Gröbner Bases Lecture Notes

Moty Katzman

Contents

Introduction

These aim of these lectures is to introduce the concept of Gröbner bases and to see some of its applications.

Initially I will be following the introductory textbook [**AL**]. We will start by defining the Gröbner basis of an ideal and fairly soon we will know how to solve the following problems:

(1) (Ideal membership) Given $f \in k[x_1, \dots, x_n]$ and and ideal $I \subset k[x_1, \dots, x_n]$ decide whether $f \in I$. If $f \in I$ and I is generated by $f_1, \dots, f_r$ find $a_1, \dots, a_r$ such that $f = \sum_{i=1}^{r} a_i f_i$

(2) Given an ideal $I \subset k[x_1, \dots, x_n]$ find a k-basis for $k[x_1, \dots, x_n]/I$. If I is homogeneous find the Hilbert series and Hilbert polynomial of $k[x_1, \dots, x_n]/I$.

(3) (Elimination) Given an ideal $I \subset k[x_1, \dots, x_n]$ find $I \cap \subset k[x_1, \dots, x_i]$ for $i < n$.

(4) (Syzygies) Given $f_1, \dots, f_r \subset k[x_1, \dots, x_n]$ compute

$$\mathrm{Syz}(f_1, \dots, f_r) = \{(a_1, \dots, a_r) \subset k[x_1, \dots, x_n]^r | a_1 f_1 + \cdots + a_r f_r = 0\}$$

We will then extend the concept of Gröbner bases to modules and we will solve the corresponding questions for modules. The solution of the fourth problem above will enable us to compute free resolutions and with a little more effort we will be able to compute Tor's and Ext's.

While we learn all this I will show you how to use Macaulay2 ([**GS**]) to carry out specific calculations. I am hoping that some members of the audience will discover that they can do useful things in their fields using these tools. If this happens the seminar could well turn into a case study of Gröbner bases applications. I strongly encourage everyone to install Macaulay2 (I'll be happy to assist) and to start playing with it.

I am also planning to follow chapter 15 of [**E**] for a geometrical view of Gröbner bases and [**S**] for a combinatorial view. The exact contents of these lectures will depend on the interests and needs of the audience.

CHAPTER 1

Basic Theory and Applications

1. Term Orderings

Throughout these notes k will be a field. The set of non-negative integers will be denoted with $\mathbb{N}$.

Let $R = k[x_1, \ldots, x_n]$. We will write x^α for the monomial $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ where $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{N}$. Whenever we write x^α it will be implicit that $\alpha \in \mathbb{N}$

DEFINITION 1.1. Let $T = \{x^\alpha | \alpha \in \mathbb{N}^n\}$. A term order $<$ on T is a total order satisfying

(1) $1 < x^\beta$ for all $\beta \neq 0$
(2) If $x^\alpha < x^\beta$ then $x^\gamma x^\alpha < x^\gamma x^\beta$ for any x^γ.

EXAMPLE 1.2. The Lexicographical order
Define $x^\alpha <_{Lex} x^\beta \iff i$ is the *first* index for which $\alpha_i \neq \beta_i$ and $\alpha_i < \beta_i$.
When $n = 2$ we have

$$1 < x_2 < x_2^2 < \cdots < x_1 < x_1 x_2 < x_1 x_2^2 < \cdots < x_1^2 < \ldots$$

EXAMPLE 1.3. The Degree Lexicographical order
Define $x^\alpha <_{DegLex} x^\beta \iff$ either $\deg(x^\alpha) < \deg(x^\beta)$ or $\deg(x^\alpha) = \deg(x^\beta)$ and $x^\alpha <_{Lex} x^\beta$.
When $n = 2$ we have

$$1 < x_2 < x_1 < x_2^2 < x_1 x_2 < x_1^2 < \ldots$$

EXAMPLE 1.4. The Reverse Lexicographical order
Define $x^\alpha <_{RevLex} x^\beta \iff$ either $\deg(x^\alpha) < \deg(x^\beta)$ or $\deg(x^\alpha) = \deg(x^\beta)$ and $\alpha_i > \beta_i$ where i is the *last* index for which $\alpha_i \neq \beta_i$.
When $n = 2$ we have $<_{DegLex} = <_{RevLex}$ but when $n > 2$ the orders are different, e.g.,

$$x_1^2 x_2 x_3 >_{DegLex} x_1 x_2^3$$

and

$$x_1^2 x_2 x_3 <_{RevLex} x_1 x_2^3$$

EXERCISE 1.5.

(1) Check that the second property of term orderings guarantees that when the largest term of $f \in R$ is x^α then the largest term in $x^\gamma f$ is $x^\alpha x^\gamma$.
(2) Convince yourself that the three orders above are indeed term orderings.

We now fix an unspecified term ordering $<$ on T.

PROPOSITION 1.6. *If x^α divides x^β then $x^\alpha < x^\beta$.*

PROOF. Write $x^\beta = x^\gamma x^\alpha$. We have $1 \leq x^\gamma$ and multiplying both sides by x^α gives us $x^\alpha \leq x^\beta$. $\square$

THEOREM 1.7. *Term orderings are well orderings.*

PROOF. Assume we can find a $A \subset T$ and an infinite chain $x^{v_1} > x^{v_2} > x^{v_3} > \dots$. Let I_l be the ideal of R generated by $x^{v_1}, \dots, x^{v_l}$. We must have $I_l \subsetneqq I_{l+1}$ for all $l \geq 1$ otherwise write $x^{v_{l+1}} = a_1 x^{v_1} + \dots a_l x^{v_l}$ with $a_1, \dots, a_l \in R$; $x^{v_{l+1}}$ must occur as a monomial in the right hand side of the equation, but all the terms there are divisible by some x^{v_i} with $i \leq l$. The previous proposition implies then that $x^{v_l} \leq x^{v_i}$ for some $i \leq l$, a contradiction.

Now the ascending chain $I_1 \subsetneqq I_2 \subsetneqq \dots$ contradicts the fact that R is Noetherian. □

We can already prove something interesting! But before we do so we need some notation: Let $f \in R$ and write $f = \lambda_1 x^{v_1} + \lambda_2 x^{v_2} + \dots + \lambda_r x^{v_r}$ with $\lambda_1, \dots, \lambda_r \in k$ and $x^{v_1} > x^{v_2} > \dots > x^{v_r}$. We define

- $\mathrm{lp}(f) = x^{v_1}$
- $\mathrm{lc}(f) = \lambda_1$
- $\mathrm{lt}(f) = \lambda_1 x^{v_1}$

THEOREM 1.8. *The algebra of symmetric polynomials in R is $k[\sigma_1, \dots, \sigma_n]$ where*

$$\sigma_r = \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq n} x_{i_1} x_{i_2} \dots x_{i_r}$$

are the elementary symmetric polynomials.

PROOF. Fix the lexicographical order on T. Assume we can find a symmetric $f \in R$ with $f \notin k[\sigma_1, \dots, \sigma_n]$. By the previous theorem we may pick such an f with minimal $\mathrm{lp}(f)$.

Let $x^\alpha = \mathrm{lp}(f)$. We must have $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$; otherwise if any of the inequalities fails apply to f a transposition switching the two variables involved and we will obtain a new term in f (f is symmetric!) satisfying the inequality.

Consider

$$g = \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \dots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n}$$

Since $\mathrm{lp}_{<_{Lex}}(\sigma_r) = x_1 x_2 \dots x_r$ we have $\mathrm{lp}(g) = \mathrm{lp}(f)$.

But now $f' = f - \mathrm{lc}(f) g$ is symmetric, not in $k[\sigma_1, \dots, \sigma_n]$ and $\mathrm{lp}(f') < \mathrm{lp}(f)$ contradicting the minimality of $\mathrm{lp}(f)$. □

EXERCISE 1.9.
Modify the argument to produce an algorithm for writing symmetric polynomials as polynomials in the elementary symmetric polynomials. Pick your favourite symmetric polynomial and apply the algorithm to it. Does the algorithm (and hence the proof) work if we choose *RevLex* as our term ordering?

2. A division algorithm

Throughout this section $R = k[x_1, \dots, x_n]$ and we fix an unspecified term ordering on the monomials of R.

We now attempt to generalise long division to multivariate polynomials:

DEFINITION 2.1.

(1) Let $f, g, h \in R$, $g \neq 0$. We say that f *reduces to h with respect to g* if $\mathrm{lp}(g)$ divides a non-zero term cx^α ($c \in k$) in f and $h = f - c\frac{x^\alpha}{\mathrm{lt}(g)} g$. We denote this with $f \underset{g}{\rightarrow} h$.

(2) Let $f, h \in R$, $G \subset R - \{0\}$. We say that f *reduces to h with respect to G* if there exists a chain

$$f \rightarrow_{g_1} f_1 \rightarrow_{g_2} f_2 \dots \rightarrow_{g_t} h$$

where $g_1, \dots, g_t \in G$. We denote this with $f \underset{G}{\rightarrow}^{+} h$.

(3) $f \in R$ is *reduced with respect to* $G \subset R - \{0\}$ if no term in f is divisible by any $\mathrm{lp}(g)$, $g \in G$.

ALGORITHM 2.2 (The division algorithm).
Input: $f \in R$, $G = \{g_1, \ldots, g_t\} \subset R - \{0\}$
Output: $u_1, \ldots, u_t, r$ such that $f = u_1 g_1 + \cdots + u_t g_t + r$ and r is reduced with respect to G and $\mathrm{lp}(f) = \max\{lp(u_1)\,\mathrm{lp}(g_1), \ldots, lp(u_t)\,\mathrm{lp}(g_t)\}$
Start: Initialise $u_1 = \cdots = u_t = r = 0$ and $h = f$.

`while` $(h \neq 0)$ `do`
{
    `If` $\mathrm{lp}(g_i)$ `divides` $\mathrm{lp}(f)$ `for some` $g_i \in G$ `then`
    {

$$u_i \leftarrow u_i + \frac{\mathrm{lp}(h)}{\mathrm{lp}(g_i)}$$

$$h \leftarrow h - \frac{\mathrm{lp}(h)}{\mathrm{lp}(g_i)} g_i$$

    }
    `else`
    {

$$r \leftarrow r + \mathrm{lt}(h)$$

$$h \leftarrow h + \mathrm{lt}(h)$$

    }
}

Note that the reduced remainder produced by this algorithm is not unique, e.g., take $G = \{x - y, x\}$, $f = x$ and use the Lex term ordering with $x > y$. Then both $x \underset{G}{\longrightarrow}^{+} y$ and $x \underset{G}{\longrightarrow}^{+} 0$.

Obviously, if $f \underset{G}{\longrightarrow}^{+} 0$ then $f \in \langle G \rangle$. It is not true though that for all $f \in \langle G \rangle$, $f \underset{G}{\longrightarrow}^{+} 0$. For example, working with the Lex term ordering with the variables $a > b > c > d > e$, let $G = \{ac - d^2, bc - e^2\}$. Then $ae^2 - bd^2 \in \langle G \rangle$ but $ae^2 - bd^2$ is reduced with respect to G. We will remedy this in the next section by choosing a special set of generators for $\langle G \rangle$.

3. Gröbner Bases

Throughout this section $R = k[x_1, \ldots, x_n]$ and we fix an unspecified term ordering on the monomials of R.

We are now ready to introduce the main protagonist in these lectures:

DEFINITION 3.1. Let $I \subset R$ be an ideal. A finite set $G \subset I$ is a *Gröbner basis* for I if for any $f \in I$ there exists $g \in G$ such that $\mathrm{lp}(g) \in \mathrm{lp}(f)$.

Note that being a Gröbner basis depends on the term ordering being used: a set may be a Gröbner basis with one term ordering but not with another.

DEFINITION 3.2. Let $A \subset R$ be a subset. The initial ideal of A, denoted with $\mathrm{in}(A)$ is the monomial ideal generated by $\{\mathrm{lp}(a) | a \in A\}$. (Note that these also depend on the term ordering used.)

The next two theorems give a list of nice properties of Gröbner bases:

THEOREM 3.3. *Let $I \subset R$ be an ideal and $G = \{g_1, \ldots, g_t\} \subset R$. The following are equivalent:*

(1) *G is a Gröbner basis for I.*
(2) $f \in I \iff f \underset{G}{\longrightarrow}^{+} 0$

(3) $f \in I \iff f = h_1 g_1 + \cdots + h_t g_t$ *with* $\mathrm{lp}(f) = \max\{\mathrm{lp}(h_1 g_1), \ldots, \mathrm{lp}(h_t g_t)\}$

(4) $\mathrm{in}(G) = \mathrm{in}(I)$

EXERCISE 3.4. Prove the theorem.

COROLLARY 3.5. *If G is a Gröbner basis for an ideal I then the elements of G generate I.*

COROLLARY 3.6. *Gröbner bases exist!*

PROOF. Let $I \subset R$. $\mathrm{in}(I)$ is finitely generated, say by $\mathrm{lp}(g_1), \ldots, \mathrm{lp}(g_t)$ with $g_1, \ldots, g_t$. These elements form a Gröbner basis for I. □

From now on we will refer sometimes to finite set as being a Gröbner basis without reference to an ideal. This will mean that the given set is a Gröbner basis for the ideal generated by its elements.

THEOREM 3.7. *$G = \{g_1, \ldots, g_t\}$ is a Gröbner basis if and only if for any $f \in R$ the remainder of the division of f by G is unique.*

PROOF. If both $f \underset{G}{\longrightarrow}_+ r_1$ and $f \underset{G}{\longrightarrow}_+ r_2$ then $r_1 - r_2 = (f - r_2) - (f - r_1) \in \langle G \rangle$ and is reduced with respect to G. This can only happen if $r_1 = r_2$.

Assume now we have unique remainders. Pick any $f \in \langle G \rangle$. It will be enough to show that $f \underset{g}{\longrightarrow}_+ 0$. We may write $f = \sum_{\nu=1}^{l} c_\nu x^{\alpha_\nu} g_{i_\nu}$ with $c_\nu \in k$. It is not hard to see that if $f \underset{g}{\longrightarrow}_+ r$ with r reduced then also $f - \sum_{\nu=1}^{l} c_\nu x^{\alpha_\nu} g_{i_\nu} \underset{g}{\longrightarrow}_+ r$ implying that $r = 0$. □

EXAMPLE 3.8 (Homogenisation).
Let $f \in k[x_1, \ldots, x_n]$ have total degree d. We define the homogenisation of f with respect to t to be

$$f^h = t^d f(\frac{x_1}{t}, \ldots, \frac{x_n}{t}) \in k[x_1, \ldots, x_n, t].$$

Notice that f^h is homogeneous of degree d.

For an ideal $I \subset k[x_1, \ldots, x_n]$ we define I^h to be the ideal of $k[x_1, \ldots, x_n, t]$ generated by $\{f^h | f \in I\}$. Notice that if I is generated by $f_1, \ldots, f_t$ then we do not necessarily have $I^h = \langle f_1, \ldots, f_t \rangle$, e.g., $x_2 x_4 - x_3^2 \in \langle x_1 x_2 - x_3, x_1 x_3 - x_4 \rangle^h$ but $x_2 x_4 - x_3^2 \notin \langle x_1 x_2 - x_3 t, x_1 x_3 - x_4 t \rangle$

Let $<$ be a term ordering in $k[x_1, \ldots, x_n]$ which refines the degree ordering, e.g., *DegLex* or *RevLex*. Extend this to a term ordering for $k[x_1, \ldots, x_n, t]$ by defining $x^\alpha t^a <_h x^\beta t^b$ if and only if $x^\alpha < x^\beta$ or $x^\alpha = x^\beta$ and $a < b$. Notice that $\mathrm{lt}(f^h) = \mathrm{lt}(f)$.

Let G be a Gröbner basis for I. It turns out that $G^h := \{g_1^h, \ldots, g_t^h\}$ is a Gröbner basis for I^h and in particular, it generates the homogenisation. To see this pick any $f \in I^h$; we show that $\mathrm{lp}(f) \in \mathrm{in}(G^h)$.

Since I^h is homogeneous, it is enough to prove this claim for the homogeneous summands of f, so we may assume that f is homogeneous. Now write $f = f_i t^i + f_{i+1} t^{i+1} + \ldots$ where $f_i, f_{i+1}, \cdots \in k[x_1, \ldots, x_n]$ and $f_i \neq 0$. Define $f_h = f(x_1, \ldots, x_n, 1)$. We have $f = t^i (f_h)^h$ hence $\mathrm{lp}(f) = t^i \,\mathrm{lp}(f_h)$ and since $\mathrm{lp}(f_h) \in \mathrm{in}\, G = \mathrm{in}\, G^h$ we are done.

(Geometrically we are embedding an affine variety into a projective variety, so that the original variety is obtained by looking at the affine piece defined by $t = 1$.)

4. The Buchberger algorithm

Now that we have seen that Gröbner bases have such nice properties and that they exist we want to find a way to produce them. It turns out that one need only do the obvious thing!

DEFINITION 4.1. For any non-zero $f, g \in R$ we define the *S-polynomial* of f and g to be

$$\mathrm{S}(f, g) = \frac{\mathrm{lcm}(\mathrm{lp}(f), \mathrm{lp}(g))}{\mathrm{lt}(f)} f - \frac{\mathrm{lcm}(\mathrm{lp}(f), \mathrm{lp}(g))}{\mathrm{lt}(g)} g$$

What we are doing is to knock of the highest terms of f and g; by doing so we are creating a new polynomial which has the potential of having a highest term not divisible by $\mathrm{lp}(f)$ or $\mathrm{lp}(g)$.

This is the basic operation needed to compute Gröbner bases :

ALGORITHM 4.2 (The Buchberger algorithm).
Input: $G = \{g_1, \ldots, g_t\} \subset R - \{0\}$
Output: A Gröbner basis for the ideal generated by G.
Start:
`repeat`
$\{$
`Set` $G' \leftarrow \emptyset$
`For all pairs` $f, g \in G$ `do`
$\{$
`Write` $\mathrm{S}(f, g) \xrightarrow[G\cup G']{}{}^{+} r$ `with` r `reduced.`
`If` $r \neq 0$ `then set` $G' \leftarrow G' \cup \{r\}$
$\}$
$\}$ `until` $G' = \emptyset$

Note that this is indeed an algorithm, i.e., it terminates after a finite number of steps. To see this note that each time the condition $G' = \emptyset$ fails, we have added elements r to G' with $\mathrm{lp}(r) \notin \mathrm{in}(G)$ and, therefore, $\mathrm{in}(G) \subsetneqq \mathrm{in}(G' \cup G)$. Since R is Noetherian this cannot happen for ever.

It remains to show that the algorithm produces a Gröbner basis. Before we show that lets see the algorithm in action:

EXAMPLE 4.3. Let $R = k[a, b, c, d, e]$ where k is any field and lets use the lexicographical order in R with $a > b > c > d > e$. We find a Gröbner basis for the ideal generated by $g_1 = \underline{ac} - d^2$ and $g_2 = \underline{bc} - e^2$ (the leading terms are underlined.) We start with $G = \{g_1, g_2\}$. We have $g_3 = \mathrm{S}(g_1, g_2) = b(ac - d^2) - a(bc - e^2) = \underline{ae^2} - bd^2$. Since g_3 is reduced with respect to $\{g_1, g_2\}$ we add it to our provisional Gröbner basis.

In the next iteration we get

$$S(g_1, g_2) = g_3 \xrightarrow[g_3]{} 0$$

$$S(g_1, g_3) = bcd^2 - d^2e^2 \xrightarrow[g_2]{} d^2e^2 - d^2e^2 = 0$$

$$S(g_2, g_3) = \underline{-ae^4} + b^2cd^2 \xrightarrow[g_3]{} bd^2e^2 - b^2cd^2 \xrightarrow[g_2]{} bd^2e^2 - bd^2e^2 = 0$$

We stop here and declare $\{g_1, g_2, g_3\}$ to be a Gröbner basis.

Do not be mislead by this simple example: Gröbner bases of very simple ideals can turn out to be monstrous sets!

We now proceed to prove the validity of the Buchberger algorithm. We start by describing the syzygies of a set of monomials:

LEMMA 4.4. *Let $M_1, \ldots, M_t \in R$ be monomials and define $\phi : R^t \to R$ by $\phi(a_1, \ldots, a_t) = \sum_{i=1}^t a_i M_i$.*

(1)

$$\ker\phi = \bigoplus_{X^\alpha} \left\{ \sum_{u=1}^t \lambda_u Y_u \mathbf{e}_u \in \ker\phi \;\middle|\; M_u \text{ divides } X^\alpha, Y_u = \frac{X^\alpha}{M_u}, \lambda_u \in k \right\}$$

where the sum ranges over all terms X^α and $\mathbf{e_1}, \ldots, \mathbf{e_t}$ are the standard vectors.

(2) *Each element of* $(\ker\phi)_{X^\alpha}$ *is in the module generated by*
$$\sigma_{ij} := \frac{\operatorname{lcm}(M_i, M_j)}{M_i}\mathbf{e}_i - \frac{\operatorname{lcm}(M_i, M_j)}{M_j}\mathbf{e}_j$$

PROOF. To prove the first item note that $\sum_{i=1}^t a_i M_i = 0$ if and only if the coefficient of all terms X^α occurring in this expression are zero. Write each such term as $\sum_{i=1}^t b_{\alpha,i} M_i$; each of these gives us a new syzygy of the required form.

Now pick any $\sigma = \sum_{i=1}^t \lambda_i Y_i \mathbf{e}_i \in (\ker\phi)_{X^\alpha}$. We show that σ is in the module generated by $\{\sigma_{ij}\}_{1\le i,j\le t}$ by induction on the number of non-zero coordinates in σ.

If $\sigma \neq 0$ then at least two coordinates $\lambda_i Y_i$ and $\lambda_j Y_j$ are non-zero, thus X^α is divisible by both M_i and M_j so it must be divisible by $\operatorname{lcm}(M_i, M_j)$. But then $Y_i = X^\alpha/M_i$ is divisible by $\operatorname{lcm}(M_i, M_j)/M_i$. We may now subtract a multiple of σ_{ij} from σ to obtain a syzygy with fewer non-zero coordinates. $\square$

THEOREM 4.5 (The Buchberger Criterion). *Let* $G = \{g_1, \dots, g_t\} \subset R$. *Then* G *is a Gröbner basis if and only if* $\mathrm{S}(g_i, g_j) \xrightarrow[G]{}_+ 0$ *for all* $1 \le i, j \le t$.

PROOF. If G is a Gröbner basis then since each $\mathrm{S}(g_i, g_j)$ is in the ideal generated by G they must reduce to zero with respect to G.

Assume now that for all $1 \le i, j \le t$ we can write
$$\mathrm{S}(g_i, g_j) = \sum_{u=1}^t f_u^{ij} g_u \qquad \text{where} \qquad \max_{1\le u\le t} \operatorname{lp}(f_u^{ij}) \operatorname{lp}(g_u) < \operatorname{lcm}(\operatorname{lp}(g_i), \operatorname{lp}(g_j))).$$
Assume further that $\operatorname{lc}(g_i) = 1$ for $1 \le i \le t$.

Assume by way of contradiction that G is not a Gröbner basis and pick some $f = \sum_{i=1}^t f_i g_i$ with $\operatorname{lp}(f) \notin \operatorname{in}(G)$. Let $X^\alpha = \max_{1\le i\le t} \operatorname{lp}(f_i g_i)$ and assume we chose our f with minimal X^α. Let $I = \{1 \le i \le t \mid \operatorname{lp}(f_i g_i) = X^\alpha\}$.

Since $X^\alpha \in \operatorname{in}(G)$ we must have $\sum_{i\in I} \operatorname{lt}(f_i)\operatorname{lp}(g_i) = 0$. By the previous lemma we can write
$$\sum_{i\in I} \operatorname{lt}(f_i)\mathbf{e}_i = \sum_{i,j\in I, i<j} a_{ij}\sigma_{ij}$$
where a_{ij} is a scalar times $X^\alpha/\operatorname{lcm}(\operatorname{lp}(g_i), \operatorname{lp}(g_j))$ Mapping $\mathbf{e}_i \mapsto g_i$ we obtain
$$\sum_{i\in I} \operatorname{lt}(f_i)\operatorname{lt}(g_i) = \sum_{i,j\in I, i<j} a_{ij}\,\mathrm{S}(g_i, g_j) = \sum_{i,j\in I, i<j} a_{ij}\left(\sum_{u=1}^t f_u^{ij} g_u\right) = \sum_{u=1}^t \left(\sum_{i,j\in I, i<j} a_{ij} f_u^{ij}\right) g_u$$
Call the coefficient of g_u in the last expression h_u and note that
$$\operatorname{lp}(a_{ij} f_u^{ij} g_u) = \frac{X^\alpha}{\operatorname{lcm}(\operatorname{lp}(g_i), \operatorname{lp}(g_j))} \operatorname{lp}(f_u^{ij})\operatorname{lp}(g_u) < X^\alpha$$
and, therefore, $\operatorname{lp}(h_u)\operatorname{lp}(g_u) < X^\alpha$ for all $1 \le u \le t$.

Now subtract $\sum_{i\in I} \operatorname{lt}(f_i) g_i - \sum_{1\le u\le t} h_u g_u$ from f: all terms involving X^α get cancelled and are replaced by smaller terms. This contradicts our choice of f. $\square$

COROLLARY 4.6.

(1) *Any set of monomials is a Gröbner basis.*
(2) *If* $\operatorname{lp}(g_1), \dots, \operatorname{lp}(g_t)$ *are coprime in pairs then* $\{g_1, \dots, g_t\}$ *is a Gröbner basis.*
(3) *Homogeneous ideals have Gröbner bases consisting of homogeneous polynomials.*
(4) *Binomial ideals have Gröbner bases consisting of binomials.*

(5) *If* $\{g_1,\dots,g_t\}$ *is a Gröbner basis and* $k \subset K$ *is a field extension then the images of* $g_1,\dots,g_t$ *in* $R \otimes_k K$ *form a Gröbner basis.*

EXAMPLE 4.7. Let $G = \{x^3+y^3+z^3, y^4, z^4\}$. Verify that G is a Gröbner basis with respect to any term ordering satisfying $x^3 > y^3$ and $x^3 > z^3$. If we pick the lexicographical term ordering with $z > y > x$ then

$$\operatorname{in}\langle G\rangle = \begin{cases} \langle z^3, y^4, zy^3, zyx^3, y^3x^3, yx^6, zx^6, x^9\rangle & \operatorname{char} k \neq 2 \\ \langle z^3, y^4, zy^3, zyx^3, x^6\rangle & \operatorname{char} k = 2 \end{cases}$$

EXERCISE 4.8. Every student of Gröbner bases should compute at least one non-trivial Gröbner basis by hand: Verify the claim above.

EXERCISE 4.9. For any positive integers m, n let X be m by n the matrix whose (i,j)th entry is the indeterminate x_{ij}. Show that if we use the RevLex term ordering with $x_{11} > \cdots > x_{1n} > x_{21} \cdots > x_{2n} > \cdots > x_{mn}$ then the set of 2 by 2 minors of X form a Gröbner basis. Is this true for general r by r minors?

We finish this section by highlighting two special types Gröbner bases:

DEFINITION 4.10. Let $G = \{g_1,\dots,g_t\}$ be a Gröbner basis.

(1) G is minimal if $\operatorname{lc}(g_i) = 1$ for all $1 \le i \le t$ and for all $i \neq j$ $\operatorname{lp}(g_i)$ does not divide $\operatorname{lp}(g_j)$.
(2) G is reduced if it is minimal and in addition g_i is reduced with respect to $G - \{g_i\}$ for all $1 \le i \le t$.

Note that given a Gröbner basis $G = \{g_1,\dots,g_t\}$ we may produce a minimal Gröbner basis by dividing each g_i by $\operatorname{lc}(g_i)$ and getting rid of all g_is whose leading term is divisible by $\operatorname{lp}(g_j)$ for $j \neq i$.

Also note that if both $G = \{g_1,\dots,g_t\}$ and $F = \{f_1,\dots,f_s\}$ are minimal Gröbner bases of the same ideal then $s = t$ and after permuting the elements of F $\operatorname{lt}(g_i) = \operatorname{lt}(f_i)$. The point is that any $\operatorname{lp}(g_i)$ is divisible by some $\operatorname{lp}(f_j)$ and $\operatorname{lp}(f_j)$ must be divisible by some $\operatorname{lp}(g_l)$; but this implies that $\operatorname{lp}(g_i)$ is divisible by $\operatorname{lp}(g_l)$ forcing $i = l$ and $\operatorname{lp}(g_i) = \operatorname{lp}(f_j)$.

We now produce reduced Gröbner bases:

PROPOSITION 4.11. *Let* $G = \{g_1,\dots,g_t\}$ *be a minimal Gröbner basis for an ideal* I. *Define*

$$\begin{aligned}
&g_1 \xrightarrow[H_1]{}{}_+ h_1, && \text{where } h_1 \text{ is reduced with respect to } H_1 = \{g_2,\dots,g_t\}\\
&g_2 \xrightarrow[H_2]{}{}_+ h_2, && \text{where } h_2 \text{ is reduced with respect to } H_2 = \{h_1, g_3,\dots,g_t\}\\
&g_3 \xrightarrow[H_3]{}{}_+ h_3, && \text{where } h_3 \text{ is reduced with respect to } H_3 = \{h_1, h_2, g_4,\dots,g_t\}\\
&\vdots\\
&g_t \xrightarrow[H_t]{}{}_+ h_t, && \text{where } h_t \text{ is reduced with respect to } H_t = \{h_1, h_2,\dots,h_{t-1}\}
\end{aligned}$$

$H = \{h_1,\dots,h_t\}$ *is a reduced Gröbner basis for* I.

PROOF. We have $\operatorname{lp}(h_i) = \operatorname{lp}(g_i)$ for all $1 \le i \le t$ so H is a (minimal) Gröbner basis. It is easy to verify that H is reduced. □

THEOREM 4.12. *Fix a term ordering in* R. *Every ideal has a unique reduced Gröbner basis with respect to that term ordering.*

PROOF. We already saw that reduced Gröbner bases exist. To prove uniqueness let $H = \{h_1,\dots,h_t\}$ and $G = \{g_1,\dots,g_t\}$ be two reduced Gröbner bases for the same ideal I. Order these polynomials so that $\operatorname{lp}(h_i) = \operatorname{lp}(g_i)$ for all $1 \le i \le t$. If $h_i \neq g_i$ for some $1 \le i \le t$ then since $h_i - g_i \in I$ there exists a $1 \le j \le t$ so that $\operatorname{lp}(h_j)$ divides $\operatorname{lp}(h_i - g_i) < \operatorname{lp}(h_i)$ and we must have $j \neq i$. But then $\operatorname{lp}(h_j)$ divides a term of h_i or a term of g_i, a contradiction. □

5. Elimination

In this section we solve the following problems:

(1) Given an ideal $I \subset k[x_1, \dots, x_m, y_1, \dots, y_n]$ find $I \cap k[y_1, \dots, y_n]$.
(2) Given a map $\phi : k[y_1, \dots, y_n] \to k[x_1, \dots, x_m]$ find $\ker \phi$. If we are also given a $f \in k[x_1, \dots, x_m]$ decide whether $f \in \operatorname{Im} \phi$.

DEFINITION 5.1. A term ordering $<$ in $k[x_1, \dots, x_m, y_1, \dots, y_n]$ is *an elimination order for* $x_1, \dots, x_m$ if for all exponents $\alpha \neq 0, \beta, \gamma$ one has $x^\alpha y^\beta > y^\gamma$. (I.e., any x is bigger that any monomial in the y's.)

EXAMPLE 5.2.

(1) Let $<_x$ and $<_y$ be term ordering in $k[x_1, \dots, x_m]$ and $k[y_1, \dots, y_n]$ respectively. Define a new term ordering $<$ as follows: $x^\alpha y^\beta < x^\gamma y^\delta \iff x^\alpha < x^\gamma$ or $x^\alpha = x^\gamma$ and $y^\beta < y^\delta$. Verify that $<$ is an elimination order for $x_1, \dots, x_m$.
(2) The lexicographical term ordering with $x_1 > \dots > x_m$ is an elimination order for all initial segments of the variables $x_1, \dots, x_i$ $(i \leq m)$. To verify this notice that the lexicographical ordering on $x_1 > \dots > x_m$ is the product of the lexicographical orderings on $x_1 > \dots > x_i$ and $x_{i+1} > \dots > x_m$.
(3) Any term ordering refining the degree ordering is not an elimination order (except for the uninteresting case of one variable).

THEOREM 5.3. *Fix an elimination order for $x_1, \dots, x_m$ in $S = k[x_1, \dots, x_m, y_1, \dots, y_n]$ and let G be a Gröbner basis for an ideal $I \subset S$ with respect to this term ordering. Then $G \cap k[y_1, \dots, y_n]$ is a Gröbner basis for $I \cap k[y_1, \dots, y_n]$ with respect to the term ordering obtained by restricting the original term ordering to $k[y_1, \dots, y_n]$. In particular $G \cap k[y_1, \dots, y_n]$ generates $I \cap k[y_1, \dots, y_n]$.*

PROOF. Clearly $G \cap k[y_1, \dots, y_n] \subset I \cap k[y_1, \dots, y_n]$. Pick any $0 \neq f \in I \cap k[y_1, \dots, y_n]$. Since $f \in I$ there exists $g \in G$ such that $\operatorname{lp}(g) | \operatorname{lp}(f)$; but since $f \in k[y_1, \dots, y_n]$ we must have $\operatorname{lp}(g) \in k[y_1, \dots, y_n]$ and the fact that our term ordering is an elimination order for $x_1, \dots, x_m$ implies then that $g \in\in k[y_1, \dots, y_n]$. This shows that f can be reduced to zero with respect to $G \cap k[y_1, \dots, y_n]$. ☐

EXERCISE 5.4 (Computing the intersection of ideals).
Let $I, J \subset k[y_1, \dots, y_n]$ be ideals and consider the ideal L of $k[x, y_1, \dots, y_n]$ generated by the elements of xI and $(1-x)J$. Show that $I \cap J = L \cap k[y_1, \dots, y_n]$.

EXERCISE 5.5 (Computing colon ideals).
Let $I \subset k[x_1, \dots, x_m]$ be an ideal and let $f \in k[x_1, \dots, x_m]$. Show that

$$(I : f) := \{r \in k[x_1, \dots, x_m] \mid rf \in I\} = \frac{1}{f}(I \cap \langle f \rangle).$$

Use this to compute Let $I : J := \{r \in k[x_1, \dots, x_m] \mid rJ \in I\}$ for any two ideals $I, J \subset k[x_1, \dots, x_m]$.

THEOREM 5.6. *Define $\phi : k[y_1, \dots, y_n] \to k[x_1, \dots, x_m]$ by $\phi(y_i) = f_i$ where $f_1, \dots, f_n \in k[x_1, \dots, x_m]$. Let $I \subset S = k[x_1, \dots, x_m, y_1, \dots, y_n]$ be the ideal generated by $y_1 - f_1, \dots, y_n - f_n$. Then* $\ker \phi = I \cap k[y_1, \dots, y_n]$.

PROOF. If $h \in I \cap k[y_1, \dots, y_n]$ then $h(f_1, \dots, f_n) = 0$ and, therefore, $I \cap k[y_1, \dots, y_n] \subset \ker \phi$. Pick $h \in \ker \phi$ and write $h = \sum_{\nu=1}^s c_\nu y^{\alpha_\nu}$ where $c_1, \dots, c_s \in k$. We have $h = h - h(f_1, \dots, h_n) = \sum_{\nu=1}^s c_\nu (y^{\alpha_\nu} - f^{\alpha_\nu}) \equiv 0(\mod I)$. ☐

One can generalise the previous theorem as follows:

THEOREM 5.7. *Let $J \subset k[x_1, \ldots, x_m]$ be an ideal and define $\phi : k[y_1, \ldots, y_n] \to k[x_1, \ldots, x_m]/J$ by $\phi(y_i) = f_i$ where $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$. Let $I \subset S = k[x_1, \ldots, x_m, y_1, \ldots, y_n]$ be the ideal generated by J and $y_1 - f_1, \ldots, y_n - f_n$. Then $\ker \phi = I \cap k[y_1, \ldots, y_n]$.*

THEOREM 5.8. *Let $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$. Fix an elimination order for $x_1, \ldots, x_m$ in $S = k[x_1, \ldots, x_m, y_1, \ldots, y_n]$ and let G be a Gröbner basis for the ideal $I = \langle y_1 - f_1, \ldots, y_n - f_n \rangle \subset S$ with respect to this term ordering. Then $p \in k[x_1, \ldots, x_m]$ is in $k[f_1, \ldots, f_n] \iff p \xrightarrow[G]{}_+ h$ where $h \in k[y_1, \ldots, y_n]$. If this occurs then $p = h(f_1, \ldots, f_n)$.*

PROOF. Assume first that $p = g(f_1, \ldots, f_n)$ where $g \in k[y_1, \ldots, y_n]$. We have $p(x_1, \ldots, x_m) - g(y_1, \ldots, y_n) = g(f_1, \ldots, f_n) - g(y_1, \ldots, y_n) \equiv 0 \mod I$. There exist unique $h_1, h_2 \in S$ reduced with respect to G such that $p(x_1, \ldots, x_m) \xrightarrow[G]{}_+ h_1$ and $g(f_1, \ldots, f_n) \xrightarrow[G]{}_+ h_2$, and since $h_1 - h_2$ is reduced, we must have $h_1 = h_2$. All reductions of $g(y_1, \ldots, y_n)$ must be with elements of $G \cap k[y_1, \ldots, y_n]$, i.e., $h_2 = h_1 \in k[y_1, \ldots, y_n]$.

Assume now that $p(x_1, \ldots, x_m) \xrightarrow[G]{}_+ h \in k[y_1, \ldots, y_n]$. Then $p(x_1, \ldots, x_m) - h(y_1, \ldots, y_n) \in I$ and substituting $y_1 \mapsto f_1, \ldots, y_n \mapsto f_n$ we get $p(x_1, \ldots, x_m) = h(f_1, \ldots, f_n)$. □

6. Solving systems of polynomial equations

Throughout this section $R = k[x_1, \ldots, x_n]$.

DEFINITION 6.1. An ideal $I \subset R$ is *zero dimensional* if any of the following equivalent conditions holds:

(1) $V_{\overline{k}}(I)$ is finite, where $\overline{k}$ is the algebraic closure of k.
(2) Fix any term ordering in R. For any $1 \le i \le n$ there exists a $g_i \in I$ such that $\mathrm{lp}(g_i) = x_i^{a_i}$ for some positive integer a_i.
(3) $\dim_k R/I < \infty$.

PROPOSITION 6.2. *Let I be a zero dimensional ideal of R. Fix the lexicographical term ordering in R and let G be a Gröbner basis for I with respect to this ordering. There exist $g_1, \ldots, g_n \in G$ with $g_i \in k[x_i, \ldots, x_n]$.*

PROOF. The second condition of the definition above guarantees the existence of $g_1, \ldots, g_n \in G$ with $\mathrm{lp}(g_i) = x_i^{a_i}$ for some positive integer a_i. But our choice of term ordering then implies that $g_i \in k[x_i, \ldots, x_n]$. □

EXAMPLE 6.3. We solve $x^2 + 2y^2 - 2 = 0, x^2 + xy + y^2 - 2 = 0$ over $\mathbb{C}$. The corresponding Gröbner basis is $\{y^3 - 2/3y, xy - y^2, x^2 + 2y^2 - 2\}$. We immediately deduce that I is zero-dimensional: $\{1, x, y, y^2\}$ is a k-basis for $k[x, y]/I$.

The first element of our Gröbner basis forces $y \in \{0, \sqrt{2/3}, -\sqrt{2/3}\}$. Substituting these values of y into out original equations gives us six solutions: $(\pm\sqrt{2}, 0), (\pm\sqrt{2/3}, \pm\sqrt{2/3})$

Note that when k is algebraically closed and I is zero-dimensional, the number of solutions is just $\prod_{i=1}^{n} a_i$.

What can we say when I is not zero dimensional?

Assume henceforth that $k = \overline{k}$.

THEOREM 6.4. *Let $I \subset R$ be the ideal generated by $f_1, \ldots, f_r$ and let $V = V(I)$. Let $\pi_s : k^n \to k^{n-s}$ be the projection onto the last $n - s$ coordinates, and write $I_s = I \cap k[x_{s+1}, \ldots, x_n]$. Then $V(I_s)$ is the Zariski closure of $\pi_s(V)$, i.e., $V(I_s) = V(I(\pi_s(V)))$.*

PROOF. Clearly, $\pi_s(V) \subset V(I_s)$.

Pick $f \in I(\pi_s(V))$; we have $f(a_{s+1}, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in V$ and if we regard f as a function on k^n then $f(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in V$. Hilbert's Nullstellesatz implies that $f^N \in I \cap k[x_{s+1}, \ldots, x_n]$, i.e., $f \in \mathrm{Rad}(I_s)$. So we have $I(\pi_s(V)) \subset \mathrm{Rad}(I_s)$ implying that $V(I(\pi_s(V))) \supset \mathrm{V}(\mathrm{Rad}(I_s)) = V(I_s)$. □

EXAMPLE 6.5. Let $I = \langle xy-1, xz-1\rangle \subset k[x, y, z]$. The $I_1 = \langle y-z\rangle$. Any point $(a, a) \in V(y-z)$ extends to a solution $(1/a, a, a) \in \mathrm{V}(I)$ *except* for the point $(0, 0)$.

Notice that in the previous example when $y = z = 0$ the leading terms of the generators of I vanish. The following theorem shows that this is all that can go wrong:

THEOREM 6.6 (The Extension Theorem). *Let I be the ideal of $k[x_1 \ldots, x_n]$ generated by $f_1, \ldots, f_r$. Write*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ terms of lower degree in } \mathrm{x}_1.$$

Let $(a_2, \ldots, a_n) \in V(I_1)$. If $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_r)$ then there exists an $a_1 \in K$ such that $(a_1, \ldots, a_n) \in V(I)$.

PROOF. We prove the theorem for $r = 2$. The proof for $r > 2$ is similar but more technical– it can be found in the third chapter of [**CLO2**].

If we regard f_1, f_2 as polynomials in x_1 we can compute the Sylvester resultant $R = \mathrm{Res}(f_1, f_2) \in I_1$ and $R(a_2, \ldots, a_n) = 0$.

If $C_1 := g_1(a_2, \ldots, a_n) \neq 0$ and $C_2 := g_2(a_2, \ldots, a_n) \neq 0$ then $f_1(x_1, a_2, \ldots, a_n)$ and $f_2(x_1, a_2, \ldots, a_n)$ have a common root and we are done.

If $C_2 = 0$ (in which case $C_1 \neq 0$) replace f_2 with $f_2 + x_1^N f_1$ where N is chosen so that the x_1-degree of the new polynomial increases. The leading coefficient of the new polynomial is $C_1 \neq 0$. Now we can apply the previous argument to conclude that we can extend the solution to $V(f_1, f_2 + x_1^N f_1) = V(f_1, f_2)$.

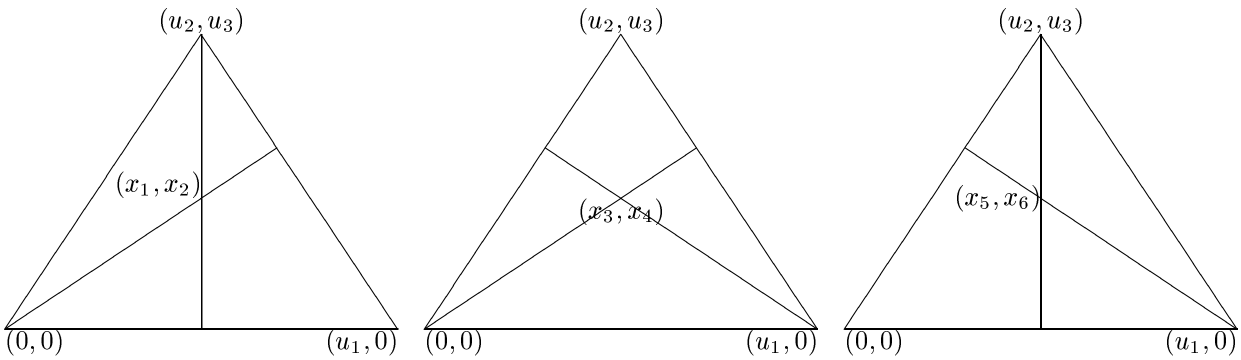
□

7. Automatic proofs of geometrical theorems

In this section we continue the equation solving theme, but from a different perspective.

We will produce an machine proof for the fact that the heights from the three vertices of a triangle meet in one point.

We start by placing one vertex of our triangle in the points $(0, 0)$, $(0, u_1)$ and (u_2, u_3). We then give names to the pairwise intersections of heights as illustrated below:



The hypotheses of the theorem can one be stated as the vanishing of

$$\begin{array}{ll} x_1(u_2-u_1)+x_2u_3, & u_2-x_1, \\ (x_3-u_1)u_2+x_4u_3, & x_3(u_2-u_1)+x_4u_3, \\ x_5-u_2, & (x_5-u_1)u_2+x_6u_3. \end{array}$$

while the conclusions can be written as vanishing of

$$x_1-x_3, x_1-x_5, x_2-x_4, x_2-x_6$$

Let H be the ideal of $R := \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4, x_5, x_6]$ generated by these six hypotheses and call the conclusions c_1, c_2, c_3 and c_4.

To prove the theorem one needs to show that $\mathrm{V}(c_i) \supset \mathrm{V}(H)$, i.e., $c_i \in I(\mathrm{V}(H))$.

A first attempt to prove this could be to try and show that $c_i \in H$, but this does not hold:

```
i27 : R=QQ[x_1..x_6,u_1..u_3, U, MonomialOrder=>Lex];

i28 : H={x_1*(u_2-u_1)+x_2*u_3, u_2-x_1, (x_3-u_1)*u_2+x_4*u_3,
      x_3*(u_2-u_1)+x_4*u_3, x_5-u_2, (x_5-u_1)*u_2+x_6*u_3};

i29 : --- Make sure that the u's are independent.
      G=gb ideal H;

i30 : print (selectInSubring(6, gens G));
0
i31 : Conclusions={x_1-x_3,x_1-x_5,x_2-x_4,x_2-x_6};

i32 : --- Are the conclusions in the ideal of the hypotheses?
      apply(apply(Conclusions, t->t%ideal(H)), print);
- x  + u
   3    2
0
x  - x
 2    4
x  - x
 2    6
```

If we were working over $\mathbb{C}$ the condition $c_i \in I(\mathrm{V}(H))$ is equivalent to $c_i \in \mathrm{Rad}(I)$; working over $\mathbb{R}$ this is only sufficient.

One can try and check whether this holds using the following:

PROPOSITION 7.1. *Let $S = k[y_1, \dots, y_n]$ and let $I \subset S$ be an ideal. $f \in \mathrm{Rad}(I)$ if and only if* 1 *is in the ideal of $S[y]$ generated by I and $1 - yf$.*

PROOF. Pick generators $f_1, \dots, f_m$ for I.

If $1 = \sum_{i=1}^m p_i(y_1, \dots, y_n, y) f_i + q(y_1, \dots, y_n, y)(1 - yf)$ substitute $y = 1/f$ and clear denominators.

The proof in the other direction is similar. ☐

But even this condition fails here!

```
i33 : --- Are the conclusions in the radical of the ideal of the hypotheses?
      apply(apply(Conclusions, u->gens gb(ideal(H)+ideal(U*u-1_R))), print);
{0} | u_1 x_6u_3-u_1u_2+u_2^2 x_5-u_2 x_4u_3U-u_1u_2U+u_2^2U-u_2 x_4u_2^2U-x_6u_
```

```
2^2U+x_6u_2 x_3U-u_2U+1 x_3u_2+x_4u_3-u_1u_2 x_2u_3-u_1u_2+u_2^2 x_2u_2-x_6u_2 x
_1-u_2 |
{0} | 1 |
{0} | u_1u_3 u_1^2u_2-u_1u_2^2 x_6u_3-u_1u_2+u_2^2 x_5-u_2 x_4u_3U-u_1u_2U+u_2^2
U+u_3 x_4u_1u_2U-x_4u_2^2U-x_6u_1u_2U+x_6u_2^2U+u_1u_2-u_2^2 x_3u_2+x_4u_3-u_1u_
2 x_3u_1-u_1u_2 x_2U-x_4U-1 x_2u_3-u_1u_2+u_2^2 x_2u_1u_2-x_2u_2^2-x_6u_1u_2+x_6
u_2^2 x_1-u_2 |
{0} | u_3 u_1u_2-u_2^2 x_5-u_2 x_3u_2+x_4u_3-u_1u_2 x_3u_1-u_1u_2 x_2U-x_6U-1 x_
1-u_2 |
```

The problem is that the theorem as stated is false: we are including degenerate cases, e.g., when $u_1 = u_2 = u_3 = 0$.

The right condition to impose is the following:

Definition 7.2. The conclusion c follows generically from H if $c \in I(V')$ where V' is the union of the components of $\mathrm{V}(H)$ on which u_1, u_2, u_3 are algebraically independent.

We have a sufficient condition for c to follow generically from H:

Proposition 7.3. *c follows generically from H if $ac \in \mathrm{Rad}(H)$ for some $a \in \mathbb{R}[u_1, \ldots, u_m]$.*

Proof. Let V_j be an irreducible component of V'. We know that ac vanishes on V_j but $I(V_j)$ is prime and by hypothesis $a \notin I(V_j)$ and, therefore, $c \in I(V_j)$. □

Notice c may follow generically from H even when no such a exists! The reason for this is that Hilbert Nullstellensatz fails over $\mathbb{R}$: ac may be in $I(\mathrm{V}(H))$ but not in $\mathrm{Rad}(H)$.

Proposition 7.4. *Let $S = \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ and let $\overline{H} = HS[y] + \langle 1 - yc \rangle \subset S[y]$. $ac \in \mathrm{Rad}(H)$ for some $a \in \mathbb{R}[u_1, \ldots, u_m]$ if and only if $a \in \overline{H} \cap \mathbb{R}[u_1, \ldots, u_m]$.*

Proof. If we work over the polynomial ring $T = \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$ then the condition $ac \in \mathrm{Rad}(H)$ is equivalent to $c \in \mathrm{Rad}(HT)$ and this is equivalent to 1 being in the ideal of $T[y]$ generated by H and $yc - 1$. Clearing denominators and working over S again, this is equivalent to $\overline{H} \cap \mathbb{R}[u_1, \ldots, u_m] \neq 0$.

On the other hand, if $a \in \overline{H} \cap \mathbb{R}[u_1, \ldots, u_m]$ then we can write

$$a = \sum_{i=1}^{m} p_i(y_1, \ldots, y_n, y) f_i + q(y_1, \ldots, y_n, y)(1 - yc)$$

and if we set $y = 1/c$ and clear denominators then we see that $c^N a \in H$ for some large N, and in particular $(ac)^N \in H$.

□

```
i36 : --- What are the hidden assumptions of this theorem?
      a=apply(Conclusions, u->(
        J=ideal(H)+ideal(U*u-1);
        G2=gb J;
        G2=selectInSubring(6, gens G2)
        )
      );

i37 : apply(a, print);
{0} | u_1 |
```

```
{0} | 1 |
{0} | u_1u_3 u_1^2u_2-u_1u_2^2 |
{0} | u_3 u_1u_2-u_2^2 |
```

And the theorem is proved.

EXERCISE 7.5. Use Macaulay2 to prove that the following theorem: Let $ABCD$ be a parallelogram and let M be the midpoint of AB: line segment DM trisects the diagonal AC.

8. Hilbert functions

Let $R = k[x_1, \ldots, x_n]$ and let $I \subset R$ be a homogeneous ideal. Then R/I is a graded k-algebra generated in degree one

$$R/I = (R/I)_0 \oplus (R/I)_1 \oplus \ldots.$$

DEFINITION 8.1. The *Hilbert function of R/I* is

$$\mathrm{HF}(d) = \dim_k (R/I)_d.$$

The *Hilbert series of R/I* is

$$\mathrm{HS}(t) = \sum_{d=0}^{\infty} \mathrm{HF}(d) t^d.$$

EXAMPLE 8.2.

(1) If $I = 0$ then $\mathrm{HF}(d) = \binom{n+d-1}{d-1}$ is the number of monomials in n variables of degree d and $\mathrm{HS}(t) = 1/(1-t)^n$.
(2) Take $R = k[x, y, z]$ and $I = \langle z^3 - xy^2 \rangle$. As a basis for $(R/I)_d$ we can take the set of degree d monomials which are not divisible by z^3. Then for $d \geq 2$ we have $\mathrm{HF}(d) = \binom{d+1}{1} + \binom{d}{1} + \binom{d-1}{1}$.

Hilbert functions and series have very interesting properties– here are some:

THEOREM 8.3.

(1) *There exists a polynomial $P(d)$ such that* $\mathrm{HF}(d) = P(d)$ *for all large d.*
(2) $\deg(P) = \dim(R/I) + 1$ *where "dim" is Krull dimension.*
(3)
$$\mathrm{HS}(t) = \frac{h(t)}{(1-t)^{\dim(R)}}$$
where $h(t)$ is a polynomial and $h(1) \neq 0$.

See chapter 4 of [**BH**] for a proof of this theorem.

REMARK 8.4.

(1) The polynomial $P(d)$ in theorem 8.3 is called the Hilbert polynomial of R/I.
(2) Let $h(t)$ the numerator of theorem 8.3 and write $h(t) = h_0 + h_1 t + \ldots h_r t^r$. The sequence $(h_0, h_1, \ldots, h_r)$ is called the h-vector of R/I. These invariants of R/I have interesting combinatorial interpretations.
(3) The *a-invariant* of R, denoted by $a(R)$, is the degree of the Hilbert series of R as a rational function. When R is Cohen-Macaulay $P(d) = HF(d)$ for all $d \geq a(R)$.

We now fix a term ordering $<$ in R.

DEFINITION 8.5. The *standard monomials of R/I* are all monomials in R not in $\mathrm{in}_<(I)$.

THEOREM 8.6 (F. S. Macaulay). *The set of standard monomials of R/I of degree d is a k-basis of $(R/I)_d$.*

PROOF. Let $m_1,\dots,m_s$ be the standard monomials of R/I of degree d. If $\sum_{i=1}^s \lambda_i m_i = 0$ in $(R/I)_d$ then $\sum_{i=1}^s \lambda_i m_i \in I$ and the largest of the m_i such that $\lambda_i \neq 0$ must be in $\mathrm{in}_< I$, a contadiction unless $\lambda_1 = \cdots = \lambda_s = 0$.

To show that $m_1,\dots,m_s$ span $(R/I)_d$ suppose we can pick $f \in (R/I)_d$ not in the span of $m_1,\dots,m_s$ and assume we pick such an f with minimal $\mathrm{lp}(f)$. If $\mathrm{lp}(f) \in \{m_1,\dots,m_s\}$ then by subtracting from f a multiple of some m_i we can obtain a counterexample with smaller lp(). So $\mathrm{lp}(f) \in \mathrm{in}_<(I)$ and we may choose $g \in I$ homogeneous with $\mathrm{lp}(g) = \mathrm{lp}(f)$. But then $f' := f - g \in (R/I)_d$ is not in the span of $m_1,\dots,m_s$ and $\mathrm{lp}(f') < \mathrm{lp}(f)$, a contradiction. □

The previous theorem allows us to reduce the problem of computing Hilbert functions and series to the case where I is generated by monomials:

COROLLARY 8.7. *R/I and $R/\mathrm{in}_<(I)$ have the same Hilbert functions and Hilbert series.*

To compute Hilbert functions we note that if $f \in R$ is homogeneous of degree δ then we have a graded exact sequence

$$0 \to \frac{(I:f)}{I}(-\delta) \to \frac{R}{I}(-\delta) \xrightarrow{f} \frac{R}{I} \to \frac{R}{I + \langle f\rangle} \to 0$$

where for any graded R-module M we denote by $M(-\delta)$ the module M obtained by redefining the grading $M(-\delta)_d = M_{d-\delta}$.

We can turn this sequence into the following graded short exact sequence

$$0 \to \frac{R}{(I:f)}(-\delta) \xrightarrow{f} R/I \to \frac{R}{I+\langle f\rangle} \to 0.$$

By restricting the exact sequence to the degree d pieces we can then regard it as a collection of exact sequences of vector spaces and this gives us

$$\mathrm{HF}_{R/I}(d) = \mathrm{HF}_{\frac{R}{I+\langle f\rangle}}(d) + \mathrm{HF}_{\frac{R}{(I:f)}}(d-\delta)$$

and

$$\mathrm{HS}(R/I) = \mathrm{HS}(\frac{R}{I+\langle f\rangle}) + t^\delta\,\mathrm{HS}(\frac{R}{(I:f)}).$$

When $I \subset R$ is an ideal generated by monomials $m_1,\dots,m_{l+1}$ then we may take $f = m_{l+1}$ and $I' = m_1,\dots,m_l$. We have

$$(I:f) = \left\langle \frac{\mathrm{lcm}(m_1,f)}{f},\dots,\frac{\mathrm{lcm}(m_l,f)}{f}\right\rangle$$

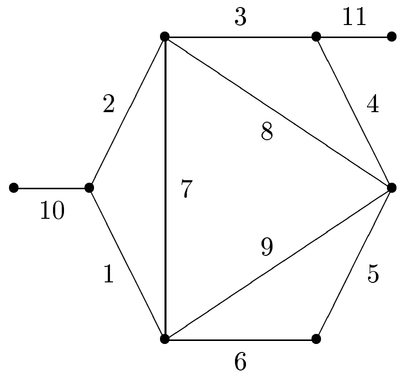
which is also a monomial ideal. We may the compute the Hilbert function and series of R/I by induction on the number of generators of I.

Application: Matching numbers of graphs. Let G be a (finite, simple) graph. A r-*matching of* G is a set of r edges in G with no common vertices. Let E be the set of edges of G and let $R = k[E]$. Define I to be the ideal generated by all ef where $e,f \in E$ share a vertex.

PROPOSITION 8.8. *The number of r-matchings of G is $\mathrm{HF}_{R/I}(r) = h_r$.*

PROOF. Note that $\{e_1,\dots,e_r\}$ is a matching if and only if $e_1e_2\dots e_r \notin I$, i.e., $e_1e_2\dots e_r$ is a standard monomial of R/I. □

EXAMPLE 8.9. Let G be the graph



We run the following Macaulay2 program

```
E={
{1,2},  {1,6},  {1,7},  {1,10},  {1,9},
{2,3}, {2,7}, {2,8}, {2,10},
{3,4}, {3,7}, {3,8},
{4,5}, {4,8}, {4,9},
{5,6}, {5,8}, {5,9}, {5,11},
{6,7}, {6,9}, {6,11},
{7,8}, {7,9},
{8,9} };

e=#E;
v=max mingle E;

R=ZZ/2[x_1..x_v];

I=apply(E, t->x_(t_0)*x_(t_1));
I=join(I,apply(1..v, t->x_t^2));
M=matrix{I};

print(hilbertSeries coker M);
```

to obtain the output

```
   4        3        2
2$T  + 21$T  + 30$T  + 11$T + 1
-------------------------------
                  1
```

so we see, for example, that G has two 4-matchings.

EXERCISE 8.10. A clique of size r in a graph G is a complete subgraph $H \subset G$ with r vertices and the rth clique number of G is the number of different cliques of size r in G. Express the sequence of clique numbers of G as the h-vector of a ring associated with G.

9. Weight orders

Throughout this section we let $R = k[x_1, \ldots, x_n]$.

For any $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$. we may define a partial order $<_\lambda$ on the monomials of R by declaring $x^\alpha <_\lambda x^\beta$ if and only if $\alpha \circ \lambda < \beta \circ \lambda$. We will refer to $<_\lambda$ as the *weight order associated with* λ.

DEFINITION 9.1. A term ordering $<$ is *compatible with* $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$ if $<$ is a refinement of $<_\lambda$, i.e., $x^\alpha <_\lambda x^\beta \Rightarrow x^\alpha < x^\beta$.

EXAMPLE 9.2. Let $<'$ be any term ordering in R and assume that $\lambda_1, \ldots, \lambda_n \geq 0$. We may define a new term ordering $<$ as follows:

$$x^\alpha < x^\beta \Leftrightarrow \alpha \circ \lambda < \beta \circ \lambda \text{ or } (\alpha \circ \lambda = \beta \circ \lambda \text{ and } x^\alpha <' x^\beta.)$$

It is not hard to see that $<$ is compatible with λ.

Weight order provide an interesting connection between convex polytopes and Gröbner bases which we will study in a later chapter. The following is an elementary application:

Application: Integer programming. Let $A = (a_{ij})$ be a n by m matrix with integer entries, $b = (b_1, \ldots, b_n) \in \mathbb{Z}^n$ and $c = (c_1, \ldots, c_m)$. We want to find a solution $s = (s_1, \ldots, s_m)$ for the system of equations $A\sigma = b$ for which $c \circ s$ is minimal.

Assume first that the entries of A and b are non-negative. We may rewrite the system of equations as

$$\begin{cases} x_1^{a_{11}\sigma_1 + \ldots a_{1m}\sigma_m} & = & x_1^{b_1} \\ \vdots & & \vdots \\ x_n^{a_{n1}\sigma_1 + \ldots a_{nm}\sigma_m} & = & x_n^{b_n} \end{cases}$$

and if we multiply these equations we end up with

$$(x_1^{a_{11}} x_2^{a_{21}} \ldots x_n^{a_{n1}})^{\sigma_1} \ldots (x_1^{a_{1m}} x_2^{a_{2m}} \ldots x_n^{a_{nm}})^{\sigma_m} = x_1^{b_1} \ldots x_n^{b_n}.$$

To solve this equation we define a homomorphism $\phi : k[y_1, \ldots, y_m] \to k[x_1, \ldots x_n]$ by $\phi(y_i) = x_1^{a_{1i}} x_2^{a_{2i}} \ldots x_n^{a_{ni}}$. We can rewrite our equation as $\phi(y_1^{\sigma_1} \ldots y_m^{\sigma_m}) = x_1^{b_1} \ldots x_n^{b_n}$.

PROPOSITION 9.3. $x_1^{b_1} \ldots x_n^{b_n} \in \operatorname{Im} \phi \Leftrightarrow x_1^{b_1} \ldots x_n^{b_n} = \phi(M)$ *for some monomial* $M \in k[y_1, \ldots, y_m]$.

PROOF. Let $I \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ be the ideal generated by

$$y_1 - x_1^{a_{11}} x_2^{a_{21}} \ldots x_n^{a_{n1}}, \ldots, y_m - x_1^{a_{1m}} x_2^{a_{2m}} \ldots x_n^{a_{nm}}$$

and let G be a Gröbner basis of I with respect to an elimination order for $x_1, \ldots, x_n$. We saw that $x_1^{b_1} \ldots x_n^{b_n} \in \operatorname{Im} \phi$ if and only if $x_1^{b_1} \ldots x_n^{b_n}$ reduces with respect to G to an element of $k[y_1, \ldots, y_m]$.

Since I is generated by binomials we may choose G to consist of binomials. With this choice, each reduction starting with the monomial $x_1^{b_1} \ldots x_n^{b_n}$ will produce a monomial, and, therefore, if $x_1^{b_1} \ldots x_n^{b_n} \xrightarrow[G]{}_+ M$ with $M \in k[y_1, \ldots, y_m]$, M will be a monomial. $\square$

The proof of the previous also gives us an algorithm to solve the system of equations: using the same notation as in the proof find M reduced with respect to G such that $x_1^{b_1} \ldots x_n^{b_n} \xrightarrow[G]{}_+ M$. If $M = y_1^{s_1} \ldots y_m^{s_m} \in k[y_1, \ldots, y_m]$ then $(s_1, \ldots, s_m)$ is a solution, otherwise if $M \notin k[y_1, \ldots, y_m]$ the system of equations has no solution.

If some of the coefficients are negative we use the following standard trick: Introduce a new variable w and let $J \subset k[x_1, \dots, x_n, w]$ be the ideal generated by $wx_1 \dots x_n - 1$. For each $1 \leq j \leq m$ choose non-negative integers $a'_{1j}, \dots, a'_{nj}$ and α_j such that

$$(a_{1j}, \dots, a_{nj}) = (a'_{1j}, \dots, a'_{nj}) + \alpha_j(-1, \dots, -1).$$

Notice that when we work modulo J we have

$$x_1^{a_{1j}} \dots x_n^{a_{nj}} + J = x_1^{a'_{1j}} \dots x_n^{a'_{nj}} w^{\alpha_j} + J.$$

Similarly, we can find $b'_1, \dots, b'_n$ and β such that

$$(b_1, \dots, b_n) = (b'_1, \dots, b'_n) + \beta(-1, -1, \dots, -1)$$

and we have

$$x_1^{b_1} \dots x_n^{b_n} + J = x_1^{b'_1} \dots x_n^{b'_n} w^{\beta} + J.$$

We now have to solve

$$\left(x_1^{a'_{11}} x_2^{a'_{21}} \dots x_n^{a'_{n1}} w^{\alpha_1}\right)^{\sigma_1} \dots \left(x_1^{a'_{1m}} x_2^{a'_{2m}} \dots x_n^{a'_{nm}} w^{\alpha_m}\right)^{\sigma_m} + J = x_1^{b'_1} \dots x_n^{b'_n} w^{\beta} + J.$$

We define a homomorphism $\phi : k[y_1, \dots, y_m] \to k[x_1, \dots x_n]/J$ by $\phi(y_i) = x_1^{a'_{1i}} x_2^{a'_{2i}} \dots x_n^{a'_{ni}} w^{\alpha_j} + J$. We can rewrite our equation as $\phi(y_1^{\sigma_1} \dots y_m^{\sigma_m}) = x_1^{b_1} \dots x_n^{b_n} w^{\beta} + J$.

Since J is generated by a binomial a similar argument as in the proof of proposition 9.3 shows that $x_1^{b'_1} \dots x_n^{b'_n} w^{\beta} + J \in \operatorname{Im} \phi \Leftrightarrow x_1^{b_1} \dots x_n^{b_n} = \phi(M)$ for some monomial $M \in k[y_1, \dots, y_m]$.

We can now solve our original problem.

THEOREM 9.4. *Let $S = k[x_1, \dots, x_n, w, y_1, \dots, y_m]$ and pick an elimination order for $x_1, \dots, x_n, w$ whose restriction to $k[y_1, \dots, y_m]$ refines $<_c$. Let G be a Gröbner basis for the ideal $I \subset S$ generated by*

$$wx_1 \dots x_n - 1, y_1 - x_1^{a'_{11}} x_2^{a'_{21}} \dots x_n^{a'_{n1}} w^{\alpha_1}, \dots, y_m - x_1^{a'_{1m}} x_2^{a'_{2m}} \dots x_n^{a'_{nm}} w^{\alpha_m}.$$

The integer programming problem has a solution if and only if $x_1^{b'_1} \dots x_n^{b'_n} w^{\beta}$ reduces with respcet to G to some monomial $y_1^{\sigma_1} \dots y_m^{\sigma_m}$ of $k[y_1, \dots, y_m]$. If such $y_1^{\sigma_1} \dots y_m^{\sigma_m}$ exists and is reduced to respect to G then $(\sigma_1, \dots, \sigma_m)$ is a solution for the integer programming problem.

PROOF. We need to prove only the last statement.

Let $(\tau_1, \dots, \tau_m)$ be a solution of the integer programming problem and $c \circ (\tau_1, \dots, \tau_m) < c \circ (\sigma_1, \dots, \sigma_m)$.

We have $\phi(y_1^{\sigma_1} \dots y_m^{\sigma_m}) = \phi(y_1^{\tau_1} \dots y_m^{\tau_m})$ hence

$$y_1^{\sigma_1} \dots y_m^{\sigma_m} - y_1^{\tau_1} \dots y_m^{\tau_m} \in \ker \phi = I \cap k[y_1, \dots, y_m]$$

and $y_1^{\sigma_1} \dots y_m^{\sigma_m} - y_1^{\tau_1} \dots y_m^{\tau_m}$ reduces to zero with respect to G. But $y_1^{\sigma_1} \dots y_m^{\sigma_m} - y_1^{\tau_1} \dots y_m^{\tau_m}$ and $y_1^{\sigma_1} \dots y_m^{\sigma_m}$ is reduced with respect to G, a contradiction. $\square$

EXAMPLE 9.5. We find a solution of

$$\begin{cases} 3\sigma_1 - 2\sigma_2 + \sigma_3 - \sigma_4 = -1 \\ 4\sigma_1 + \sigma_2 - \sigma_3 = 5 \end{cases}$$

which minimises $(1,1,1,3) \circ (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$.

We need to solve

$$(x_1^3 x_2^4)^{\sigma_1} (x_2^3 w^2)^{\sigma_2} (x_1^2 w)^{\sigma_3} (x_2 w)^{\sigma_4} + I = x_2^6 w + I.$$

We now need to find a term ordering in $k[x_1, x_2, w, y_1, \dots, y_4]$ which is an elimination order for x_1, x_2, w and whose restriction to $k[y_1, \dots, y_4]$ refines $<_{(1,1,1,3)}$. To achieve this we chose the RevLev order in $k[x_1, x_2, w]$, we declare y_1, y_2 and y_3 to have degree 1 and y_4 to have degree 3, we pick ReVLex in $k[y_1, y_2, y_3, y_4]$ and we take the product of these two orders.

We run

```
R=QQ[x_1..x_2, w, y_1..y_4, MonomialOrder=>ProductOrder{3,4}, Degrees=>{1,1,1,1,1,1,3}];

I=ideal{
    x_1 * x_2 * w - 1_R,
    y_1 - x_1^3 * x_2^4,
    y_2 - x_2^3 * w^2 ,
    y_3 - x_1^2 * w,
    y_4 - x_2 * w};

G= gb I;

print((x_2^6 * w) % G);
```

which produces the output $y_1 y_2^3 y_3^2$.

10. RevLex revisited

We now turn our attention to the properties of the reverse lexicographical term ordering introduced in Example 1.4.

Let R stand for $k[x_1, \ldots, x_n]$ throughout this section and fix the reverse lexicographical term ordering in R. We make the following observation:

PROPOSITION 10.1. *Let $f \in R$ be homogeneous. If x_n^α divides $\mathrm{lp}(f)$ then every term in f is divisible by x_n^α.*

PROOF. Since all the terms in f have the same degree, the term which turns out to be $\mathrm{lp}(f)$ is the term "with the least number of x_n's in it." □

PROPOSITION 10.2. *Let $I \subset R$ be an homogeneous ideal and let $G = \{x_n^{\alpha_1} f_1, \ldots, x_n^{\alpha_s} f_s\}$ be a Gröbner basis for I where none of $f_1, \ldots, f_s$ is divisible by x_n.*

1. *$\{x_n^{(\alpha_1-1)^+} f_1, \ldots, x_n^{(\alpha_s-1)^+} f_s\}$ is a Gröbner basis for $(I : x_n)$ where n^+ stands for $\max\{n, 0\}$.*
2. *$\{f_1, \ldots, f_s\}$ is a Gröbner basis for $(I : x_n^\infty)$.*

PROOF. Notice that since $(I : x_n^\infty) = I : x_n^N$ for some large enough N and since $I : x_n^N = (I : x_n) : x_n \cdots : x_n$ the second statement follows from the first.

Obviously, $\{x_n^{(\alpha_1-1)^+} f_1, \ldots, x_n^{(\alpha_s-1)^+} f_s\} \subset (I : x_n)$. It is enough to show that for any $f \in (I : x_n)$ we have $f \underset{G}{\longrightarrow}_+ 0$. Let $f \in (I : x_n)$ be a counterexample. We may assume that f is homogeneous and we will assume that we have chosen f with minimal leading term. Since $x_n f \in I$ there exists a $1 \le j \le s$ for which $x_n^{\alpha_j} \mathrm{lp}(f_j)$ divides $x_n \mathrm{lp}(f)$.

Since x_n does not divide f_j, the previous proposition tells us that x_n does not divide $\mathrm{lp}(f_j)$ and we deduce that $\mathrm{lp}(f_j)$ must divide $\mathrm{lp}(f)$ and so $x_n^{(\alpha_j-1)^+} \mathrm{lp}(f_j)$ divides $\mathrm{lp}(f)$. But now if $f \xrightarrow[x_n^{(\alpha_j-1)^+} \mathrm{lp}(f_j)]{} g$ then g is a counterexample with $\mathrm{lp}(g) < \mathrm{lp}(f)$.

□

EXERCISE 10.3.
1. Let $I \subset R$ be an homogeneous ideal and let $f \in R$. Use the previous proposition to describe algorithm for computing $(I : f)$.
2. Modify the algorithm in (1) to handle the case where I is not homogeneous.

(3) Let $I \subset R$ be an homogeneous ideal and let $f \in R$ be homogeneous. Describe an algorithm for computing $IR_f \cap R$.

Application: Tight closure. Let k be a field of characteristic $p > 2$. Classify all positive integers a, b for which $S = k[x, y, z]/\langle x^2 - y^a - z^b \rangle$ is F-rational.

We fix the RevLex order in $k[x, y, z]$ with $x > y > z$. Note that for all positive integers e $\{x^2 - y^a - z^b, y^{p^e}, z^{p^e}\}$ is a Gröbner basis for the ideal I_e generated by these elements. We deduce that $(I_e : z^\alpha) = \langle x^2 - y^a - z^b, y^{p^e}, z^{p^e - \alpha} \rangle$ for all $\alpha \geq 0$ and in fact these generators are also a Gröbner basis $\mathcal{G}_e$ for $(I_e : z^\alpha)$.

We now notice that (y, z) is a system of parameters in S and that S is F-regular if and only if $x \notin (y, z)^*$. Also, if p does not divide b then z is in the singular locus of S and z^α is a test element in S for some α. We will assume that p does not divide b.

Combining all this we see that S is F-regular if and only if $x^{p^e} \notin (I_e : z^\alpha) = \langle x^2 - y^a - z^b, y^{p^e}, z^{p^e - \alpha} \rangle$ for infinitely many e.

Write $p^e = 2k+1$. This condition is equivalent with $x(y^a + z^b)^k$ not reducing to zero with respect to $\mathcal{G}_e$. Furthermore, one can see that if this reduces to zero, this will happen without reducing with respect to the element $x^2 - y^a - z^b \in \mathcal{G}_e$.

Since k is not divisible by p, we have shown that S is F-regular if and only if for all $k \gg 0$ one of the terms of $(y^a + z^b)^k$ is not divisible by either y^{p^e} or $z^{p^e - \alpha}$, i.e., for all $k \gg 0$, there exists a $0 \leq i \leq k$ such that

$$\left\{ \begin{array}{lll} ai & < & p^e = 2k+1 \\ b(k-i) & < & p^e - \alpha = 2k + 1 - \alpha \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lll} i & < & \frac{2k+1}{a} \\ \frac{bk - 2k + \alpha - 1}{b} & < & i \end{array} \right. ,$$

and such an i exists if and only if $a < \frac{2b}{b-2}$.

Application: Monomial subideals. Let $I \subset R$ be an ideal. We want to compute the largest monomial ideal $J \subset I$.

PROPOSITION 10.4. *Let $I \subset R$ be an ideal let $S = k[x_1, \ldots, x_n, y_1, \ldots, y_n]$. Let $\phi : R \to S$ be the homomorphism defined by $\phi(x_1) = x_1 y_1, \ldots, \phi(x_n) = x_n y_n$. Then the largest monomial ideal in I is $(\langle \phi(I) \rangle : (y_1 \ldots y_n)^\infty) \cap R$.*

PROOF. If $m \in I$ is a monomial then $m \in \langle \phi(I) \rangle : (y_1 \ldots y_n)^\infty$.

Assume now that $f \in (\langle \phi(I) \rangle : (y_1 \ldots y_n)^\infty) \cap R$. We set a $\mathbb{Z}^n$ grading on S by setting $\deg(x_i) = e_i$ and $\deg(y_i) = -e_i$ where $e_1, \ldots, e_n$ are the standard basis elements. With this grading $\deg(\phi(I))$ is an homogeneous ideal and we may also assume that f is homogeneous with respect to this grading.

We can write

$$y_1^\alpha \ldots y_n^\alpha f = \sum_{i=1}^{s} m_i g_i(x_1 y_1, \ldots, x_n y_n)$$

where $g_1, \ldots, g_s \in \langle \phi(I) \rangle$ and $m_1, \ldots, m_s$ are monomials in S none of then divisible by any $x_j y_j$. But then the fact that all $m_1, \ldots, m_s$ have the same multi-degree implies that they must all be equal. Write $m = m_1, \ldots, m_s$.

Setting $x_1 = \cdots = x_n = 1$ gives us

$$y_1^\alpha \ldots y_n^\alpha f(1, \ldots, 1) = m' \sum_{i=1}^{s} g_i(y_1, \ldots, y_n)$$

and $g = \sum_{i=1}^{s} g_i(y_1, \ldots, y_n)$ must be a monomial; setting $y_1 = \cdots = y_n = 1$ gives us $f(x_1, \ldots, x_n) = m'' g(x_1, \ldots, x_n)$ hence f is a monomial.

$\square$

CHAPTER 2

The geometry of Gröbner bases

1. Initial ideals and flat families

In this section we compare an ideal with its initial ideal. It turns out that is some sense an initial ideal is a continuous deformation of the ideal and one can show that these two share some properties.

Fix $R = k[x_1, \dots, x_n]$ where k is a field and fix a term ordering $<$ in R. We first show that for the purposes of computing the initial ideal of an ideal of I we may replace $<$ with the partial order $<_\lambda$ for some $\lambda \in \mathbb{Z}^n$.

DEFINITION 1.1. Let $P_< \subset \mathbb{Z}^n$ be the cone $\{a - b \,|\, a, b \in \mathbb{Z}^n_{\geq 0}, x^a > x^b\}$.

LEMMA 1.2.

(1) $P_<$ *is a convex cone, i.e., for any* $u, v \in P_<$ *if* $pu + qv \in \mathbb{Z}^n$ *for some* $0 \leq p, q \in \mathbb{Q}$ *then* $pu + qv \in P_<$.

(2) $u \in P_< \Rightarrow -u \notin P_<$ *and in particular* $0 \notin P_<$.

PROOF.

Notice that if $u \in \mathbb{Z}^n$ and $lu \in P_<$ then $u \in P_<$: write $lu = a - b$ with $x^a > x^b$ and assume we chose a and b with disjoint support; then $a = la'$ and $b = lb'$ with $a', b'\mathbb{Z}^n$ and $u = a' - b' \in P_<$.

Assume that for some $u, v \in P_<$ we $pu + qv \in \mathbb{Z}^n$ for some $0 \leq p, q \in \mathbb{Q}$. We may clear denominators and assume that $0 \leq p, q \in \mathbb{Z}$. Write $u = u_1 - u_2$ and $v = v_1 - v_2$ with $x^{u_1} > x_{u_2}$ and $x^{v_1} > x_{v_2}$. Then

$$\begin{cases} x^{pu_1} & > & x^{pu_2} \\ x^{qv_1} & > & x^{qv_2} \end{cases} \Rightarrow x^{pu_1+qv_1} > x^{pu_2+qv_2}.$$

Write $u = a - b$ and $-u = a' - b'$ with $x^a > x^b$ and $x^{a'} > x^{b'}$. Then $(a - a') - (b - b') = 0$ and $x^{a-a'} = x^{b-b'}$, a contradiction.

$\square$

LEMMA 1.3. *Let* $m_1, \dots, m_t, n_1, \dots, n_t$ *be monomials in* R *such that* $m_1 > n_1, \dots, m_t > n_t$. *There exists a* $\lambda \in \mathbb{Z}^n$ *such that* $m_1 >_\lambda n_1, \dots, m_t >_\lambda n_t$.

PROOF. Notice that $m_1 - n_1, \dots, m_t - n_t \in P_<$ and since $0 \notin P_<$ we deduce that 0 is not in the convex hull K of $m_1 - n_1, \dots, m_t - n_t$.

For any $\lambda \in \mathbb{Q}^n$ and any $c \in \mathbb{Q}$ we define the half space $H_{\lambda,c} = \{x \in \mathbb{Q}^n \,|\, \lambda \circ x \geq c\}$. We can write

$$K = \cap_{j \in J} H_{\lambda_j, c_j} \text{ where } \lambda_j \in \mathbb{Z}^n \text{ and } c_j \in \mathbb{Z}$$

and since $0 \notin K$ there exists an hyperplane $\lambda_j \circ x = c_j$ which separates 0 from K, i.e., either $\lambda_j \circ (m_i - n_i) > 0$ for all $1 \leq i \leq t$ or $\lambda_j \circ (m_i - n_i) < 0$ for all $1 \leq i \leq t$. In the first case take $\lambda = \lambda_j$ and in the second take $\lambda = -\lambda_j$. $\square$

THEOREM 1.4. *Let $I \subset R$ be an ideal and let G be a Gröbner basis for I. There exists a finite set $\mathcal{S} = \{(m_1 > n_1), \ldots, (m_t > n_t)\}$ of pairs of monomials with the property that if for some $\lambda \in \mathbb{Z}^n$ we have $\lambda \circ m_1 > \lambda \circ n_1, \ldots, \lambda \circ m_t > \lambda \circ n_t$ then G is a Gröbner basis for I with respect to any term ordering refining $<_\lambda$ and* $\operatorname{in}_< I = \operatorname{in}_{<_\lambda} I$.

PROOF. At every step of the Buchberger algorithm $<_\lambda$ needs to agree with $<$ for a finite set of monomials. Since this process ends after finitely many iterations, we need to find a $<_\lambda$ which agrees with $<$ for finitely many monomials. We may now apply the previous lemma. □

Chose a λ as in the previous theorem. For any monomial $m = x^\alpha \in R$ and any $\lambda \in \mathbb{Z}^n$ we write $\lambda(m) = \lambda \circ \alpha$. Let $S = R[t]$ and for any $g(x_1, \ldots, x_n) \in R$ let $\widetilde{g} = t^b g(t^{-\lambda(x_1)}x_1, \ldots, t^{-\lambda(x_n)}x_n) \in S$ where $b = \max\{\lambda(m) \mid m \text{ is a term in } g\}$.

Then $g = \operatorname{lp}(g) + tg'$ with $g' \in S$. For any ideal $I \subset R$ let $\widetilde{I}$ be the ideal of S generated by $\{\widetilde{g} \mid g \in I\}$. We have $S/(\widetilde{I} + \langle t-1 \rangle) \cong S/I$ and $S/(\widetilde{I} + \langle t \rangle) \cong S/\operatorname{in} I$.

THEOREM 1.5. *$S/\widetilde{I}$ is $k[t]$-free (and hence $k[t]$-flat.)*

PROOF. Choose a λ such that $\operatorname{in}_< I = \operatorname{in}_{<_\lambda}$.

Let B be the set of monomials of R not in $\operatorname{in} I$. Then B is a k-basis of R/I and we now show that B is a $k[t]$-free basis for $S/\widetilde{I}$.

Let ϕ be the automorphism of $R[t, t^{-1}]$ defined by $\phi(x_i) = t^{\lambda(x_i)}x_i$. Notice that $\phi(\widetilde{I}R[t, t^{-1}]) = IR[t, t^{-1}]$.

The elements of B are $k[t, t^{-1}]$-linearly independent elements of $R[t, t^{-1}]/IR[t, t^{-1}]$, so the elements $\phi^{-1}(B)$ are $k[t, t^{-1}]$-linearly independent elements of $R[t, t^{-1}]/\widetilde{I}R[t, t^{-1}]$. But $\phi(b)$ is a unit times b for any $b \in B$, so the elements of B itself are $k[t, t^{-1}]$-linearly independent elements of $R[t, t^{-1}]/\widetilde{I}R[t, t^{-1}]$, and in particular are $k[t]$-linearly independent elements of $R[t]/\widetilde{I}R[t]$.

We now have to show that the $k[t]$-span of B contains, modulo $\widetilde{I}$ all monomials x^α. Assume we may chose x^α not in the $k[t]$-span of B and assume we chose this x^α minimal with respect to $<$. We must have $x^\alpha = \operatorname{lp}(g)$ for some $g \in I$, and $x^\alpha - \widetilde{g}$ is a $k[t]$-linear combination of monomials smaller that x^α, a contradiction. □

CHAPTER 3

Examples and Applications

1. Symmetric polynomials

In this section we write the symmetric polynomial

$$V(x_1,\dots,x_n)=\prod_{1\le i<j\le n}(x_i-x_j)^2=h_n(s_1,\dots,s_n)$$

where $s_1,\dots,s_n$ are the symmetric polynomials

$$s_i=\sum_{1\le j_1\le\cdots\le j_i\le n}x_{j_1}\dots x_{j_i}.$$

We run

```
n=3;
R=QQ[x_1..x_n, s_1..s_n, MonomialOrder=>ProductOrder{n,n}];
I=apply(1..n, u->
    (
    S=subsets(set(1..n), u);
    s_u - sum apply(S, v-> product( apply(toList(v), w-> x_w) ))
    )
);
F=product toList join apply(1..n-1, u-> apply( (u+1)..n, v->x_u-x_v));
G=gb( ideal(I)+ideal(F*F) );
h=selectInSubring(n,gens G);
print h;
```

and obtain the output

```
{0} | s_1^2s_2^2-4s_1^3s_3-4s_2^3+18s_1s_2s_3-27s_3^2 |
```

We also get $h_2=s_1^2-4s_2$,

$$h_4=s_1^2s_2^2s_3^2-4s_1^3s_3^3-4s_1^2s_2^3s_4+18s_1^3s_2s_3s_4-27s_1^4s_4^2-4s_2^3s_3^2+18s_1s_2s_3^3+$$
$$16s_2^4s_4-80s_1s_2^2s_3s_4-6s_1^2s_3^2s_4+144s_1^2s_2s_4^2-27s_3^4+144s_2s_3^2s_4-128s_2^2s_4^2-192s_1s_3s_4^2+256s_4^3$$

and

$h_5=s_1^2s_2^2s_3^2s_4^2-4s_1^3s_3^3s_4^2-4s_1^2s_2^3s_4^3+18s_1^3s_2s_3s_4^3-27s_1^4s_4^4-4s_1^2s_2^2s_3^3s_5+16s_1^3s_3^4s_5+18s_1^2s_2^3s_3s_4s_5-$
$80s_1^3s_2s_3^2s_4s_5-6s_1^3s_2^2s_4^2s_5+144s_1^4s_3s_4^2s_5-27s_1^2s_2^4s_5^2+144s_1^3s_2^2s_3s_5^2-128s_1^4s_3^2s_5^2-192s_1^4s_2s_4s_5^2+256s_1^5s_5^3-$
$4s_2^3s_3^2s_4^2+18s_1s_2s_3^3s_4^2+16s_2^4s_4^3-80s_1s_2^2s_3s_4^3-6s_1^2s_3^2s_4^3+144s_1^2s_2s_4^4+16s_2^3s_3^3s_5-72s_1s_2s_3^4s_5-72s_2^4s_3s_4s_5+$
$356s_1s_2^2s_3^2s_4s_5+24s_1^2s_3^3s_4s_5+24s_1s_2^3s_4^2s_5-746s_1^2s_2s_3s_4^2s_5-36s_1^3s_4^3s_5+108s_2^5s_5^2-630s_1s_2^3s_3s_5^2+560s_1^2s_2s_3^2s_5^2+$
$1020s_1^2s_2^2s_4s_5^2+160s_1^3s_3s_4s_5^2-1600s_1^3s_2s_5^3-27s_3^4s_4^2+144s_2s_3^2s_4^3-128s_2^2s_4^4-192s_1s_3s_4^4+108s_3^5s_5-630s_2s_3^3s_4s_5+$
$560s_2^2s_3s_4^2s_5+1020s_1s_3^2s_4^2s_5+160s_1s_2s_4^3s_5+825s_2^2s_3^2s_5^2-900s_1s_3^3s_5^2-900s_2^3s_4s_5^2-2050s_1s_2s_3s_4s_5^2-50s_1^2s_4^2s_5^2+$
$2250s_1s_2^2s_5^3+2000s_1^2s_3s_5^3+256s_4^5-1600s_3s_4^3s_5+2250s_3^2s_4s_5^2+2000s_2s_4^2s_5^2-3750s_2s_3s_5^3-2500s_1s_4s_5^3+3125s_5^4$

Do we know what h_n is?

EXERCISE 1.1. Looking at h_3 we notice that some of the coefficients are divisible by 2 and some by 3. What happens if we work over $\mathbb{F}_2$ and $\mathbb{F}_3$ instead of $\mathbb{Q}$?

2. Estimating tight closure

Although there is no known algorithm for the computation of tight closure, one can attempt to compute "approximations" to it, which in the author's experience often agree with the correct answer. The purpose of this paper is to describe these calculations and their implementation on Macaulay2.

Tight closure. Let R be a ring of prime characteristic p and let $I \subset R$ be an ideal. For any ideal $I \subset R$ and positive integer e, $I^{[p^e]}$ will stand for the ideal generated by p^eth powers of elements in I. Let R^0 be the set of all elements of R which are not in any minimal prime. We define the *tight closure of* I, I^*, as all $a \in R$ such that for some $c \in R^0$ we have $ca^{p^e} \in I^{[p^e]}$ for all large e. We refer the reader to [**HH**] and [**H**] for a systematic description of tight closure and its properties.

Educated guesses for tight closure of ideals. We now fix k to be a field of prime characteristic p and we let $R = k[x_1, \dots, x_n]/J$ for some ideal $J \subset k[x_1, \dots, x_n]$. For all positive integers e we let ϕ_e to be the Frobenius map $R \to R$ sending an element $r \in R$ to r^{p^e}. We will represent ideals in R by their preimages in $k[x_1, \dots, x_n]$. In this down-to-earth setup, given an ideal $I \subset R$ we can write

$$I^* = \bigcup_{c \in R^0} \bigcup_{e_0 \geq 0} \bigcap_{e \geq e_0} \phi_e^{-1} \left((J + I^{[p^e]} : c) \right) \tag{1}$$

Although tight closure has some very nice properties, this definition suggests that constructibility is not one of them.

There is, however, one simplification which can be made in (1):

THEOREM 2.1. *Let $V(\mathcal{S})$ be the singular locus of R. Then for every $c \in \mathcal{S}$ there exists a positive integer N such that for all ideals $I \subset R$, $a \in I^*$ if and only if $a^{p^e} \in (I^{[p^e]} :_R c^N)$ for all large e.*

The element c^N is the statement of this theorem is called a *test element.* (In fact, we need something much weaker than a test element: we want c^N to work for *one* given ideal; the existence of this element follows from the fact that tight closure is trivial in the regular ring R_c.)

Given a quotient of a polynomial ring R, $\mathcal{S}$ is easily computed by the Jacobian criterion. Fixing a $c \in \mathcal{S}$ with sufficiently large degree, we can now write

$$I^* = \bigcup_{e_0 \geq 0} \bigcap_{e \geq e_0} \phi_e^{-1} \left((J + I^{[p^e]} : c) \right) \tag{2}$$

A Macaulay2 implementation. Here is a program to find the tight closure of the image of the ideal generated by x_2 and x_3 in the ring $\mathbb{Z}/2\mathbb{Z}[x_1, x_2, x_3]/ < x_1^3 - x_2^5 - x_3^7 >$

```
p=2;
n=3;
R=ZZ/p[x_1..x_n, X_1..X_n, MonomialOrder=>Lex, MonomialSize=>16];

J=ideal(x_1^3-x_2^5-x_3^7);
I=(x_2,x_3);

testElement=x_3^20;

TightClosure=ideal(1_R);
e=1;
```

```
while (p^e<10000) do
{
    q=p^e;
    I1=J+ideal(apply(I,u->u^q));
    I2=I1 : testElement;
    I3=I2+ideal(apply(1..n, u->X_u - x_u^q));

    G=gens gb I3;
    tc=selectInSubring(n,G);
    TightClosure=intersect(TightClosure,ideal(tc));
    print tc;
    e=e+1;
};

subs=toList( apply(1..n, u->X_u => x_u) );
TightClosure= substitute(mingens TightClosure,subs) ;
<< "The tight closure seems to be " << TightClosure;
```

This will produce the output

```
{0} | 1 |
{0} | 1 |
{0} | 1 |
{0} | 1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1 |
The tight closure seems to be {0} | x_3 x_2 x_1 |
```

The first lines correspond are the values of $\phi_e^{-1}\left((J + I^{[p^e]} : c)\right)$ from (1) for $e = 1 \ldots 13$.

If we change the value of p to 11 we get

```
{0} | 1 |
{0} | X_3 X_2 X_1 |
{0} | X_3 X_2 X_1^2 |
The tight closure seems to be {0} | x_3 x_2 x_1^2 |
```

Since we are working in a domain (as long as $p \neq 3$) Theorem 1.3b in [**H**] guarantees that the tight closure is contained in the ideal generated by x_1^2, x_2, x_3.

3. A resultant Variety

The background for this example can be found in [**K1**].

Let k be a field of characteristic$\neq 2$, and consider the binary quadratic forms $f_1 = a_0x^2 + 2a_1xy + a_2y^2$, $f_2 = b_0x^2 + 2b_1xy + b_2y^2$ and $f_3 = c_0x^2 + 2c_1xy + c_2y^2$. We can think of these as polynomials in $k[a_0, a_1, a_2, b_0, b_1, b_2, c_0, c_1, c_2][x, y]$. We have an action of $\mathrm{GL}_2(k)$ on the polynomial ring $R = k[a_0, a_1, a_2, b_0, b_1, b_2, c_0, c_1, c_2]$ induced by linear changes of variables in the f's. The polynomials $r_1 = \mathrm{Res}(f_1, f_2), r_2 = \mathrm{Res}(f_1, f_3), r_3 = \mathrm{Res}(f_2, f_3)$ and $r_4 = \mathrm{Res}(f_1 + f_2, f_3)$ are joint invariants of this action. The simultaneous vanishing of these resultants define the variety (in k^9) of forms f_1, f_2, f_3 with a common non-trivial zero.

Let $I \subset R$ be the ideal generated by r_1, r_2, r_3 and r_4. When k has prime characteristic $p \neq 2$ one can show that if for some positive integer n we have

$$(r_1 r_2 r_3 r_4)^n \in \langle r_1^{n+1}, r_2^{n+1}, r_3^{n+1}, r_4^{n+1} \rangle \tag{1}$$

then $\mathrm{H}^4_I(R) = 0$.

This problem is too big for our computers!

To solve it we'll have to simplify it as follows. We noted that r_1, r_2, r_3 and r_4 are joint invariants of f_1, f_2, f_3. These joint invariants are well known. In characteristic zero they form the subalgebra of R generated by

$$B_{11} = 2a_1^2 - a_0 a_2 - a_2 a_0$$
$$B_{22} = 2b_1^2 - b_0 b_2 - b_2 b_0$$
$$B_{33} = 2c_1^2 - c_0 c_2 - c_2 c_0$$
$$B_{12} = 2a_1 b_1 - a_0 b_2 - a_2 b_0$$
$$B_{13} = 2a_1 c_1 - a_0 c_2 - a_2 c_0$$
$$B_{23} = 2b_1 c_1 - b_0 c_2 - b_2 c_0$$
$$B_{123} = a_2 b_1 c_0 - a_1 b_2 c_0 - a_2 b_0 c_1 + a_0 b_2 c_1 + a_1 b_0 c_2 - a_0 b_1 c_2$$

Although we are working in positive characteristic we can try and see if our resultants are there (it makes sense– resultants are joint invariants regardless of the characteristic.)

```
F=QQ;

R=F[a_0..a_2, b_0..b_2, c_0..c_2,
B_11, B_12, B_13, B_22, B_23, B_33, B_123,
MonomialOrder=>ProductOrder{9,7}];

JointInvariants={
B_11-(2*a_1^2 - a_0*a_2 - a_2*a_0),
B_22-(2*b_1^2 - b_0*b_2 - b_2*b_0),
B_33-(2*c_1^2 - c_0*c_2 - c_2*c_0),
B_12-(2*a_1*b_1 - a_0*b_2 - a_2*b_0),
B_13-(2*a_1*c_1 - a_0*c_2 - a_2*c_0),
B_23-(2*b_1*c_1 - b_0*c_2 - b_2*c_0),
B_123-(a_2*b_1*c_0- a_1*b_2*c_0- a_2*b_0*c_1+ a_0*b_2*c_1+ a_1*b_0*c_2- a_0* b_1* c_2)
};


r1=matrix{{a_0, 2*a_1, a_2,0}, {0, a_0, 2*a_1, a_2}, {b_0, 2*b_1, b_2,0}, {0, b_0, 2*b_1, b_2}};
r2=matrix{{a_0, 2*a_1, a_2,0}, {0, a_0, 2*a_1, a_2}, {c_0, 2*c_1, c_2,0}, {0, c_0, 2*c_1, c_2}};
r3=matrix{{c_0, 2*c_1, c_2,0}, {0, c_0, 2*c_1, c_2}, {b_0, 2*b_1, b_2,0}, {0, b_0, 2*b_1, b_2}};
r4=matrix{{a_0+b_0, 2*a_1+2*b_1, a_2+b_2,0}, {0, a_0+b_0, 2*a_1+2*b_1, a_2+b_2},
{c_0, 2*c_1, c_2,0}, {0, c_0, 2*c_1, c_2}};

d1=det r1; d2=det r2; d3=det r3; d4=det r4;
```

```
G=gb (ideal(JointInvariants));
d1=d1%G; d2=d2%G; d3=d3%G; d4=d4%G;
apply({d1,d2,d3,d4}, print);
```

This produces the following pleasant output:

```
 2
B    - B  B
 12    11 22
 2
B    - B  B
 13    11 33
 2
B    - B  B
 23    22 33
 2               2
B    + 2B  B   + B    - B  B    - 2B  B    - B  B
 13      13 23    23    11 33     12 33    22 33
```

So our resultants live in the in the subring generated by the B's and there they are rather uncomplicated expressions.

We now check the sysygies on the fundamental joint invariants:

```
print ( selectInSubring(9, gens G) );
```

we see

```
{0} | B_13^2B_22-2B_12B_13B_23+B_11B_23^2+B_12^2B_33-B_11B_22B_33-2B_123^2 |
```

so we may work in the polynomial ring on $B_{i,j}$ for $1 \leq i \leq j \leq 3$.

So far so good– now we re-run this with a finite field, say with $F = \mathbb{Z}_{101}$, and we try

```
S=ZZ/101[B_11, B_12, B_13, B_22, B_23, B_33, B_123];
d1=substitute(d1,S); d2=substitute(d2,S); d3=substitute(d3,S); d4=substitute(d4,S);

n=3;
G1=gb( ideal(d1^n, d2^n, d3^n, d4^n) );
print ((d1*d2*d3*d4)^(n-1)%G1);
```

The answer is 0!

We try this in a few other characteristics p and notice that $n = 3$ works. This is good evidence that (1) holds– and if fact one can prove this using local cohomology– Is there an elementary proof for this?

4. How many squares in an infinite chess board can a knight reach in d moves?

In this section we illustrate a powerful enumeration technique. We will apply this method to solve the following problems: how many squares can a knight in an infinite chess board reach in d moves? how many squares can be reached in d moves and no less moves? We will denote the first number with $f(d)$ and the second with $g(d)$.

Let k be any field and let R be the k-subalgebra of $k[x_1, x_2, x_1^{-1}, x_2^{-1}]$ generated by

$$M = \left\{x_1 x_2^2, x_1^2 x_2, x_1^{-1} x_2^2, x_1^{-2} x_2, x_1 x_2^{-2}, x_1^2 x_2^{-1}, x_1^{-1} x_2^{-2}, x_1^{-2} x_2^{-1}\right\}.$$

The first step towards the solution of this problem is to realize that $f(d)$ is the cardinality of $M^d := \{a_1 \dots a_d | a_1, \dots, a_d \in M\}$ while $g(d)$ is the number of elements in M^d but not in M^i for $i < d$.

We can produce a presentation for R by mapping a polynomial ring $S = k[y_1, \dots, y_8]$ to R by $y_i \to m_i$ where m_i is the ith element of M. Let K be the kernel of this map. This kernel can be computed effectively as follows: let I be the ideal of $k[u, x_1, x_2, y_1, \dots, y_8]$ generated by

$$\{ux_1x_2 - 1, y_1 - x_1x_2^2, y_2 - x_1^2x_2, y_3x_1 - x_2^2, y_4x_1^2 - x_2,$$
$$y_5x_2^2 - x_1, y_6x_2 - x_1^2, y_7x_1x_2^2 - 1, y_8x_1^2x_2 - 1\}$$

and fix an elimination order where u, x_1, x_2 are the largest variables. Then K is generated by the elements of a Gröbner basis for I which do not contain the variables u, x_1, x_2 (cf. chapter 1 of [**S**].) Recall also that K is a binomial ideal.

Let H be the ideal of S generated by all homogeneous elements in K. The elements of H are the elements of the homogenization of K with respect to a new variable, say t, which do not involve t, thus we can compute H by homogenizing a Gröbner basis for K using a graded lexicographic order (cf. exercise 1.6.19 in [**AL**]) and eliminating the variable t.

H is a binomial ideal and it is easy to see that the set of monomials of degree d in S which are not in H correspond bijectively to the elements of M^d, thus we obtain that $F(t) := \sum_{d=0}^{\infty} f(d)t^d$ is the Hilbert series of S/H. A computation with Macaulay2 shows that

$$F(t) = \frac{1 + 5t + 12t^2 - 8t^4 + 4t^5}{(1-t)^3}$$

and that the Hilbert polynomial of S/H is $1 + 4d + 7d^2$. Since the a invariant of S/H is 2 we see that

$$f(d) = \begin{cases} 1 & d = 0 \\ 8 & d = 1 \\ 33 & d = 2 \\ 1 + 4d + 7d^2 & d \geq 3 \end{cases}$$

We fix now a monomial order in S refining the degree order. Its easy to see that the set of monomials of degree d in S which do not reduce with respect to a Gröbner basis for K correspond bijectively to the elements of M^d which are not in any M^i for $i < d$, thus we obtain that $G(t) := \sum_{d=0}^{\infty} g(d)t^d$ is the Hilbert series of $S/in(K)$. A computation with Macaulay2 shows that

$$G(t) = \frac{1 + 6t + 17t^2 + 12t^3 - 8t^4 - 4t^5 + 4t^6}{(1-t)^2}$$

and that the Hilbert polynomial of $S/in(K)$ is $28d - 20$. Since the a-invariant of $S/in(K)$ is 4 we have

$$g(d) = \begin{cases} 1 & d = 0 \\ 8 & d = 1 \\ 32 & d = 2 \\ 68 & d = 3 \\ 96 & d = 4 \\ 28d - 20 & d \geq 5 \end{cases}$$

The general method. We now give an algorithm for enumerating monomials in monomial k-algebras.

Let $x = (x_1, \dots, x_n)$ be a sequence of indeterminates, and for a sequence of non-negative integers $\alpha = (\alpha^{(1)}, \dots, \alpha^{(n)})$ let $x^\alpha = x_1^{\alpha^{(1)}} \dots x_n^{\alpha^{(n)}}$.

Let

$$M = \left\{x^{\alpha_1 - \beta_1}, \dots, x^{\alpha_m - \beta_m}\right\} \subset k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$$

where each α_i and β_i is a non-negative integer multi-index.

As before, let $f(d)$ be the cardinality of M^d and let $g(d)$ be the cardinality of $M^d - \cup_{i=0}^{d-1} M^i$.

We can also interpret $f(d)$ and $g(d)$ as follows: let A be a n by m matrix whose ith column is $\alpha_i - \beta_i$. Let v stand for a m by 1 column vector with non-negative integer entries. Then $f(d)$ is the cardinality of the set $A_d := \{Av| \, \|v\|_\infty = d\}$ while $g(d)$ is the cardinality of $A_d - \cup_{i=0}^{d-1} A_i$.

We now produce $f(d)$ and $g(d)$ together with their generating functions. Let I be the ideal of $k[u, x_1, \ldots, x_n, y_1, \ldots, y_m]$ generated by $ux_1 \ldots x_n$ and $\{y_i x^{\beta_i} - x^{\alpha_i} | 1 \le i \le m\}$ and let $K = I \cap k[y_1, \ldots, y_m]$. Let $H' \subset k[t, y_1, \ldots, y_m]$ be the homogenization of K with respect to t and let $H = H' \cap k[y_1, \ldots, y_m]$.

The generating function of $f(d)$ is given by the Hilbert series of $k[y_1, \ldots, y_m]/H$ while $f(d)$ equals the value of the Hilbert polynomial of $k[y_1, \ldots, y_m]/H$ for all d larger than the a-invariant of $k[y_1, \ldots, y_m]/H$ (=the degree of the Hilbert series as a rational function.)

Fix a monomial order in $[y_1, \ldots, y_m]$ refining the degree order; $g(d)$ and its generating function are produced similarly replacing H with $in(K)$.

A Macaulay2 implementation. The following is a Macaulay2 program for the original enumeration problem:

```
R=ZZ/101[u,a,b,y_{1}..y_{8},MonomialOrder=>Lex];
I={u*a*b-1_R,y_{1}-a*b^2,y_{2}-a^2*b,y_{3}*a-b^2,y_{4}*a^2-b,
y_{5}*b^2-a,y_{6}*b-a^2,y_{7}*a*b^2-1_R,y_{8}*a^2*b-1_R};
G=gens gb ideal I;
J=selectInSubring(3,G);

S1=ZZ/101[y_{1}..y_{8},t];
J=substitute(J,S1);
H0=homogenize(gens gb J,t);

S2=ZZ/101[t,y_{1}..y_{8},MonomialOrder=>Lex];
H0=substitute(H0,S2);
G=gens gb ideal H0;
H=selectInSubring(1,G);

S=ZZ/101[y_{1}..y_{8}];
J=substitute(J,S);
H=substitute(H,S);
print(hilbertSeries coker J);
print(hilbertPolynomial(coker J, Projective=>false));
print(hilbertSeries coker H);
print(hilbertPolynomial(coker H, Projective=>false));
```

This produces the following output:

```
   6     5     4      3      2
4$T -4$T -8$T +12$T +17$T +6$T+1
--------------------------------
                     2
            (-$T+1)
28$i-20
   5     4      2
4$T -8$T +12$T +5$T+1
---------------------
              3
```

```
       (-$T+1)
   2
7$i +4$i+1
```

Bibliography

[AL] W. W. Adams and P. Loustaunau. *An introduction to Gröbner bases,* Graduate Studies in Mathematics, **3**, American Mathematical Society, Providence, RI, 1994.

[BH] W. Bruns and J. Herzog. *Cohen-Macaulay rings,* Cambridge Studies in Advanced Mathematics, **39**, Cambridge University Press, Cambridge, 1993.

[CLO1] D. Cox, J, Little and D. O'Shea. *Using algebraic geometry,* Graduate Texts in Mathematics, **185** Springer-Verlag, New York, 1998.

[CLO2] D. Cox, J, Little and D. O'Shea. *Ideals, varieties and algorithms,* Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[E] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry.* Graduate Texts in Mathematics, **150** Springer-Verlag, New York, 1995.

[H] C. Huneke, *Tight closure and its applications*, CBMS Regional Conference Series in Mathematics, **88**.

[HH] M. Hochster and C. Huneke, *Tight closure, invariant theory, and the Briançon-Skoda theorem*, J. Amer. Math. Soc. **3** (1990), 31–116.

[K1] M. Katzman. *The cohomological dimension of a resultant variety in prime characteristic p.* J. Algebra 191 (1997), no. 2, 510–517.

[GS] D. Grayson and M. Stillman: Macaulay 2 – a software system for algebraic geometry and commutative algebra, available at `http://www.math.uiuc.edu/Macaulay2`.

[S] B. Sturmfels. *Gröbner bases and convex polytopes, University Lecture Series,* **8**, American Mathematical Society, Providence, RI 1996