.

$$f(x,y) = 1 - 2x + yx^2 = 0$$

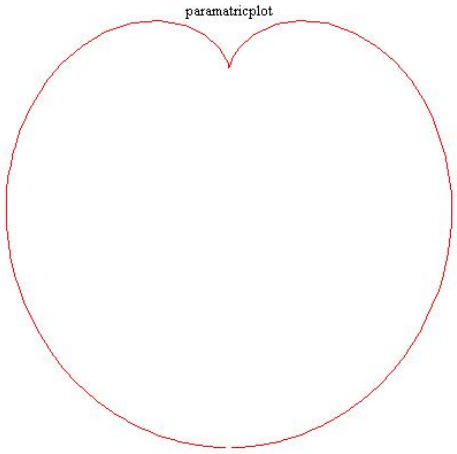
Example 9.2.2

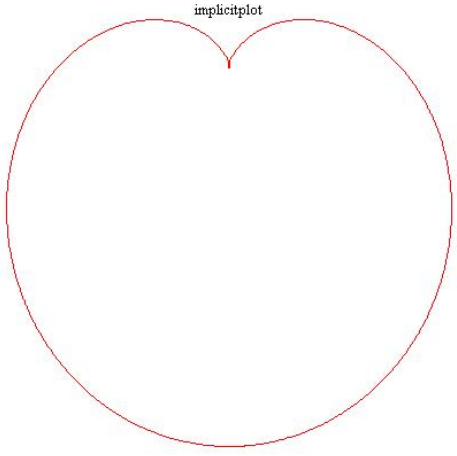
$$f(t) = \begin{cases} x = \frac{-1024t^3}{256t^4+32t^2+1} \\ y = \frac{-2048t^4+128t^2}{256t^4+32t^2+1} \end{cases}$$

We calculate the Gröbner basis, $\mathfrak{G} = [-16x^2 + 8yx^2 + 8y^3 + x^4 + 2y^2x^2 + y^4, y^2 + x^2 + 16xt, 16x + 16y^2t + 128yt - y^2x - x^3, -2y - y^2 - x^2 + 256t^2 + 32yt^2]$ *and*

$$f(x,y) = -16x^2 + 8yx^2 + 8y^3 + x^4 + 2y^2x^2 + y^4$$

For fun we have also plotted the curve.


paramatricplot


implicitplot

Example 9.2.3 *We want the implicit form of f where*

$$f(t) = \begin{cases} x = t^8 \\ y = t^{12} + t^{14} + t^{15} \end{cases}$$

We calculate the Gröbner basis which we find is to large to present here, but we single out the polynomial which only depend on x, y and get

$f(x,y) = 4y^2x^9 - 21x^{14} + 24y^3x^9 + 20y^2x^{11} + 26y^4x^7 - 16yx^{12} + 8y^5x^5 - 6y^4x^6 - 6x^{13} + 8yx^1 1 - 16y^3x^8 + 4x^3y^6 - 36x^{10}y^2 + x^{15} - y^8 + 8x^{13}y - x^{12}$ *As you can imagine this implicitization problem would be hard to solve without the aid of computers and Gröbner bases.*

Example 9.2.4 *We can also solve implicitization problem where we start with a surface on parametric form.*

$$f(u,v) = \begin{cases} x = uv - 1 \\ y = u^2 - v^2 \\ z = u^2 \end{cases}$$

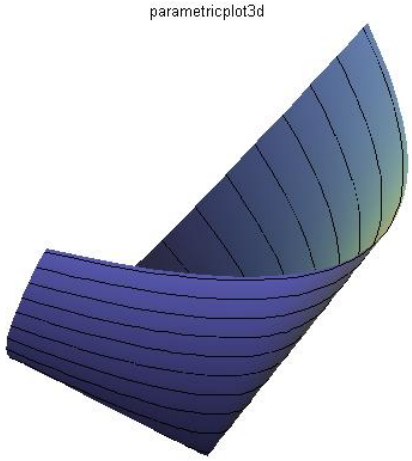
We calculate the Gröbner basis

$\mathfrak{G} = [x^2+1+yz-z^2+2x, xv+yu-zu+v, -zv+xu+u, v^2+y-z, -x+uv-1, -z+u^2]$

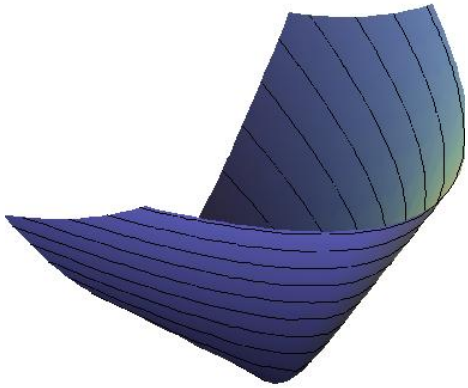
and get the implicit form of f

$$f(x,y,z) = x^2 + 1 + yz - z^2 + 2x$$

parametricplot3d



implicitplot3d



Chapter 10

Monomial orderings examples

10.1 Elucidatory examples

In the chapter about Monomial orderings we mentioned that you should take care to choose an good ordering. We will give some examples. We use Maple12 to do the calculations. The Maple-code is available in the appendix.

Example 10.1.1 *Calculate Gröbner Bases for* $\mathfrak{a}$ *using the Lex- and Degrevlex-ordering.*

$$\mathfrak{a} = \langle x^5 + y^4 + z^2 - 1, x^3 + y^3 + z - 1 \rangle$$

With Lex-ordering we get the following Gröbner basis:

$$5z+30zy^6+10y^9+z^5+5z^4y^3+10z^3y^6+10z^2y^9-6y^12+y^15-3z^4y^4-3y^4-13z^2+5y^3-10y^6-20y^3z+3y^8-z^6+30y^3z^2+6y^4z^2+10z^3-20z^3y^3-30z^2y^6-20zy^9-3z^2y^8-2z^4+5zy^12,\ -80zy-80z+2z^3y^2-48zy^6-32y^5+128y^7-10z^5y^13-6z^6y^12-y^4z^10-80y^9+8z^9x+7z^11+z^12x+39z^5+283z^4y^3+92z^3y^6+58z^2y^9+54z^5y+22z^3y-94z^3y^8-292z^4y^5-138z^5y^2+84z^5x+16y^12+2z^11y^3+14yz^8-56z^6y^7-41z^4y^11+76z^4y^9+11z^5y^8+z^6y^14-40zy^10-76z^2y^7-76z^3y^4-80y^10-3z^9+17z^10+z^12-120z^3y^7+16y^14+126z^3y^10-66z^7x-34z^5y^6-2z^9y^7+2z^7y^11-20z^7y^9+z^8y^8+6yz^10+z^10y^6-z^8y^10+12z^8y^5+14z^2y^13+32y^4z^7+10z^9y^2-37z^4y^4-40zy^11-32y^4+88z^2-80y^3+24zy^13+3z^4y^14-9z^8y^6-52z^6y^10+72z^6y^5-33z^8x+16y^13+14z^7y^2-30z^4y^13-24z^5y^12+2y^4z^9+10z^2y^12+z^6x+15z^10x-171y^3z^6+145y^4z^6+24y^14z-4z^3y^14-19z^8y^3-16z^7y^6-80z^5y^10-29z^8+128y^6+120y^3z-80z^7y^7-36z^5y^11+48z^5y^9-51z^6y^8-14z^3y^13-20z^4y^12-3y^4z^8+80y^8+88yz^2-80y^2z+88y^2z^2+192y^5z-14z^7y+250z^5y^7+104z^3y^11-4z^5y^3-175z^4y^6+12z^3y^9+104z^5y^5+228z^4y^8+38z^2y^10+6z^5y^14+9z^10y^3+91z^6+18z^2y^11+192y^4z+16z^4y^7-22y^3z^2-72y^4z^2-48y^7z+106z^3-118z^6y-150z^5y^4-176z^3y^3-108z^2y^6-40zy^9+10z^4y-80z^2y^5-64z^3x+48z^4x+132z^4y^2+20z^3y^5-62z^2y^8-168z^4-69z^7-120zy^8-48z^6y^2+24zy^12+6z^11x-80y^11+18z^2y^14+58z^7y^3+163z^6y^6+95z^4y^10-12z^8y^7+9z^6y^11-54z^6y^9+7z^7y^8+18yz^9+6z^9y^6-6z^7y^10+4z^7y^5+20z^8y^2,\ 8192+18768zy-51888z-16384xzy+46422z^3y^2-73552zy^6+1568y^5-7296y^7-17072y^9+2374z^9x+201z^11+23359z^5-8192x+9139z^4y^3-42336z^3y^6-16098z^2y^9-20526z^5y-126z^3y-8192y+49972z^3y^8+17056z^4y^5-9668z^5y^2+8316z^5x+2800y^12+3048yz^8-14798z^6y^7-8233z^4y^11+16198z^4y^9-10987z^5y^8-17544zy^10-36164z^2y^7+8948z^3y^4+4432y^10+2681z^9+1312z^10-35564z^3y^7+2800y^14+29092z^3y^10-7163z^7x+36217z^5y^6+746z^2y^13-1314z^3y^12-722y^4z^7-48343z^4y^4-14984zy^11+22048y^4+97528z^2-35504y^3+$$

$$3544zy^{13}+1111z^4y^{14}+1619z^9y^3+1111z^8y^6-1111z^6y^{10}-336z^6y^5+30z^8x-272y^{13}+3070z^7y^2-2010z^4y^{13}-1206z^5y^{12}-201y^4z^9+1966z^2y^{12}-8021z^6x+1111z^{10}x+15234y^3z^6+6302y^4z^6+5080y^{14}z-38z^3y^{14}-997z^8y^3-2450z^7y^6-9811z^5y^{10}-2442z^8+31616y^6+104152y^3z-6144xz^2+8192xy-2222z^7y^7+1619z^5y^{11}-8954z^5y^9+1312z^6y^8-5080z^3y^{13}-4254z^4y^{12}+497y^4z^8+7856y^8-15624yz^2+16384xz+1360y^2z-21256y^2z^2-7584y^5z+678z^7y-3350z^5y^7-4914z^3y^{11}-40337z^5y^3-25057z^4y^6+9090z^3y^9+13240z^5y^5+6832z^4y^8+9202z^2y^{10}+201z^5y^{14}+402z^{10}y^3-8020z^6+29126z^2y^{11}-35232y^4z+58660z^4y^7-135730y^3z^2+19496y^4z^2+41136y^7z-67474z^3-3784z^6y+27207z^5y^4+8192z^2yx+85934z^3y^3+76764z^2y^6+23928zy^9+24552z^4y+50352z^2y^5-13248z^3x+14352z^4x-22142z^4y^2-76708z^3y^5-57018z^2y^8+1734z^4-5183z^7+3880zy^8+204z^6y^2-1064zy^{12}+201z^{11}x-12976y^{11}-1242z^2y^{14}-3912z^7y^3-2514z^6y^6-10987z^4y^{10}-402z^8y^7+402z^6y^{11}-4020z^6y^9+201z^7y^8+1206zy^9+201z^9y^6-201z^7y^{10}+2412z^7y^5+2010z^8y^2,1-x-2z+z^2-2y^3+xz^2+2y^3z+xy^4+y^6,16384-35120zy-93488z+110886z^3y^2-130256zy^6+97568y^5-24704y^7-32768y^2xz-27952y^9+32768y^2x+3478z^9x+449z^{11}+68231z^5-16384x+158043z^4y^3+66208z^3y^6-1874z^2y^9+16384xy^3z-34366z^5y-112398z^3y+51092z^3y^8-4192z^4y^5-19108z^5y^2+18588z^5x+2928y^{12}+4008yz^8-29406z^6y^7-20641z^4y^{11}+41878z^4y^9-26835z^5y^8+6072zy^{10}+110044z^2y^7+174932z^3y^4+30416y^{10}+3697z^9+2464z^{10}-178828z^3y^7-3216y^{14}+56196z^3y^{10}-9699z^7x+74993z^5y^6+5914z^2y^{13}+2414z^3y^{12}-3522y^4z^7-133727z^4y^4-77384zy^{11}+17696y^4+118072z^2-77104y^3-4328zy^{13}+2015z^4y^{14}+2683z^9y^3+2015z^8y^6-2015z^6y^{10}-6352z^6y^5-2130z^8x-6288y^{13}+2190z^7y^2-4490z^4y^{13}-2694z^5y^{12}-449y^4z^9-3394z^2y^{12}-4461z^6x+2015z^{10}x+36850y^3z^6+18478y^4z^6+11544y^{14}z-1910z^3y^{14}-4477z^8y^3-7298z^7y^6-20091z^5y^{10}-7610z^8+61312y^6-16384x^2z+170008y^3z+16384xz^2-4030z^7y^7+2683z^5y^{11}-10666z^5y^9+2464z^6y^8-6680z^3y^{13}-6702z^4y^{12}+1577y^4z^8-16384xy^3-32768y^2-81616y^8+84792yz^2+16384xz+4096x^2z^2+109264y^2z-158408y^2z^2-225440y^5z-1034z^7y+20250z^5y^7+12510z^3y^{11}-128841z^5y^3-132249z^4y^6-33806z^3y^9+39416z^5y^5+44848z^4y^8-53278z^2y^{10}+449z^5y^{14}+898z^{10}y^3-17460z^6+43030z^2y^{11}+47968y^4z+88324z^4y^7-114210y^3z^2-162072y^4z^2+23344y^7z+20350z^3-3720z^6y+39119z^5y^4-41794z^3y^3+69628z^2y^6+47544zy^9+95144z^4y+243504z^2y^5-11712z^3x-12912z^4x+4096z^4x^2-17422z^4y^2-133508z^3y^5-161898z^2y^8-111850z^4+761z^7+8192x^2z^3+157160zy^8+876z^6y^2-6888zy^{12}+449z^{11}x+27344y^{11}+630z^2y^{14}-2056z^7y^3+3390z^6y^6-5075z^4y^{10}-898z^8y^7+898z^6y^{11}-8980z^6y^9+449z^7y^8+2694yz^9+449z^9y^6-449z^7y^{10}+5388z^7y^5+4490z^8y^2,-1024+1680zy+5776z+1024yx^2z-8818z^3y^2+8816zy^6-7008y^5+896y^7+2048y^2xz+2192y^9-2048y^2x-258z^9x-35z^{11}-5909z^5-11921z^4y^3-3424z^3y^6+502z^2y^9-2048xy^3z+2938z^5y+7722z^3y+1024y-4604z^3y^8+416z^4y^5+1772z^5y^2-2004z^5x-336y^{12}-312yz^8+2266z^6y^7+1635z^4y^{11}-3522z^4y^9+2105z^5y^8+472zy^{10}-5524z^2y^7-12028z^3y^4-880y^{10}-275z^9-192z^{10}+13092z^3y^7+176y^{14}-5068z^3y^{10}+969z^7x-5939z^5y^6-590z^2y^{13}-266z^3y^{12}+262y^4z^7+10909z^4y^4+5336zy^{11}-352y^4-8104z^2+3728y^3-72zy^{13}-157z^4y^{14}-209z^9y^3-157z^8y^6+157z^6y^{10}+496z^6y^5+246z^8x+176y^{13}-170z^7y^2+350z^4y^{13}+210z^5y^{12}+35y^4z^9-58z^2y^{12}+455z^6x-157z^{10}x-2838y^3z^6-1418y^4z^6-840y^{14}z+162z^3y^{14}+375z^8y^3+582z^7y^6+1553z^5y^{10}+686z^8+1024x^2-3712y^6-10824y^3z-512xz^2+314z^7y^7-209z^5y^{11}+830z^5y^9-192z^6y^8+520z^3y^{13}+522z^4y^{12}-123y^4z^8+2048xy^3+2048y^2+4464y^8-1024yx^2-6312yz^2-1024x^2z^2-7024y^2z+10840y^2z^2+14304y^5z+158z^7y-1742z^5y^7-858z^3y^{11}+9723z^5y^3+10059z^4y^6+1898z^3y^9-2920z^5y^5-3408z^4y^8+3034z^2y^{10}-35z^5y^{14}-70z^{10}y^3+1340z^6-3778z^2y^{11}-3616y^4z-7948z^4y^7+10726y^3z^2+9416y^4z^2-1424y^7z+262z^3+536z^6y-3085z^5y^4+1030z^3y^3-6004z^2y^6-2856zy^9-7224z^4y-17296z^2y^5+1344z^3x-48z^4x+1642z^4y^2+11404z^3y^5+12606z^2y^8+7294z^4+181z^7-9912zy^8+60z^6y^2+184zy^{12}-35z^{11}x-1392y^{11}+30z^2y^{14}+280z^7y^3-186z^6y^6+313z^4y^{10}+70z^8y^7-70z^6y^{11}+700z^6y^9-35z^7y^8-210yz^9-35z^9y^6+35z^7y^{10}-420z^7y^5-350z^8y^2,1-x^2-z^2+x^2z-y^4+y^3x^2,x^3+y^3+z-1$$

With Degrevlex-ordering we get the following Gröbner basis:

$$[x^3+y^3+z-1,1-x^2-z^2+x^2z-y^4+y^3x^2,1-x-2z+z^2-2y^3+xz^2+2y^3z+xy^4+y^6]$$

From the same Ideal!

To get an idea of the difference in workload we use the showtime-command in Maple which display the time and space used by Maple for the execution of each

statement and got the following result for the calculation of the Gröbner bases:

Ordering	*Time*	*Space*
Lex	*0.55 seconds*	*2754263 bytes*
Degrevlex	*0.03 seconds*	*12851 bytes*

And remember the Gröbner basis itself is usually not the answer to your question. The purpose of this example was to show that you can save a lot of space and time by using a suitable monomial ordering and I think you get the picture now. Note that the showtime result variates, depending on the circumstances, but it will give you a hint.

Unfortunately, the fastest ordering will not always help you to solve your problem and we will give an example of that.

Example 10.1.2 *Solve the following system of equations:*

$$\begin{cases} f_1 = x^2 - y \\ f_2 = y^2 - z \\ f_3 = z^2 - y \end{cases}$$

If we calculate Gröbner basis, $\boldsymbol{G1}$*, for* $\mathfrak{a} = \langle x^2 - y, y^2 - z, z^2 - y\rangle$ *with the degrevlex order we see that* $\boldsymbol{G1} = \mathfrak{a}$ *and will not help us solve the system. But if we calculate the Gröbner basis,* $\mathfrak{G}_2$*, with the lex order we get* $\boldsymbol{G2} = \langle -z + z^4, -z^2+y, -z^2+x^2\rangle$ *and we can solve the system by solving the equation* $-z+z^4$ *and the use the result to solve the other two.*

Bibliography

[1] Cox, David, Little, John , O'Shea, Donal: *Ideals, varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra, Second Edition*, USA (1997) *Springer-Verlag* New York

[2] Fröberg, Ralf: *An Introduction to Gröbner Bases*, England (1997) *John Wilson & sons*

[3] Kreuzer, Martin, Robbiano, Lorenzo: *Computational Commutative Algebra 1*, Germany(2000) *Springer-Verlag* Berlin Heidelberg

Internet

Buchberger, Bruno <bruno.buchberger@risc.uni-linz.ac.at>:*Homepage of Bruno Buchberger*, <http://www.risc.uni-linz.ac.at/people/buchberg/>, last modified:2005-05-25, access date:2009-05-18

Appendix

We have used Maple12 to do calculations and plots in chapter 9 and chapter 10. This is the script for the input, example by example.

Example 9.1.1

```
>with(Groebner)
>f := {x^2-y-2*z+1, x^2+x*y+y^2-z^2, x^2-x*z+y-2, x^4+x*y*z+y*z+z^2-2}
>g := Basis(f, plex(x, y, z))
```

Example 9.1.2

```
>with(Groebner)
>f := {2*x*z-2*lambda*y, 3*x^2+2*y*z-2*lambda*x,
2*x*y-2*z-2*lambda*z, x^2+y^2+z^2-1}
>g := Basis(f, plex(lambda, z, y, x))
>solve(g)
```

Example 9.1.3

```
>with(Groebner)
>f := {z^2-y, x*y-1, y*z-x}
>g := Basis(f, tdeg(x, y, z))
```

Example 9.1.4

```
>with(Groebner)
>with(PolynomialIdeals)
>f := {a*b*c*d*e-1, a+b+c+d+e, a*b+b*c+c*d+d*e+a*e,
a*b*c+b*c*d+c*d*e+d*e*a+e*a*b, a*b*c*d+b*c*d*e+c*d*e*a+d*e*a*b+e*a*b*c}
>g := Basis(f, plex(a, b, c, d, e))
>NumberOfSolutions(<g>))
```

Example 9.2.1

```
>with(Groebner)
>f := {x = t/(1+t), y = 1-1/t^2}
>g := Basis(map(proc (eq) options operator, arrow;
 numer(lhs(eq)-rhs(eq)) end proc, f), lexdeg([t], [x, y]))
>remove(has, %, t)
```

Example 9.2.2

```
>with(Groebner)
>with(plots)
>f := {x = (-1024*t^3)*(1/(256*t^4+32*t^2+1)),
 y = (-2048*t^4+128*t^2)/(256*t^4+32*t^2+1)}
>g := Basis(map(proc (eq) options operator, arrow;
numer(lhs(eq)-rhs(eq)) end proc, f), lexdeg([t], [x, y]))
>remove(has, %, t)
>plot([(-1024*t^3)*(1/(256*t^4+32*t^2+1)),
(-2048*t^4+128*t^2)/(256*t^4+32*t^2+1), t = -50 .. 50],
 axes = none, numpoints = 250)
>implicitplot(-16*x^2+8*y*x^2+8*y^3+x^4+2*y^2*x^2+y^4 = 0,
 x = -6 .. 6, y = -10 .. 2, axes = none, numpoints = 10000)
```

Example 9.2.3

```
>with(Groebner)
>f := {x = t^8, y = t^12+t^14+t^15}
>g := Basis(map(proc (eq) options operator, arrow;
 numer(lhs(eq)-rhs(eq)) end proc, f), lexdeg([t], [x, y]))
>remove(has, %, t)
```

Example 9.2.4

```
>with(Groebner)
>with(plots)
>f := {x = u*v-1, y = u^2-v^2, z = u^2}
>g := Basis(map(proc (eq) options operator, arrow;
 numer(lhs(eq)-rhs(eq)) end proc, f), lexdeg([u, v], [x, y, z]))
>remove(has, %, [u, v])
>plot3d([u*v-1, u^2-v^2, u^2], u = 0 .. 1, v = -1 .. 1,
 shading = zgrayscale, style = patchnogrid, style = patchcontour,
 title = parametricplot3d, lightmodel = light2)
>implicitplot3d(x^2+1+y*z-z^2+2*x = 0, x = -5 .. 3, y = -4 .. 4,
 z = 0 .. 4,grid = [20, 20, 20], shading = zgrayscale,
 style = patchnogrid, style = patchcontour, title = implicitplot3d,
 lightmodel = light2)
```

Example 10.0.1

```
>with(Groebner)
>f := {x^3+y^3+z-1, x^5+y^4+z^2-1}
>showtime
>on
 g:=Basis(f,plex(x,y,z))
 g1:=Basis(f,tdeg(x,y,z))
 off
```

Example 10.0.2

```
>with(Groebner)
>f := {x^2-y,y^2-z,z^2-y}
>g:=Basis(f,tdeg(x,y,z))
>g1 := Basis(f, plex(x, y, z))
```