When and Why Are Gröbner Bases Hard to Compute?

Reijnders, Luuk E.R.M.

Award date:
2021

When and Why Are Gröbner Bases Hard to Compute?

Author
L.E.R.M. Reijnders 1367862 Applied Mathematics

Supervisor
R.H. Eggermont

Eindhoven University of Technology
Department of Applied Mathematics
2WH40 Bachelor Final Project

Friday 23rd July, 2021
Eindhoven University of Technology

Abstract

In this report I investigate the difficulties that come with computing Gröbner bases, hoping to come to a deeper understanding of what causes these difficulties to occur in the first place. The first topic covered are some of the most notable Gröbner basis algorithms. Buchberger's algorithm, as well as Faugère's F_4 and F_5 algorithms will be briefly explained. Afterwards, I take a look at how Gröbner bases are easy to determine in both the linear and single variable case. Next I take an in depth look at two ideals with complex Gröbner basis, proving their complexity. In the final section of the report, I investigated what happens to Gröbner bases under symmetry. This symmetry specifically being on the variables. So, in addition to a starting polynomial in a generating set, e.g. $x^2 + y$, I will also consider the polynomial $y^2 + x$ to be in the generating set in this case. Symmetry results in more polynomials generating the ideal, which in turn might allow for more cancellation, meaning more leading terms, and, possibly, simpler Gröbner bases.

Contents

1 Introduction

Gröbner bases are a concept from the field of Computational Algebra. A Gröbner basis is a generating set for an ideal in a multivariate polynomial ring with specific properties. They are, in a way, a multivariate version of both the greatest common divisor for single variate polynomial rings and Gaussian elimination for linear polynomials. The specific properties that Gröbner bases possess make them very useful for solving various mathematical problems that can be related back to polynomials. Some examples include:

- Solving polynomial equations
- Automatic geometric proofs
- Error-correcting codes

Gröbner bases were first introduced by Buchberger in his PhD thesis [1]. In his thesis, Buchberger also presented an algorithm for computing these Gröbner bases, aptly named Buchberger's algorithm. However, the computation of Gröbner bases using this algorithm turned out to be rather intensive. Later results showed that, when considering polynomials with degree less than or equal to d in n variables, the degrees of the polynomials involved in computing Gröbner bases could grow as large as d^{2^n} [2]. While results like this initially brought into question the viability of Gröbner bases in practice, further research lead to more positive conclusions [3]. Additionally different algorithms have been created, which have considerably faster computation times. The most notable algorithms being Faugére's F4 and F5 algorithms [4, 5].

Despite all these improvements, Gröbner basis computation remains intensive. So, while they are certainly useful, one has to wonder in what cases the computation takes an excessively long time, and why this is. A better understanding of when and why a computation might take a long time would be of great use in deciding when to apply Gröbner bases to a given problem, and might even lead to ideas for improved algorithms. For this reason I will be looking into when and why Gröbner bases are hard to compute, for my bachelor final project.

The main notion of complexity for Gröbner bases that will be focused on, is the degree of the polynomials in the Gröbner basis. This is because it is easier to work with compared to, for instance, the total number of polynomials in a Gröbner basis. It is not hard to see that large degree polynomials in a Gröbner basis implies it must contain many too, this follows from Buchberger's algorithm.

This report will be split into several sections. First I reintroduce some prerequisite mathematical knowledge. After that I will talk about some of the most relevant algorithms for Gröbner basis computation. Their strengths will be highlighted and I will touch on some of the problems that occur despite optimizations. Then, some simple cases will be discussed. Afterwards, I will look at some examples of ideals that have particularly hard to compute Gröbner bases, and explain what makes them so hard to compute. Finally, what happens when some kind of symmetry is applied will be discussed. In particular, symmetry applied to the variables.

2 Mathematical Background

To start, I have to cover the mathematical background behind Gröbner bases and related topics. Many theorems will be given without direct proof, and instead I will refer to proofs given in the book "Ideals, Varieties, and Algorithms" by Cox, Little and O'shea [3].

2.1 Some Notation

Before we begin some notation needs to be defined and/or clarified.

- We use $\mathbb{N}$ to denote the set of all non-negative integers $\{0, 1, \dots\}$. In particular note that 0 is included in this set.
- Consider a monomial in some polynomial ring $k[x_1, \dots, x_n]$. We use the following compact notation: $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, with $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. Additionally, I will sometimes refer to x^α by simply α.
- For a monomial we call $|\alpha| = \sum_{i=1}^n \alpha_i$ the total degree of α.

2.2 Ideals

Definition 2.2.1 (Ideal)**.** Given a commutative ring R, a non-empty additive subset $I \subset R$ is called an ideal if:

$$\forall_{r \in R,\ a \in I} : a * r \in I.$$

In particular we will concern ourselves with the case where $R = k[x_1, \dots, x_n]$ is a polynomial ring with the usual addition and multiplication.

Definition 2.2.2 (Ideal Generated by Polynomials)**.** Let $F = \{f_1, \dots, f_m\} \subset k[x_1, \dots, x_n]$, we define the ideal generated by F:

$$\langle F \rangle = \left\{ \sum_{i=1}^m g_i f_i \mid \forall_i\ g_i \in k[x_1, \dots, x_n] \right\}$$

It can be easily verified that this is indeed an ideal.

Next are some important that will be used. First, we have the Hilbert Basis Theorem. Proof can be found on pages 77-78 of Ideals, Varieties, and Algorithms [3] (Theorem 4).

Theorem 2.2.3 (Hilbert Basis Theorem)**.** *Let $I \subset k[x_1, \dots, x_n]$ be an ideal. Then there exists a finite set $G = \{g_1, \dots, g_m\} \subset I$ such that $\langle G \rangle = I$. I.e. every ideal I has a finite generating set G.*

Another theorem is the ascending chain condition, proof of which can be found on page 80 of Ideals, Varieties, and Algorithms [3] (Theorem 7).

Theorem 2.2.4 (The Ascending Chain Condition)**.** *Let $(I_n)_{n \in \mathbb{N}}$ be an increasing sequence of ideals in $k[x_1, \dots, x_n]$ (i.e. $\forall_{n \in \mathbb{N}} : I_n \subset I_{n+1}$). Then there exists an N such that for all $n, m \geq N$ we have $I_n = I_m$.*

2.3 Monomials

Recall the shorthand notation for monomials and observe that α fully defines the monomial x^α. This means that the monoid (i.e. a group without inverses) of monomials in $k[x_1, \dots, x_n]$ with multiplication is isomorphic to the monoid $\mathbb{N}^n$ with addition. We use this fact to define a monomial ordering in terms of α in $\mathbb{N}^n$.

Definition 2.3.1 (Monomial Ordering)**.** A monomial ordering ">" is a relation on the monomials of some polynomial ring $k[x_1, \dots, x_n]$, or alternatively a relation on $\mathbb{N}^n$, with the following properties:

1. $>$ is a total ordering on $\mathbb{N}^n$.
2. If $\alpha, \beta, \gamma \in \mathbb{N}^n$ and $\alpha > \beta$ then also $\alpha + \gamma > \beta + \gamma$.
3. $>$ is a well-ordering on $\mathbb{N}^n$.

Before we continue there are a two frequently used monomial orderings that need to be defined.

Definition 2.3.2 (Graded Lexicographic Order (grlex))**.** Given two monomials with exponents $\alpha, \beta \in \mathbb{N}^n$, we say $\alpha > \beta$ if either:

- $|\alpha| > |\beta|$
- $|\alpha| = |\beta|$ and for the smallest i such that $\alpha_i \neq \beta_i$ we have $\alpha_i > \beta_i$.

Definition 2.3.3 (Graded Reverse Lexicographic Order (grevlex))**.** Given two monomials with exponents $\alpha, \beta \in \mathbb{N}^n$, we say $\alpha > \beta$ if either:

- $|\alpha| > |\beta|$
- $|\alpha| = |\beta|$ and for the largest $i \leq n$ such that $\alpha_i \neq \beta_i$ we have $\alpha_i < \beta_i$.

Grlex can be (roughly) interpreted as considering which monomial put the most of its "total degree" into the higher ranked variable. Grevlex on the other hand can be (roughly) interpreted as considering which monomial put the least of its "total degree" into the lower ranked variable.

Remark. Grevlex ordering in particular will be used frequently in this report. This is because it is a particularly good ordering for computing Gröbner bases.

Example 2.3.4 (Monomial Orders)**.** We consider two monomials in $k[x, y, z]$ with $x > y > z$:

- First $x^\alpha = y^2 z$ and $x^\beta = x^2$. Since $|\alpha| = 3 > 2 = |\beta|$ we find $\alpha >_{grlex} \beta$ and $\alpha >_{grevlex} \beta$.
- Next consider the two monomials $x^\alpha = x^2 z$ and $x^\beta = xy^2$. First grlex ordering tells us $\alpha >_{\text{grlex}} \beta$ because $|\alpha| = |\beta|$ and $\alpha_1 > \beta_1$. On the other hand grevlex order tells us $\alpha <_{\text{grevlex}} \beta$ because $|\alpha| = |\beta|$ and $\alpha_3 > \beta_3$.

Now that we have defined a monomial ordering we can use this to define several useful terms:

Definition 2.3.5 (Leading Term, Monomial and Coefficient)**.** Given a monomial ordering ">", and a polynomial $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \ldots, x_n]$. Consider the α with $c_\alpha \neq 0$ such that $\alpha > \beta$ for all $\beta \in \mathbb{N}^n$ where $c_\beta \neq 0$. Then:

1. We call $c_\alpha x^\alpha$ the leading term of f and denote it by $\text{LT}(f)$.
2. We call x^α the leading monomial of f and denote it by $\text{LM}(f)$.
3. We call c_α the leading coefficient of f and denote it by $\text{LC}(f)$.

As a generalisation, if $F = \{f_1, \ldots, f_m\} \subset k[x_1, \ldots, x_n]$. Then we define

$$\text{LT}(F) := \{cx^\alpha \mid \text{LT}(f_i) = cx^\alpha \text{ for some } i\}.$$

Remark. For some polynomial f, I refer to $\big|\text{LT}(f)\big|$ as the total degree, or just "degree", of f. Similarly, when referring to the (total) degree of a set of polynomials F, I am talking about $\max\{\big|\text{LT}(f)\big| \mid f \in F\}$.

Example 2.3.6. Let $f = 2y^2 z + 3x^2 + z \in k[x, y, z]$. We use grlex order with $x > y > z$, then:

- $\text{LT}(f) = 2y^2 z$
- $\text{LM}(f) = y^2 z$.

- $\mathrm{LC}(f) = 2$.

In addition to the total degree, $|\alpha|$, another useful definition is the variable specific degree.

Definition 2.3.7 (Variable Specific Degree)**.** Let x^α be a monomial in $k[x_1, \ldots, x_n]$ We define:

$$\phi(x^\alpha, x_i) = \mathrm{Deg}_{x_i}(x^\alpha) = \max\{m \in \mathbb{N} \mid x_i^m \text{ divides } x^\alpha\}$$

In essence this tells us what power of a certain variable appears in the monomial.

Example 2.3.8. Let $\alpha = x^4y$ be a monomial in $k[x, y, z]$, then:

$$\phi(f, x) = 4$$
$$\phi(f, y) = 1$$
$$\phi(f, z) = 0$$

2.4 Polynomial Division

Definition 2.4.1 (Divisibility)**.** Let $f, g \in k[x_1, \ldots, x_n]$. We say f is divisible by g if there exists a polynomial $h \in k[x_1, \ldots, x_n]$ such that $f = g \cdot h$.

The following theorem on the division algorithm can be found on page 64 of Ideals, Varieties, and Algorithms [3] (Theorem 3), along with a proof.

Theorem 2.4.2 (Division with Remainder)**.** *Fix a monomial ordering $>$, and an ordered tuple of polynomials $F = (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$ For any polynomial $g \in k[x_1, \ldots, x_n]$ there are $q_i, r \in k[x_1, \ldots, x_n]$ for all i, such that no element of $LT(F)$ divides any term of r and:*

$$g = q_1 f_1 + \cdots + q_m f_m + r$$

with the total degree of every term $q_i f_i$ not being larger than that of g. Note that the q_i and r are not unique.
In particular there is an algorithm that computes r and the q_i in question.
The algorithm (as seen in [3]) is as follows:

Algorithm 1: Division Algorithm in $k[x_1, \ldots, x_n]$

input : $F = (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$, $g \in k[x_1, \ldots, x_n]$
output: $q_1, \ldots, q_m, r \in k[x_1, \ldots, x_n]$

```
for i ∈ [1, m] do
    q_i = 0
r = 0
p = g
while p ≠ 0 do
    i = 1
    NoDiv = True
    while i ≤ m and NoDiv do
        if LT(f_i) divides LT(p) then
            q_i = q_i + LT(p)/LT(f_i)
            p = p − (LT(p)/LT(f_i)) f_i
            NoDiv = False
        else
            i = i + 1
    if NoDiv then
        r = r + LT(p)
        p = p − LT(p)
return q_1, ..., q_m, r
```

We write $\overline{g}^F = r$ for r computed using this algorithm.

Definition 2.4.3 (Reduction to 0)**.** Given a monomial order, a subset $F = \{f_1, \ldots, f_m\} \subset k[x_1, \ldots, x_n]$ and a polynomial $g \in [x_1, \ldots, x_n]$ we say g reduces to 0 modulo F if there exist $h_1, \ldots, h_m \in k[x_1, \ldots, x_n]$ such that:

1. $g = h_1 f_1 + \ldots + h_m f_m$
2. multidegree$(g) \geq$ multidegree$(h_i f_i)$ $\forall_{i \in [1,m]}$

We write $g \to_F 0$.

Remark. Note that while $\overline{g}^F = 0$ and $f \to_G 0$ seem very similar in definition, they truly mean different things. $\overline{g}^F = 0$ implies the reduction algorithm returns a representation with remainder 0, whereas $f \to_G 0$ only implies such a representation exists. In particular $\overline{g}^F = 0 \implies f \to_G 0$, but the inverse need not be true. To illustrate this, consider the following example:

Example 2.4.4. Let $F = (xy+1, y+1)$, and $g = xy + x$. Clearly $g = x \cdot (y+1) + 0 \cdot (xy+1)$, with multidegree$(g) = 2 \geq 2 =$ multidegree$(x(y+1))$ thus $g \to_F 0$. However, if we apply the division algorithm we find: $g = 1 \cdot (xy+1) + 0 \cdot (y+1) + x - 1$. In other words $\overline{g}^F = x - 1 \neq 0$.

Definition 2.4.5 (Greatest Common Divisor)**.** The greatest common divisor, or gcd for short, of a set of polynomials $F \subset k[x_1, \ldots, x_n]$, with $F \neq \{0\}$ is the unique polynomial $h \in k[x_1, \ldots, x_n]$ such that:

1. h divides all $f \in F$.
2. if some p also divides all $f \in F$, then p must divide h too.
3. LC$(h) = 1$

We denote $\gcd(F) = h$. If $F = \{0\}$, then we say $\gcd F = 0$

The extended Euclidean algorithm for polynomials works much the same as it does for integers. An explanation and proof of how it works can be found in Ideals, Varieties, and Algorithms [3] (Proposition 8, page 44).

Theorem 2.4.6 (Extended Euclidean Algorithm)**.** *There exists an algorithm, called the extended euclidean algorithm, such that for a set of polynomials $F = \{f_1, \ldots, f_m\} \subset k[x]$ we can find $g_1, \ldots, g_m \in k[x]$ such that:*

$$\gcd(F) = f_1 g_1 + \ldots + f_m g_m$$

2.5 Gröbner Bases

Finally we can define the central concept investigated in this report, the Gröbner basis.

Definition 2.5.1 (Gröbner Basis)**.** Given a monomial ordering on a polynomial ring $k[x_1, \ldots, x_n]$ consider a subset $G = \{g_1, \ldots, g_m\}$ of an ideal $I \subset k[x_1, \ldots, x_n]$, $I \neq \{0\}$. We call G a Gröbner basis if $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$

The following theorem about the reduced Gröbner basis, along with a proof of the method for obtaining it, can be found in pages 93-94 of Ideals, Varieties, and Algorithms [3] (Theorem 5)

Theorem 2.5.2 (Reduced Gröbner Basis)**.** *Given an ideal $I \subset k[x_1, \ldots, x_n]$ and a monomial ordering, I has a unique Gröbner Basis G such that for all $g \in G$:*

1. *$LC(g) = 1$*
2. *$x^\alpha \notin \langle LT(G \setminus \{g\}) \rangle$ for all monomials x^α in g.*

We call this G the reduced Gröbner basis of I.
Furthermore, the reduced Gröbner basis can be constructed from any Gröbner basis as follows:

Let G be an arbitrary Gröbner basis for some polynomial ideal I. Then do:

1. *For all $g \in G$, if $LT(g) \in \langle G \setminus \{g\} \rangle$ then do $G = G \setminus g$.*
2. *For all $g \in G$ do $G = (G \setminus \{g\}) \cup \overline{g}^{G \setminus \{g\}}$.*

Definition 2.5.3 (Least Common Multiple (for monomials))**.** The least common multiple, or lcm for short, of a set of monomials $F \subset k[x_1, \ldots, x_n]$ is the unique monomial $x^\beta \in k[x_1, \ldots, x_n]$ such that:

1. all $x^\alpha \in F$ divide x^β.
2. for any x^γ such that all $x^\alpha \in F$ divide x^γ, we have x^β divides x^γ too.
3. $\mathrm{LC}(x^\beta) = 1$

We denote this x^β by $\mathrm{lcm}(F)$.

The following definition and accompanying theorem are vital for Buchberger's algorithm, an algorithm for computing Gröbner basis. This will be discussed in Section 3.

Definition 2.5.4 (S-polynomial)**.** Given two nonzero polynomials $f, g \in k[x_1, \ldots, x_n]$ we define their S-polynomial as follows:

$$S(f,g) = \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} \cdot f - \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} \cdot g$$

A proof of the two versions of Buchberger's criterion can be found in pages 86-88 (Theorem 6) and pages 105-106 (Theorem 3) of Ideals, Varieties, and Algorithms [3].

Theorem 2.5.5 (Buchberger's Criterion)**.** *Given an ideal $I \subset k[x_1, \ldots, x_n]$ and a monomial ordering, a subset $G = \{g_1, \ldots, g_m\} \subset k[x_1, \ldots, x_n]$ is a Gröbner basis of I if and only if:*

$$S(g_i, g_j) \to_G 0, \quad \textit{for all } i \neq j$$

Remark. Note that a less general version of Buchberger's criterion also exists with $\overline{S(g_i,g_j)}^G = 0$ being required instead of $S(g_i, g_j) \to_G 0$

This criterion is the driving force of Buchberger's algorithm, which will be discussed in Section 3.1.

During this report I will often work with ideals generated by binomials. For this reason the following result on Gröbner bases of binomials will be useful:

Theorem 2.5.6 (Gröbner bases of binomial ideals)**.** *Let $F \subset k[x_1, \ldots, x_n]$ be a set of binomials and let $I = \langle F \rangle$. Then the reduced Gröbner basis G of I is comprised solely of binomials.*

Proof. First I will show there is a Gröbner basis which is made up of just binomials, then use this to construct the reduced Gröbner basis.

In order to show such a Gröbner basis exists, I will show one can be obtained by using Buchberger's algorithm (this algorithm can be found in Section 3.1). First note that the S-polynomial of two binomials is, again, a binomial. This is because the S-polynomial is constructed exactly such that two terms will cancel, leaving us with just two terms again. By the same reasoning, every step in the division algorithm that we take after computing the S-polynomial will also be the sum of two binomials, such that two terms cancel one another. Indeed once the (division) algorithm is finished we either end up with 0, or a binomial. In the latter case we add this binomial to G, but this is not a problem as G will still consist exclusively of binomials going forward.

Indeed after every step we take G will exclusively consist of binomials. Thus once the full algorithm is finished, and G is a Gröbner basis, it will only contain binomials.

Now from this Gröbner basis G we can construct the reduced Gröbner basis G'. During this process we only have that binomials are removed, or are replaced by binomials that were reduced by binomials

using the division algorithm. The latter, as already explained, is still a binomial after application of the division algorithm. Thus we conclude G', the reduced Gröbner basis of I, is made up of just binomials □

2.6 Symmetry

One thing researched in this report, is what happens to Gröbner bases when symmetry is applied. First, I will need to make clear what symmetry means in this context.

Definition 2.6.1 (Left Group Action)**.** Let G be a group with identity e and operator $*$. Let X be a set. Consider the map:

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

We call this map a left group action of G on X if it satisfies the following properties:

1. $e \cdot x = x$ for all $x \in X$
2. $g \cdot (h \cdot x) = (g * h) \cdot x$ for all $x \in X$ and $g, h \in G$

Definition 2.6.2 (Sym(n))**.** We define Sym(n) as the set of all permutations of $\{1, \ldots, n\}$. Note that this is in fact a group, with composition as operator.

Definition 2.6.3 (Cycle Notation)**.** We use $(x_1, x_2, \ldots, x_n)$, with $x_i \in \mathbb{N}$, to denote the permutation σ for which:

$$\sigma(x) = \begin{cases} x_{i+1} & \text{if } x = x_i \\ x & \text{if } x \neq x_i \text{ for all } i \in [1, n] \end{cases}$$

Definition 2.6.4 (Symmetric Action on Polynomials)**.** We define the symmetric action of Sym(n) on the polynomial ring $k[x_1, \ldots, x_n]$ as follows:

$$\begin{aligned} \text{Sym}(n) \times k[x_1, \ldots, x_n] &\to k[x_1, \ldots, x_n] \\ (\sigma, f) &\mapsto \sigma(f) = f(x_{\sigma(1)} \ldots, x_{\sigma(n)}) \end{aligned}$$

Note that this is indeed a left group action, as (1) maps every f to itself, and:

$$\sigma_1(\sigma_2(f)) = f(x_{\sigma_1(\sigma_2(1))} \ldots, x_{\sigma_1(\sigma_2(n))}) = (\sigma_1\sigma_2)(f)$$

Example 2.6.5 (Cycle Notation Example)**.** Let $f = x_1^3 + x_2^2 + x_3 \in k[x, y]$, then:

$$(1, 2, 3)f = x_2^3 + x_3^2 + x_1$$

Definition 2.6.6 (Useful Set Definition)**.** Let $f \in k[x_1, \ldots, x_n]$. We define the set:

$$\text{Sym}(n)f = \{\sigma(f) \mid \sigma \in \text{Sym}(n)\}$$

We can extend this definition to sets of polynomials as follows:
Let $F \subset k[x_1, \ldots, x_n]$. We define:

$$\text{Sym}(n)F = \{\sigma f \mid \sigma \in \text{Sym}(n), f \in F\}$$

Remark. A different way of writing Sym(n)f is Sym($\{x_1, \ldots, x_n\}$)f. This notation will be used in particular when working with variables that aren't indexed (e.g. when working in $k[x, y]$), as the other notation would be ill-defined.

Example 2.6.7. Let $F = \{x_1^2 + x_2, x_2^3\} \subset k[x_1, x_2]$. Then we find:

$$\text{Sym}(2)F = \{x_1^2 + x_2, x_2^2 + x_1, x_2^3, x_1^3\}$$

3 Algorithms

Regardless of how useful Gröbner bases might be, if there was no way to compute them, their viability as a mathematical tool would drop significantly. Thankfully, in his thesis introducing Gröbner Bases [1], Buchberger also included an algorithm that allows computation of the Gröbner Basis of any polynomial ideal.

3.1 Buchberger's Algorithm

Buchberger's original algorithm makes use of his criterion that poses a requirement on the S-polynomials of the pairs of polynomials in a Gröbner basis. It does this by repeatedly checking all S-polynomials, and if any of them reduces to an $r \neq 0$ then r gets added to the candidate Gröbner basis. In pseudo-code it looks as follows:

Algorithm 2: Buchberger's Algorithm

input : $F = (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$
output: Gröbner basis $G = (g_1, \ldots, g_s)$ of $I = \langle F \rangle$

```
G = F
G' = ∅
while G' ≠ G do
    G' = G
    for each pair {p, q} ⊂ G', p ≠ q do
        r = S(p, q)^{G'}
        if r ≠ 0 then
            G = G ∪ {r}
return G
```

It is easy to verify that the output G is indeed a Gröbner basis for I. A proof that the algorithm does actually terminate is based on the fact that every time a polynomial gets added to G, $\langle \mathrm{LT}(G) \rangle$ increases. Then by the ascending chain condition we conclude G must stabilize.

While we know that Buchberger's algorithm does terminate, how long it takes to terminate is a much harder question to answer. This is due to the number of S-polynomials that need to be reduced varying greatly depending on both the order of polynomials that get applied when performing the reduction algorithm, as well as the general choice of which S-polynomials to reduce first.

Buchberger's algorithm is a good starting point, but it is not very optimized. As mentioned, the algorithm requires the user to make several choices (choice of pair, order of polynomials when reducing), and these choices can greatly affect the speed of the algorithm. The critical pair (being the pair used to create an S-polynomial to evaluate) selection strategy might then be the place to start looking for optimizations. One such strategy is the sugar strategy, which was experimentally shown to work quite well [6].

3.2 Faugère's F_4 and F_5 Algorithms

Faugère, however, had a better idea regarding selection strategies, this he implemented in his F_4 algorithm [4]. Rather than implementing a specific selection strategy, the F_4 algorithm negates the choice of critical pair by considering several critical pairs simultaneously. It does this by transforming the polynomials into a matrix, with each row representing a polynomial and each column a possible term. The columns are ordered using the monomial ordering.

Example 3.2.1. Let $f = xy^2 + 5y^3$, $g = 3x^3 + 6xy^2$ be polynomials in $k[x, y]$. We use grevlex ordering with $x > y$. Then the matrix representation described by Faugère would be:

$$\begin{pmatrix} 0 & 1 & 5 \\ 3 & 6 & 0 \end{pmatrix}$$

Here we see the top and bottom row representing f and g respectively. Similarly the columns represent x^3, xy^2 and y^3 in that order.

This matrix representation forms the basis for the F_4 algorithm. To not go into too much detail, the algorithm uses tricks from linear algebra applied to sets of polynomials in matrix form to quickly compute a Gröbner basis. For instance reducing the matrix to row echelon form.

A second point of improvement Faugère focused in on, was the excessive amounts of useless computations. In Buchberger's algorithm, 90% of the time is spent on just computing zeros. So, if there was some way to know in advance what polynomials would result in 0, then the algorithm could be sped up greatly.

This is what he did in his F_5 algorithm. By first computing Gröbner bases for only subsets of polynomials, the algorithm manages to avoid a large amount of useless critical pairs compared to Buchberger's algorithm.

While Faugère's algorithms manage to greatly reduce computation times, there will always be worst case scenario's where the complexity of the reduced Gröbner basis can be absurdly large. The question then becomes: when is it that these Gröbner bases can have such a high degree?

4 Simple Cases

Before investigating what happens in a general setting, we zoom in on some simpler cases and see how their Gröbner bases behave.

4.1 Single Variable Case

When considering ideals in a polynomial ring $k[x]$ of just a single variable, computing Gröbner bases is significantly simpler to do than in the general case. This is due to the following result:

Theorem 4.1.1 (gcd as GB)**.** *Let $I = \langle F \rangle \subset k[x]$ be a nonzero ideal in a polynomial ring of a single variable, then $\{\gcd(F)\}$ is the reduced Gröbner basis for I.*

Proof. Let I be generated by $\{f_1, \ldots, f_n\} \subset k[x]$. We know such a generating set exists for every ideal by the Hilbert Basis Theorem. Denote $f' = \gcd(\{f_1, \ldots, f_n\})$. In order to show $\langle f' \rangle$ is a Gröbner basis for I we need to show two inclusions: $\langle \mathrm{LT}(I) \rangle \subset \langle \mathrm{LT}(f') \rangle$ and $\langle \mathrm{LT}(f') \rangle \subset \langle \mathrm{LT}(I) \rangle$

1. Let $x^\beta \in \langle \mathrm{LT}(I) \rangle$, then x^β is divisible by the leading term of a polynomial, say f^*, in I. But because f^* is a combination of the f_i, and all f_i are divisible by f', we conclude that f^* is also divisible by f'. Thus the degree of $\mathrm{LT}(f^*)$ is greater or equal to the degree of $\mathrm{LT}(f')$. This means, since we are working with just 1 variable, $\mathrm{LT}(f')$ divides $\mathrm{LT}(f^*)$, which in turn means it also divides x^β. This implies $x^\beta \in \langle \mathrm{LT}(f') \rangle$
2. Next suppose $x^\beta \in \langle \mathrm{LT}(f') \rangle$, then $x^\beta = h \cdot \mathrm{LT}(f')$ for some $h \in k[x]$. Now using the extended Euclidean algorithm we can find $g_1, \ldots, g_n \in k[x]$ such that $f' = g_1 f_1 + \ldots + g_n f_n$. Then we find $h \cdot f' = h \cdot (g_1 f_1 + \ldots + g_n f_n) \in I \implies x^\beta \in \langle \mathrm{LT}(I) \rangle$

In conclusion $\langle \mathrm{LT}(f') \rangle$ and $\langle \mathrm{LT}(I) \rangle$ contain the same monomials, and thus (since they are both generated by monomials) are identical. So $\{\gcd(\{f_1, \ldots, f_n\})\}$ is indeed a Gröbner basis.

One can then quickly verify $\{\gcd(\{f_1, \ldots, f_n\})\}$ is also the reduced Gröbner basis, by virtue of it consisting of just a single polynomial. □

This result is to be expected, considering Buchberger's algorithm is a generalization of the Euclidean algorithm in the first place.

Using the powerful fact that the gcd is the reduced Gröbner basis we can compute a Gröbner basis for an ideal by just simply computing the gcd of the polynomials that generate it. For this we use the Euclidean algorithm, which generally is much faster than any Gröbner basis specific algorithm.

4.2 Linear Case

Another simple case to consider is the linear case. I.e. we will look at the Gröbner basis of ideals generated by linear polynomials. The important result here is that, instead of applying a Gröbner basis specific algorithm, we can actually just use Gaussian elimination.
Let us first consider an example:

Example 4.2.1. We work in $k[x, y, z]$ with $x > y > z$ grevlex order.

$$\begin{aligned} f_1 &= x + y \\ f_2 &= x + 3y - z \\ f_3 &= 2x + 2y \end{aligned}$$

We can then write this in matrix form:

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 3 & -1 \\ 2 & 2 & 0 \end{pmatrix}$$

After applying Gaussian elimination we are left with:

$$\begin{pmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 \end{pmatrix}$$

So we get $g_1 = x + \frac{1}{2}z$ and $g_2 = y - \frac{1}{2}z$, with $G = \{g_1, g_2\}$ being the candidate Gröbner basis. We verify if it is truly a Gröbner basis by using Buchberger's criterion:

$$S(g_1, g_2) = \frac{xy}{x}(x + \frac{1}{2}z) - \frac{xy}{y}(y - \frac{1}{2}z) = xy + \frac{1}{2}zy - xy + \frac{1}{2}zx = \frac{1}{2}zx + \frac{1}{2}zy$$

We can now apply the division algorithm:

$$\frac{1}{2}zx + \frac{1}{2}zy - \frac{1}{2}zg_1 = \frac{1}{2}zx + \frac{1}{2}zy - \frac{1}{2}z(x + \frac{1}{2}z) = \frac{1}{2}zy - \frac{1}{4}z^2$$
$$\frac{1}{2}zy - \frac{1}{4}z^2 - \frac{1}{2}zg_2 = \frac{1}{2}zy - \frac{1}{4}z^2 - \frac{1}{2}z(y - \frac{1}{2}z) = 0$$

So indeed $\overline{S(g_1, g_2)}^G = 0$ which means G is a Gröbner basis.

Of course a single example does not show us what happens in general, for that we need a full proof.

Theorem 4.2.2 (Gaussian Elimination for GB)**.** *Let $F = \{f_1, \ldots, f_m\} \subset k[x_1, ..., x_n]$ be a subset containing only linear polynomials. Let $>$ be some monomial order. Let $G = \{g_1, \ldots, g_r\}$ be the result of applying Gaussian elimination on F following the order established by the monomial order. I.e. if $x > y$, then first eliminate x. Then G is a Gröbner basis for the ideal generated by F.*

Proof. First consider the following homomorphism from $k[x_1, ..., x_n]$ to $k[x_j \mid \forall i : x_j \neq \mathrm{LM}(g_i)]$:

$$\mu(x_j) = \begin{cases} x_j & \text{if } \forall_i : x_j \neq \mathrm{LM}(g_i) \\ \mathrm{LT}(g_i) - g_i & \text{if } \exists_i : x_j = \mathrm{LM}(g_i) \end{cases}$$

Note that since we have applied Gaussian elimination, we know that all variables which belong to the second case appear in exactly one polynomial. Furthermore, we know, by definition, that this x_j that appears in some g_i, must also be the leading term of the g_i. Thus, for any g_i, $\mathrm{LT}(g_i) - g_i$ contains exclusively variables in $k[x_j \mid \forall i : x_j \neq \mathrm{LM}(g_i)]$.

Next we show that kernel of this map is exactly $I = \langle F \rangle$, and its image is exactly $k[x_j \mid \forall i : x_j \neq \mathrm{LM}(g_i)]$. The latter can be easily seen by observing that it is a subset of the domain and that all elements that are also in $k[x_j \mid \forall i : x_j \neq \mathrm{LM}(g_i)]$ will be mapped to themselves.

Additionally observe that, because the g_i only contain the variable $\mathrm{LT}(g_i)$ and variables in $k[x_j \mid \forall i : x_j \neq \mathrm{LM}(g_i)]$, we have that $g_i - \mathrm{LT}(g_i)$ contains exclusively variables in $k[x_j \mid \forall i : x_j \neq \mathrm{LM}(g_i)]$. Thus we find, by linearity:

$$\mu(g_i) = \mu(\mathrm{LT}(g_i) + (g_i - \mathrm{LT}(g_i)) = \mu(\mathrm{LT}(g_i)) + \mu((g_i - \mathrm{LT}(g_i)) = \mathrm{LT}(g_i) - g_i + g_i - \mathrm{LT}(g_i) = 0$$

Now suppose we have an element $h \in I$, we know: $h = p_1 g_1 + \ldots + p_n g_n$, then using linearity: $\mu(h) = \mu(p_1 g_1 + \ldots + p_n g_n) = \mu(p_1)\mu(g_1) \ldots \mu(p_n)\mu(g_n) = 0$. Thus $h \in \mathrm{Ker}(\mu)$.

Next suppose we have a $h \in k[x_1, ..., x_n]$ such that $\mu(h) = 0$. Then, by Theorem 2.4.2, we find a representation of the form $h = q_1 g_1 + \ldots q_n g_n + r$, with r not divisible by the leading term of any g_i. Now observe:

$$0 = \mu(h) = \mu(q_1 g_1 + \ldots q_n g_n + r) = \mu(q_1)\mu(g_1) + \ldots \mu(q_n)\mu(g_n) + \mu(r) = \mu(r)$$

In particular, since the leading terms of the g_i are also the largest variables in the ordering we find that r does not contain any of the $\mathrm{LM}(g_i)$. However, since $\mu(r) = 0$ this means $r = 0$, which means that h must be in I, as all we did to get to r from h was subtract multiples of the g_i. So indeed if $\mu(h) = 0 \iff h \in I$.

In conclusion $\mathrm{Ker}(\mu) = I$, and $\mathrm{im}(\mu) = k[x_j \mid \forall i, j : x_j \neq \mathrm{LM}(g_i)]$. We can now apply the first isomorphism theorem for rings to conclude $k[x_1, ..., x_n]/I$ and $k[x_j \mid \forall i : x_j \neq \mathrm{LM}(g_i)]$ are isomorphic.

Now let $F = \{f_1, \ldots, f_m\} \subset k[x_1, ..., x_n]$. Apply Gaussian elimination on F to get $G = (g_1, \ldots, g_r)$, an ordered tuple such that $\mathrm{LM}(g_i) > \mathrm{LM}(g_j)$ if $i > j$. Observe that all the g_i have different leading terms (also meaning $r \leq n$).
Then suppose $\overline{S(g_i, g_j)}^G = g'$ for some i, j. Then no monomial of g' is divisible by any $\mathrm{LM}(g_i)$, $i \in [1, r]$. So $g' \in k[x_j \mid \forall i, j : x_j \neq \mathrm{LM}(g_i)]$

Clearly $\mu(g') = g'$, as it contains none of the $\mathrm{LM}(g_i)$. However we also have

$$\mu(g') = \mu(p_1 g_1 + \ldots + p_n g_n) = \mu(p_1)\mu(g_1) \ldots \mu(p_n)\mu(g_n) = 0$$

This implies $g' = 0$ and thus, since i, j was arbitrary, $\overline{S(g_i, g_j)}^G = 0 \ \ \forall_{i,j \in [1,r]}$. This in turn means that G is a Gröbner basis.

□

Again, this result is to be expected, given how Gröbner bases can be seen as a generalisation of the single variate gcd.

5 Some Examples

To illustrate how Gröbner basis degrees can grow very large we will discuss some examples. I will discuss a fairly simple to understand example which has exponential growth and I will go in depth on a more complex example, which will have double exponential growth of the degree of the Gröbner basis.

5.1 d^2

First, the easier to follow, but also less egregious example. We can show that the reduced Gröbner basis of a set of polynomials of degree at most $d+1$, can still contain polynomials of degree d^2+1. This one came from F. Mora and can be found, without proof, in the appendix of a paper by Lazard [7]. It goes as follows:

Lemma 5.1.1. Let $I = \langle\{f_1, f_2, f_3\}\rangle = \langle\{x^{n+1} - yz^{n-1}w, xy^{n-1} - z^n, x^n z - y^n w\}\rangle$. The reduced Gröbner basis G of I contains the polynomial $z^{n^2+1} - y^{n^2}w$ if we use grevlex ordering ($x > y > z > w$).

Proof. In order to show this, we need to prove two things. First $z^{n^2+1} - y^{n^2}w \in I$ and second we need there to be no term in $\langle LT(G)\backslash(z^{n^2+1} - y^{n^2}w)\rangle$ that divides either of the terms of $z^{n^2+1} - y^{n^2}w$. Note that, because the ideal is generated by binomials, we know the Gröbner basis will consist solely of binomials too by Lemma 2.5.6. (Recall the unicity of the reduced Gröbner basis).

First I will show no polynomial with leading term z^i, $0 \leq i \leq n^2$ can exist in I. To do this we will attempt to get a leading term of the form z^i, $i \geq 0$, and in the process conclude this can only happen for $i \geq n^2 + 1$.
In order to get z^i to be as a leading term, we first need to get it as a term in general. The only place we'd be able to get a monomial consisting exclusively of a power of z would be f_2. We find we must start with:

$$z^l f_2 = z^l(xy^{n-1} - z^n) = xy^{n-1}z^l - z^{n+l}$$

for some $l \geq 0$. In order to make z^{n+l} the leading term we'd need to somehow cancel out the first term $xy^{n-1}z^l$. We now find that almost every term in all three polynomials either contains an x^n or a w. If either of these are present we clearly can't use those terms to cancel $xy^{n-1}z^l$. The first term of f_2 also won't work, as we'd end up cancelling z^{n+l} too. So we must use the second term of f_2. We do this as follows:

$$z^l \cdot f_2 + xy^{n-1}z^{l-n} \cdot f_2 = xy^{n-1}z^l - z^{l+n} + x^2y^{2n-2}z^{l-n} - xy^{n-1}z^l = x^2y^{2n-2}z^{l-n} - z^{l+n}$$

Note that in order to apply this cancellation in the first place we needed $l \geq n$, otherwise we'd be multiplying by a negative power of z, which is not legal in this setting.
We now still don't have a power of z as leading term, so we need to cancel $x^2y^{2n-2}z^{l-n}$. By the same reasoning as before our only choices are the terms of f_2. The first term would just undo what we just did, so we again use the second term of f_2. We take:

$$\begin{aligned} x^2y^{2n-2}z^{l-n} - z^{l+n} + x^2y^{2n-2}z^{l-2n} \cdot f_2 &= x^2y^{2n-2}z^{l-n} - z^{l+n} + x^3y^{3n-3}z^{l-3n} - x^2y^{2n-2}z^{l-n} \\ &= x^3y^{3n-3}z^{l-2n} - z^{l+n} \end{aligned}$$

Note that this time we needed $l \geq 2n$ in order to apply this cancellation. Even still z^{l+n} is not the leading term.

We are now forced to keep repeating the cancellation applied the last two times until our leading term could potentially be cancelled out by a different term from a different polynomial. This is still because of the x^n and w present in all other terms. Indeed, we will only be able to use a different term for cancellation once the leading term contains x^n (this can be easily verified as all terms either contain w or a power of x greater than or equal to n). This would mean we'd have to repeat the process $n-1$ times, the caveat is that we can only cancel the leading term this many

times if l is large enough, as after i iterations of this process, the z in the leading term has a power of $l - i \cdot n$. So since we need to repeat this process n times, we need $l \geq n(n-1) = n^2 - n$.

Now let us consider what we are left with after these $n-1$ iterations, this is: $x^n y^{n^2-n} z^{l-n(n-1)} - z^{l+n}$. Now since our power of x is high enough, we are able to cancel this leading term using f_3 as follows:

$$\begin{aligned} x^n y^{n^2-n} z^{l-n(n-1)} - z^{l+n} - y^{n^2-n} z^{l-n(n-1)-1} \cdot f_3 = \\ x^n y^{n^2-n} z^{l-n(n-1)} - z^{l+n} - x^n y^{n^2-n} z^{l-n(n-1)} + y^{n^2} z^{l-n(n-1)-1} w = \\ -z^{l+n} + y^{n^2} z^{l-n^2+n-1} w \end{aligned}$$

Briefly consider $l = n^2 - n$ and observe that the polynomial we multiply f_3 with will contain z^{-1}, which is not allowed. So $l \geq n^2 - n + 1$. And in particular if $l = n^2 - n + 1$:

$$-z^{l+n} + y^{n^2} z^{l-n^2+n-1} w = -z^{n^2+1} + y^{n^2} w$$

This is exactly the polynomial we were looking for (up to a minus sign). So we have seen that no polynomial with leading term z^l, $l \leq n^2$ can exist in I by exhausting all options to obtain such a polynomial, and we have shown that $z^{n^2+1} - y^{n^2} w \in I$.

If we now observe that the only way to cancel $y^{n^2} w$ is by undoing the cancellation from before, we can conclude $z^{n^2+1} - y^{n^2} w$ is the only binomial in I with leading term z^{n^2+1}. This is because we exhausted every option to get z^{n^2+1} as a leading term before arriving at $z^{n^2+1} - y^{n^2} w$, and we can't do any new cancellation from there.

A similar strategy to the one used for z^{n^2+1} can be used to show no polynomial with leading term that divides $y^{n^2} w$ exists in I (using f_3 instead of f_2).

Now since $z^{n^2+1} - y^{n^2} w \in I$, we have $z^{n^2+1} \in \langle \mathrm{LT}(I) \rangle$. But since no power of z less than $n^2 + 1$ is in $\langle \mathrm{LT}(I) \rangle$ we know there must be a polynomial in G with leading term z^{n^2+1}. Then, due to $z^{n^2+1} - y^{n^2} w$ being the only binomial with this particular leading term, we conclude $z^{n^2+1} - y^{n^2} w \in G$ in order to satisfy $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle$. □

5.2 d^{2^n}

In order to truly show how large the degrees can grow we will need a far more complex example. This example was originally given by Mayr and Meyer [2], before being adapted into a context more closely related to Gröbner bases by Möller and Mora [8].

First I will give the example in full, then I will focus on proving a major preliminary result, before finally proving the lower bound on the degree of Gröbner basis in this example has double exponential growth.

5.2.1 The Setting

Fix some $d \in \mathbb{N}$. We define:

$$\begin{aligned}
P_0 &:= k[S_0, Q_{1,0}, Q_{2,0}, Q_{3,0}, Q_{4,0}, F_0, C_{1,0}, C_{2,0}, C_{3,0}, C_{4,0}, B_{1,0}, B_{2,0}, B_{3,0}, B_{4,0}] \\
P_n &:= P_{n-1}[S_n, Q_{1,n}, Q_{2,n}, Q_{3,n}, Q_{4,n}, F_n, C_{1,n}, C_{2,n}, C_{3,n}, C_{4,n}, B_{1,n}, B_{2,n}, B_{3,n}, B_{4,n}] \\
I_0 &:= \langle \{S_0 C_{i,0} - F_0 C_{i,0} B_{i,0}^d \mid i \in [1,4]\} \rangle \subset P_0 \\
J_{n-1} &:= \langle I_{n-1} \cup \{S_n - Q_{1,n} S_{n-1} C_{1,n-1},\ Q_{1,n} F_{n-1} C_{1,n-1} B_{1,n-1} - Q_{2,n} S_{n-1} C_{2,n-1}, \\
&\quad Q_{2,n} F_{n-1} C_{2,n-1} - Q_{3,n} F_{n-1} C_{3,n-1}\} \\
&\quad \cup \{Q_{2,n} C_{i,n} F_{n-1} B_{2,n-1} - Q_{2,n} C_{i,n} F_{n-1} B_{3,n-1} B_{i,n} \mid i \in [1,4]\} \rangle \subset P_n \\
I_n &:= \langle J_{n-1} \cup \{Q_{3,n} S_{n-1} C_{3,n-1} B_{1,n-1} - Q_{2,n} S_{n-1} C_{2,n-1} B_{4,n-1},\ Q_{4,n} S_{n-1}, C_{4,n-1} - F_n, \\
&\quad Q_{3,n} S_{n-1} C_{3,n-1} - Q_{4,n} F_{n-1} C_{4,n-1} B_{4,n-1}\} \rangle \subset P_n \\
e_n &:= d^{2^n}
\end{aligned}$$

As part of the proof we will be working modulo I_n, which means the polynomials in I_n will be seen as equivalences. We will give these equivalences a unique label to easily be able to refer to them.

$$S_n \equiv Q_{1,n} S_{n-1} C_{1,n-1} \tag{1a}$$
$$Q_{1,n} F_{n-1} C_{1,n-1} B_{1,n-1} \equiv Q_{2,n} S_{n-1} C_{2,n-1} \tag{1b}$$
$$Q_{2,n} F_{n-1} C_{2,n-1} \equiv Q_{3,n} F_{n-1} C_{3,n-1} \tag{1c}$$
$$Q_{3,n} S_{n-1} C_{3,n-1} B_{1,n-1} \equiv Q_{2,n} S_{n-1} C_{2,n-1} B_{4,n-1} \tag{1d}$$
$$Q_{3,n} S_{n-1} C_{3,n-1} \equiv Q_{4,n} F_{n-1} C_{4,n-1} B_{4,n-1} \tag{1e}$$
$$Q_{4,n} S_{n-1}, C_{4,n-1} \equiv F_n \tag{1f}$$
$$Q_{2,n} C_{1,n} F_{n-1} B_{2,n-1} \equiv Q_{2,n} C_{1,n} F_{n-1} B_{3,n-1} B_{1,n} \tag{1g}$$
$$Q_{2,n} C_{2,n} F_{n-1} B_{2,n-1} \equiv Q_{2,n} C_{2,n} F_{n-1} B_{3,n-1} B_{2,n} \tag{1h}$$
$$Q_{2,n} C_{3,n} F_{n-1} B_{2,n-1} \equiv Q_{2,n} C_{3,n} F_{n-1} B_{3,n-1} B_{3,n} \tag{1i}$$
$$Q_{2,n} C_{4,n} F_{n-1} B_{2,n-1} \equiv Q_{2,n} C_{4,n} F_{n-1} B_{3,n-1} B_{4,n} \tag{1j}$$

It is important to note that these equivalences hold for all $n \in [1, m]$ when working modulo I_m. I will henceforth call the second index of the variables (or only index, in the case of S and F) their "level" and use this to differentiate between them. Similarly I will refer to the equivalences by their level too, this level being based on the highest level variable present in the equivalence. e.g. $S_5 \equiv Q_{1,5} S_4 C_{1,4}$ is equivalence (1a) of level 5.
Do observe that, while I_n simply contains all equivalences of level less than or equal to n, the situation for J_n is slightly more complicated. On top of all equivalences in I_n, J_n also contains equivalences (1a) - (1c) and (1g) - (1j) of level $n+1$. This observation will be important later.

5.2.2 $S_n C_{i,n}$'s Only Equivalence

This section is devoted to proving that the only nontrivial monomial containing S_n or F_n that is equivalent to $S_n C_{i,n} \mod I_n$ is $F_n C_{i,n} B_{i,n}^{e_n}$. The first step will be proving that this is an equivalence in the first place.

The following lemma and its proof were adapted from Lemma 6 of the paper by Mayr and Meyer [2] (pages 316-317).

Lemma 5.2.1. Let $i \in [1,4]$, $n \geq 0$, variables, rings and ideals defined as above. Then:

$$S_n C_{i,n} \equiv F_n C_{i,n} B_{i,n}^{e_n} \mod I_n$$

Proof. We will use induction. For $n = 0$ the equivalence is already given.
Now assume $S_nC_{i,n} \equiv F_nC_{i,n}B_{i,n}^{e_n} \mod I_n$ holds for all $i \in [1,4]$ and all $n < m$ for some $m \geq 1$. Then:

$$\begin{aligned}
S_mC_{i,m} &\equiv C_{i,m}Q_{1,m}S_{m-1}C_{1,m-1} && \text{by (1a)} && \text{(2a)}\\
&\equiv C_{i,m}Q_{1,m}F_{m-1}C_{1,m-1}B_{1,m-1}^{e_{m-1}} && \text{by the induction hypothesis} && \text{(2b)}\\
&\equiv C_{i,m}B_{1,m-1}^{e_{m-1}-1}Q_{2,m}S_{m-1}C_{2,m-1} && \text{by (1b)} && \text{(2c)}\\
&\equiv C_{i,m}B_{1,m-1}^{e_{m-1}-1}Q_{2,m}F_{m-1}C_{2,m-1}B_{2,m-1}^{e_{m-1}} && \text{by the induction hypothesis} && \text{(2d)}\\
&\equiv C_{i,m}B_{1,m-1}^{e_{m-1}-1}Q_{2,m}F_{m-1}C_{2,m-1}B_{3,m-1}^{e_{m-1}}B_{i,m}^{e_{m-1}} && \text{by one of (1g) - (1j) } e_{m-1} \text{ times} && \text{(2e)}\\
&\equiv C_{i,m}B_{i,m}^{e_{m-1}}B_{1,m-1}^{e_{m-1}-1}Q_{3,m}F_{m-1}C_{3,m-1}B_{3,m-1}^{e_{m-1}} && \text{by (1c)} && \text{(2f)}\\
&\equiv C_{i,m}B_{i,m}^{e_{m-1}}B_{1,m-1}^{e_{m-1}-1}Q_{3,m}S_{m-1}C_{3,m-1} && \text{by the induction hypothesis} && \text{(2g)}\\
&\equiv C_{i,m}B_{i,m}^{e_{m-1}}B_{1,m-1}^{e_{m-1}-2}B_{4,m-1}Q_{2,m}S_{m-1}C_{2,m-1} && \text{by (1d)} && \text{(2h)}\\
&\equiv C_{i,m}B_{i,m}^{e_{m-1}(e_{m-1}-1)}B_{4,m-1}^{e_{m-1}-1}Q_{2,m}S_{m-1}C_{2,m-1} && \text{by (2d) - (2h) } e_{m-1}-2 \text{ times} && \text{(2i)}\\
&\equiv C_{i,m}B_{i,m}^{e_{m-1}e_{m-1}}B_{4,m-1}^{e_{m-1}-1}Q_{3,m}S_{m-1}C_{3,m-1} && \text{by (2d) - (2g)} && \text{(2j)}\\
&\equiv C_{i,m}B_{i,m}^{e_m}Q_{4,m}F_{m-1}C_{4,m-1}B_{4,m-1}^{e_{m-1}-1} && \text{by (1e) and } e_{m-1}^2 = e_m && \text{(2k)}\\
&\equiv C_{i,m}B_{i,m}^{e_m}Q_{4,m}S_{m-1}C_{4,m-1} && \text{by the induction hypothesis} && \text{(2l)}\\
&\equiv F_mC_{i,m}B_{i,m}^{e_m} && \text{by (1f)} && \text{(2m)}
\end{aligned}$$

Since m and i were arbitrary we conclude by induction that

$$S_nC_{i,n} \equiv F_nC_{i,n}B_{i,n}^{e_n} \mod I_n$$

holds for all $n \geq 0$ and $i \in [1,4]$. □

Before we continue with the proof we need to define a few things. First, recall the definition of ϕ, the variable specific degree, as it will be heavily utilized going forward.

Definition 5.2.2 (Height)**.** Let α be a monomial in P_n be such that $\alpha \equiv S_nC_{i,n} \mod I_n$, then we define the height of α:

$$h(\alpha) = \min\{m \in \mathbb{N} \mid \exists_{j\in[1,4]} : \ \phi(\alpha, C_{j,m}) > 0\}$$

Definition 5.2.3 (F-Path)**.** Fix an $F \subset k[x_1, \ldots, x_n]$ for some polynomial ring. Let $I = \langle F \rangle$. Take:

$$\alpha = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_r = \beta \mod I$$

with all the γ_i's monomials in I. We call this an F-path, or path for short, from α to β, if:

1. $\gamma_{n+1} - \gamma_n$ is divisible by a polynomial in F.
2. $\gamma_i \neq \gamma_j$ for all $i \neq j$.

This can be interpreted as a path in a graph, if we consider monomials the vertices, and equivalences (polynomials) in F the edges.

Now we will just need a few more preliminary results about these definitions before we can start proving the main result.

The following lemma is adapted from Lemma 7 (page 317) in the aforementioned paper by Mayr and Meyer [2], where it is given without proof.

Lemma 5.2.4. We work in the scenario presented in Section 5.2.1. Let $S_nC_{i,n} = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_r = \alpha \mod I_n$ be a path from $S_nC_{i,n}$ to α, then:

$$\sum_{j=1}^{4} \phi(\alpha, C_{j,m}) = \begin{cases} 1 \text{ for m such that } h(\alpha) \leq m \leq n \\ 0 \text{ otherwise} \end{cases} \tag{3a}$$

$$\sum_{j=1}^{4} \phi(\alpha, Q_{j,m}) = \begin{cases} 1 \text{ for m such that } h(\alpha) < m \leq n \\ 0 \text{ otherwise} \end{cases} \tag{3b}$$

$$\phi(\alpha, S_m) + \phi(\alpha, F_m) = \begin{cases} 1 \text{ if } m = h(\alpha) \\ 0 \text{ otherwise} \end{cases} \tag{3c}$$

$$\left|h(\gamma_j) - h(\gamma_{j-1})\right| \leq 1 \text{ for all } j \in [1, r] \tag{3d}$$

$$\text{The only equivalences applicable to } \alpha \text{ are in } \{I_{h(\alpha)+1)} \setminus I_{h(\alpha)-1}\}. \tag{3e}$$

Proof. **(3a)** We do this by induction. First for γ_0 we have $h(\gamma_0) = n$ and $\sum_{j=1}^{4} \phi(\gamma_0, C_{j,m}) = \phi(\gamma_0, C_{i,m}) = 1$ for $m \in [h(\gamma_0), n]$ and 0 otherwise.
Now assume we have an $l \in [0, r)$ such that:

$$\sum_{j=1}^{4} \phi(\gamma_l, C_{j,m}) = \begin{cases} 1 \text{ for m such that } h(\gamma_l) \leq m \leq n \\ 0 \text{ otherwise} \end{cases}$$

A very important observation to make is that S (or F) changes in level if and only if a C does too. We now go over what equivalences can be applied, and how this affects the sum of interest. First note that all equivalences besides (1a) and (1f) only swap C's of the same level. Because of this we have $\sum_{j=1}^{4} \phi(\gamma_{l+1}, C_{j,m}) = \sum_{j=1}^{4} \phi(\gamma_l, C_{j,m})$ if one of these is applied. For the same reason $h(\gamma_l) = h(\gamma_{l+1})$, thus we can now focus on what happens when one of (1a) and (1f) is applied.

Observe that all equivalences have exactly one of S or F on either side. That means that after l equivalences have been applied, we still have exactly one occurrence of an S_j or of an F_j in the monomial. Now note that the only way to get a $C_{j,m}$ after applying an equivalence that wasn't there before, is to use (1a) (or (1f)), which simultaneously lowers the level of S (or F). On a similar note, to increase the level of S (or F) we would have to apply (1a) (or (1f)) in reverse, thus losing the $C_{j,m}$. From this we conclude S (or F) must be of level $h(\gamma_l)$.

Now we have two options. The first is to apply (1a) (or (1f)) of level $h(\gamma_l)$. This means $h(\gamma_{l+1}) = h(\gamma_l) - 1$ by way of introducing a C of level $h(\gamma_l) - 1$. Note that this means $\sum_{j=1}^{4} \phi(\gamma_{l+1}, C_{j,h(\gamma_{l+1})}) = 1$. Additionally it does not affect any other C of any level, thus meaning that for all $m \neq h(\gamma_l) - 1$: $\sum_{j=1}^{4} \phi(\gamma_{l+1}, C_{j,m}) = \sum_{j=1}^{4} \phi(\gamma_l, C_{j,m})$. So we have what we were looking for

The other option is to apply (1a) (or (1f)) of level $h(\gamma_{l_1}) + 1$. Recall that there is only one C of level $h(\gamma_l)$ in γ_l by the induction hypothesis, and this one must disappear when applying either of these equivalences, thus meaning the height increases to $h(\gamma_l) + 1$. Note that again C of level $m \neq h(\gamma_l)$ remain unaffected: $\sum_{j=1}^{4} \phi(\gamma_{l+1}, C_{j,m}) = \sum_{j=1}^{4} \phi(\gamma_l, C_{j,m})$ and now we get $\sum_{j=1}^{4} \phi(\gamma_{l+1}, C_{j,h(\gamma_l)} = 0$, again exactly what we needed.

We have now considered all cases and by induction can then conclude:

$$\sum_{j=1}^{4} \phi(\gamma_l, C_{j,m}) = \begin{cases} 1 \text{ for m such that } h(\gamma_l) \leq m \leq n \\ 0 \text{ otherwise} \end{cases}$$

For all $l \in [0, r]$, and in particular for $\gamma_r = \alpha$.

(3b) The proof here is nearly identical to that of (3a), just with every occurrence of $C_{j,l}$ swapped with $Q_{j,l+1}$.

(3c) We do this by induction. For γ_0 we clearly have:

$$\phi(\gamma_0, S_m) + \phi(\gamma_0, F_m) = \begin{cases} 1 \text{ if } m = h(\gamma_0) \\ 0 \text{ otherwise} \end{cases}$$

Now assume we have an $l \in [0, r)$ such that

$$\phi(\gamma_l, S_m) + \phi(\gamma_l, F_m) = \begin{cases} 1 \text{ if } m = h(\gamma_l) \\ 0 \text{ otherwise} \end{cases}$$

Then we have three cases: $h(\gamma_{l+1}) = h(\gamma_l)$, $h(\gamma_{l+1}) = h(\gamma_l) - 1$ or $h(\gamma_{l+1}) = h(\gamma_l) + 1$. Recall our observation from earlier: S (or F) change from level n to level $n+1$ if and only if a C of level n disappears. In the first case we know C of level $h(\gamma_l)$ disappears, thus S (or F) increases to level $h(\gamma_{l+1})$. In the second case, we find that no C of level $h(\gamma_l)$ disappears. This is because, by (3a), there was only one C of level $h(\gamma_l)$ in γ_l, and we know there must still be exactly 1 in γ_{l+1}. Because of this S (or F) cannot change from level n to level $n+1$. Finally, S (or F) cannot change to level $n-1$ either, as this would introduce a C of level $n-1$, which would no longer be the second case. Finally the third case. The fact that the equation must still hold true in this case is due to (3a). As there can only be 1 C of any given level and a C of level $m-1$ is "used" when increasing the level of S (or F), so if S (or F) increases in level, then the lowest level C disappears, which means the height increases by 1 too. So we find

$$\phi(\gamma_l, S_m) + \phi(\gamma_{l+1}, F_m) = \begin{cases} 1 \text{ if } m = h(\gamma_{l+1}) \\ 0 \text{ otherwise} \end{cases}$$

Then by induction we find this holds for all l, and thus also for $\gamma_r = \alpha$.

(3d) Fix some $l \in [1, r-1]$. First observe that the only equivalences that can change the height of γ_l are (1a) and (1f) This is because all other equivalences have C of the same level on both sides. Now we can either apply them of level $h(\gamma_l)$ or of $h(\gamma_1) + 1$ because of (3c). In the first case no C is lost, and we only gain a $C_{j,h(\gamma_l)-1}$, meaning $h(\gamma_{l-1}) = h(\gamma_l) - 1$, satisfying $\left|h(\gamma_l) - h(\gamma_{l-1})\right| \leq 1$ In the second case we lose a C of level $h(\gamma_l)$ and don't gain any. Note that this case only applies when $h(\gamma_l) < n$, otherwise we would need to use an equivalence in I_{n+1} that isn't in I_n. Then by (3a) we know there was only 1 C of level $h(\gamma_l)$, meaning the height has decreased. (3a) also tells us there was a C of level $h(\gamma_l) + 1 (\leq n)$ in γ_l, which we know is unaffected by the equivalence used to get from γ_l to $\gamma_l + 1$. Thus we find $h(\gamma_{l+1}) = h(\gamma_l) + 1$. Again meaning $\left|h(\gamma_l) - h(\gamma_{l-1})\right| \leq 1$. We have now considered all the cases and thus in conclusion $\left|h(\gamma_j) - h(\gamma_{j-1})\right| \leq 1$ for all $j \in [1, r]$.

(3e) First by looking at the equivalences we observe all equivalences of level m contain an S or F of level m or $m-1$ on both sides. Thus to use any equivalence of level m we must need an S or F of level m or $m-1$. We then recall from (3c) that if $h(\gamma_l) = m$ then only S or F of level m appear in the monomial. So if $h(\gamma_l) = m$ we will only be able to use equivalences of level m or $m+1$. In other words only equivalences in $\{I_{h(\alpha)+1)} \setminus I_{h(\alpha)-1}\}$ □

We can now get to proving the main result from this part. This following lemma and its proof can both be found in the paper by Mayr and Meyer [2] (Lemma 8, pages 318-320). It is adapted and given in a bit more detail here.

Lemma 5.2.5. We work in the scenario presented in Section 5.2.1. Let $S_n C_{i,n} \equiv \alpha \mod I_n$ for some α such that $\phi(\alpha, S_n) + \phi(\alpha, F_n) \neq 0$. Then α is either $S_n C_{i,n}$ or $F_n C_{i,n} B_{i,n}^{e_n}$.

Proof. We prove this by induction on the level n. We will assume $\alpha \neq S_n C_{i,n}$, as this option is trivial, and show $\alpha = F_n C_{i,n} B_{i,n}^{e_n}$.

First take $n = 0$, then this is trivial, as the only equivalence that can be used is $S_0C_{i,0} \equiv F_0C_{i,0}B_{i,0}^d$ for $i \in [1, 4]$.

Take $n > 0$, and assume the lemma holds for $0 \leq m < n$. Now let:

$$S_nC_{i,n} = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_r = \alpha \mod I_n$$

be a path from $S_nC_{i,n}$ to α. First we show that $h(\gamma_l) < n$ for $l \in [1, r)$. Assume there is some $l \in [1, r)$ for which $h(\gamma_l) = n$, then we know by (3c) that γ_l contains an S or F of height n. From this it follows either (1a) or (1f) was used to get from γ_{l-1} to γ_l, as only then can there be an S or F or height n. Now since we are working modulo I_n the only equivalence that can be applied to go from γ_l to γ_{l+1} is the same as the one used to go from γ_{l-1} to γ_l (with the exact equivalence depending on whether F or S is present, and recall only one of them can be present at a time). However now $\gamma_{l-1} = \gamma_{l+1}$ which violates the non-repetition condition. Thus we conclude $h(\gamma_l) < n$ for $l \in [1, r)$.
One can then observe only (1a) of level n is applicable to γ_0. We find: $\gamma_1 = C_{i,n}Q_{1,n}S_{n-1}C_{1,n-1}$, and $h(\gamma_1) = n - 1$. Then, the only equivalence that can be applied is (1a) of level $n - 1$. The main takeaway from this is that $h(\gamma_2) = n - 2$.
We can now use (3d) to determine there must be a minimal $l_1 < r$ such that $h(\gamma_{l_1}) = n - 1$. We shift our focus to the subpath:

$$\gamma_1 \to \ldots \to \gamma_{l_1} \mod I_n.$$

By the minimality of γ_{l_1} we know the height of any γ in this subpath is strictly less than $n - 1$. We can then use (3e) to know that only equivalences of level less than n are used in this path. This in turn means $C_{i,n}$ and $Q_{1,n}$ will not be used during in this path, as they are of level n, and thus only occur in equivalences of level at least n. We rewrite $\gamma_1 = C_{i,n}Q_{1,n}S_{n-1}C_{1,n-1} = C_{i,n}Q_{1,n}\gamma_1'$. The subpath simplifies to:

$$S_{n-1}C_{1,n-1} = \gamma_1' \to \ldots \to \gamma_{l_1}' \mod I_{n-1}.$$

But now note that by (3c) γ_{l_1}' contains an S or F of level $n - 1$. This then means we can use the induction hypothesis to find $\gamma_{l_1}' = F_{n-1}C_{1,n-1}B_{1,n-1}^{e_{n-1}}$. Thus

$$\gamma_{l_1} = C_{i,n}Q_{1,n}F_{n-1}C_{1,n-1}B_{1,n-1}^{e_{n-1}}.$$

By the induction hypothesis and the non-repetition requirement we know we must use an equivalence affecting at least one of $C_{i,n}$ and $Q_{1,n}$. In other words, an equivalence of level n. The only possibility is (1b). We get $\gamma_{l_1+1} = C_{i,n}Q_{2,n}S_{n-1}C_{2,n-1}B_{1,n-1}^{e_{n-1}-1}$. Running through the possible equivalences reveals we must use (1a) of level $n - 1$ now, in particular this means $h(\gamma_{l_1+2}) = n - 2$. We can now repeat the argument from before and take γ_{l_2} to be the minimum γ after γ_{l_1+1} of height $n - 1$. We focus on the subpath:

$$\gamma_{l_1+1} \to \ldots \to \gamma_{l_2} \mod I_n.$$

We again can exclude $C_{i,n}Q_{2,n}$ from the subpath, for reasons motivated earlier. Furthermore, the only equivalences of level less than n that uses $C_{2,n-1}$ is (1h), which does not change it. From this we conclude $C_{2,n-1}$ is present in every step of the subpath, and by (3a) we know no other C of level $n - 1$ is ever present. Because of this we know $B_{1,n-1}^{e_{n-1}-1}$ will not be affected in the subpath, as it requires a $C_{1,n-1}$, which we've just shown will never be present. In total we are able to just focus on the path:

$$S_{n-1}C_{2,n-1} = \gamma_{l_1+1}' \to \ldots \to \gamma_{l_2}' \mod I_{n-1}.$$

with $\gamma_{l_1+1} = C_{i,n}Q_{2,n}B_{1,n-1}^{e_{n-1}-1}\gamma_{l_1+1}'$ etc. Now by the same reasoning as for γ_{l_1} we can conclude $\gamma_{l_2}' = F_{n-1}C_{2,n-1}B_{2,n-1}^{e_{n-1}}$ by (3c) and the induction hypothesis. And thus:

$$\gamma_{l_2} = C_{i,n}Q_{2,n}B_{1,n-1}^{e_{n-1}-1}F_{n-1}C_{2,n-1}B_{2,n-1}^{e_{n-1}}.$$

Once again by the induction hypothesis and the non-repetition requirement we know we must use an equivalence affecting at least one of the variables we were able to exclude in the subpath. We have

two options, either apply (1c) or one of (1g) - (1j) depending on the choice of i. If we choose the latter option this does not affect what equivalences can be applied as we only gain a $B_{i,n}$ and exchange a $B_{2,n-1}$ for a $B_{3,n-1}$. $B_{i,n}$ can only be affected by equivalences of level n (without repetition that is). $B_{2,n-1}$ and $B_{3,n-1}$ are exclusively affected by (1g) - (1j), of which only 1 is usable (again which one depends on choice of i). From this we conclude that no matter how often we apply one of (1g) - (1j), we must eventually use (1c). This happens after at most e_{n-1} uses of (1g) - (1j). For now we just say it was applied an arbitrary number of k times, with $k \in [0, e_{n-1}]$. Following this logic we can call:

$$\gamma_{l_3} = \gamma_{l_2+k+1} = C_{i,n}Q_{3,n}B_{1,n}^{k}B_{1,n-1}^{e_{n-1}-1}F_{n-1}C_{3,n-1}B_{2,n-1}^{e_{n-1}-k}B_{3,n-1}^{k}$$

with γ_{l_3} following from γ_{l_2} after k times (1g) - (1j) and one (1c), all of level n.
Now from (3e) and a look at the equivalences, we can conclude we must apply (1f) of level $n-1$ next. This means $h(\gamma_{l_3+1}) = n-2$. As before we take γ_{l_4} to be the next smallest γ such that $h(\gamma_{l_4}) = n-1$ and focus on the subpath:

$$\gamma_{l_3} \to \ldots \to \gamma_{l_4} \mod I_n.$$

By the same reasoning as before we have that every γ in this subpath contains $C_{3,n-1}$, meaning neither $B_{2,n-1}$ nor $B_{3,n-1}$ will be used. Combined with the fact that variables of level n won't be used, as motivated before, we can simplify the subpath to:

$$F_{n-1}C_{3,n-1}B_{3,n-1}^{k} = \gamma'_{l_3} \to \ldots \to \gamma'_{l_4} \mod I_{n-1}.$$

We have that S_{n-1} or F_{n-1} appears in γ'_{l_4}. Let us first look at the possibilities if we assume F_{n-1} appears. Recall that $C_{3,n-1}$ is present in every γ in this subdpath. We can then in general write $\gamma'_{l_4} = F_{n-1}C_{3,n-1}\eta$, with $\eta \in P_{n-1}$. Note $\eta \neq B_{3,n-1}^{k}$, because we do not allow repetition. Using lemma 5.2.1 we can obtain the following path:

$$\begin{aligned} S_{n-1}C_{3,n-1} &\to \ldots \to F_{n-1}C_{3,n-1}B_{3,n-1}^{e_{n-1}} = F_{n-1}C_{3,n-1}B_{3,n-1}^{k}B_{3,n-1}^{e_{n-1}-k} \\ &= \gamma'_{l_3}B_{3,n-1}^{e_{n-1}-k} \to \ldots \to \gamma'_{l_4}B_{3,n-1}^{e_{n-1}-k} = F_{n-1}C_{3,n-1}B_{3,n-1}^{e_{n-1}-k}\eta \mod I_{n-1} \end{aligned}$$

However we have now found a different equivalence for $S_{n-1}C_{3,n-1}$ containing F_{n-1}, which contradicts the induction hypothesis.
We now instead assume S_{n-1} appears in γ'_{l_4}. We know $\gamma'_{l_4} = S_{n-1}C_{3,n-1}\eta$, $\eta \in P_{n-1}$. Note that we still have $\eta \neq B_{3,n-1}^{k}$. Once more we will use lemma 5.2.1. We obtain the following path:

$$\begin{aligned} S_{n-1}C_{3,n-1} &\to \ldots \to F_{n-1}C_{3,n-1}B_{3,n-1}^{e_{n-1}} = F_{n-1}C_{3,n-1}B_{3,n-1}^{k}B_{3,n-1}^{e_{n-1}-k} \\ &= \gamma'_{l_3}B_{3,n-1}^{e_{n-1}-k} \to \ldots \to \gamma'_{l_4}B_{3,n-1}^{e_{n-1}-k} = S_{n-1}C_{3,n-1}B_{3,n-1}^{e_{n-1}-k}\eta \mod I_{n-1} \end{aligned}$$

If $\eta \neq 1$ or $k \neq e_{n-1}$, we again have a contradiction with the induction hypothesis. This is because we have a different equivalence for $S_{n-1}C_{3,n-1}$ containing S_{n-1}. If, however, we assume $\eta = 1$ and $k = e_{n-1}$ then $S_{n-1}C_{3,n-1}B_{3,n-1}^{e_{n-1}-k} = S_{n-1}C_{3,n-1}$ and we do not get a contradiction. The path presented does contain a repetition, but this can be fixed easily:

$$F_{n-1}C_{3,n-1}B_{3,n-1}^{e_n} = \gamma'_{l_3} \to \ldots \to \gamma'_{l_4} = S_{n-1}C_{3,n-1} \mod I_{n-1}$$

Indeed this is the only valid option for γ'_{l_4}. We now have:

$$\gamma_{l_4} = C_{i,n}Q_{3,n}B_{1,n}^{e_{n-1}}B_{1,n-1}^{e_{n-1}-1}S_{n-1}C_{3,n-1}.$$

By the induction hypothesis and the non-repetition requirement we know we must use an equivalence of level n. We have two options, (1d) and (1e). We first show why the latter is impossible.
If we apply (1e) we are left with:

$$C_{i,n}Q_{4,n}B_{1,n}^{e_{n-1}}B_{1,n-1}^{e_{n-1}-1}F_{n-1}C_{4,n-1}B_{4,n-1}$$

We can now only apply (1f) of level $n-1$, with our resulting monomial being of height $n-2$. Next, we again reason that there is a minimal $\hat{\gamma}$ for which we return to height $n-1$ by (3d). Once more we can exclude several variables for reasons given before. We have $\gamma_{l_4} = C_{i,n}Q_{4,n}B_{1,n}^{e_{n-1}}B_{1,n-1}^{e_{n-1}-1}\gamma'_{l_4}$. with $\gamma'_{l_4} = F_{n-1}C_{4,n-1}B_{4,n-1}$. We can now apply the same reasoning that was previously used to determine $k = e_n$, to conclude there is no $\hat{\gamma}'$ of level $n-1$ to get to without repetition, as we now have $k = 1$ set in stone.

In conclusion we must use (1d):

$$\gamma_{l_4+1} = C_{i,n}Q_{2,n}B_{1,n}^{e_{n-1}}B_{1,n-1}^{e_{n-1}-2}B_{4,n-1}S_{n-1}C_{2,n-1}.$$

We can now apply either (1a) of level $n-1$ or (1b) of level n. The latter would be impossible by the same reasoning used to show (1e) was impossible just before. This time with $k = e_{n-1} - 1$ instead of 1. We thus apply (1a), resulting in $h(\gamma_{l_4+2}) = n-2$. Now if we let $\gamma'_{l_4+1} = C_{i,n}Q_{2,n}B_{1,n-1}^{e_{n-1}-2}S_{n-1}C_{2,n-1}$, such that $\gamma_{l_4} = B_{1,n}^{e_{n-1}}B_{4,n-1}\gamma'_{l_4+1}$. Observe $\gamma'_{l_4+1}B_{1,n-1} = \gamma_{l_1+1}$. We now note that the argumentation to get from γ_{l_1+1} to γ_{l_4} still holds even with the additional $B_{1,n}^{e_{n-1}}B_{4,n-1}$ and loss of $B_{1,n-1}$. Combining the fact that we must use equivalences applicable to γ'_{l_4+1} and the fact that we can reuse the argumentation from before, we must run through the same sequence of steps as before. We can repeat this process an arbitrary number of $0 \leq k \leq e_n - 1$ times. However for $k < e_n - 1$ we will repeatedly be forced to take the same step we took to get from γ_{l_4} to γ_{l_4+1} as our $B_{4,n-1}$ is not large enough. We conclude we must run through the process exactly $e_n - 1$ times in total, and end up with a γ_{l_5}:

$$\gamma_{l_5} = C_{i,n}Q_{3,n}B_{1,n}^{e_{n-1}\cdot e_{n-1}}S_{n-1}C_{3,n-1}B_{4,n-1}^{e_{n-1}-1}$$

Unlike before, (1d) is no longer possible as we are out of $B_{1,n-1}$'s. So we must apply (1e). If we also recall $e_n^2 = e_{n+1}$ we find

$$\gamma_{l_5+1} = C_{i,n}Q_{4,n}B_{1,n}^{e_n}F_{n-1}C_{4,n-1}B_{4,n-1}^{e_{n-1}}$$

We can now only apply (1f) of level $n-1$, such that $h(\gamma_{l_5+2}) = n-2$. We use (3d) to find there is a minimal γ_{l_6} such that $h(\gamma_{l_6}) = n-1$. As before we have several variables that will remain unused in this subpath, and can focus on:

$$F_{n-1}C_{4,n-1}B_{4,n-1}^{e_{n-1}} = \gamma'_{l_5+1} \to \ldots \to \gamma'_{l_6} \mod I_{n-1}$$

The induction hypothesis tells us $\gamma'_{l_6} = S_{n-1}C_{4,n-1}$ and thus:

$$\gamma_{l_6} = C_{i,n}Q_{4,n}B_{1,n}^{e_n}S_{n-1}C_{4,n-1}$$

We must use an equivalence of level n by the induction hypothesis in order to avoid repetition. Our only option for this turns out to be (1f) due to the presence of $Q_{4,n}$:

$$\gamma_{l_6+1} = C_{i,n}B_{1,n}^{e_n}F_n$$

So $\gamma_{l_6+1} = \gamma_{l_r}$ and

$$\gamma_{l_r} = F_nC_{i,n}B_{1,n}^{e_n}$$

which is exactly what we wanted to show.
Since n and i were arbitrary we can conclude this holds for all i as well as all n by induction. □

Thus we have proven what we set out to proof and can move on to the next part of the proof.

5.2.3 The Required Leading Term

Before we start there is one more preliminary thing to show. This is Lemma 3.3 in the previously mentioned paper by Möller and Mora [8], where it is given without proof on page 182.

Lemma 5.2.6. We work in the scenario presented in Section 5.2.1. Then:

$$Q_{3,n+1}C_{i,n+1}C_{3,n}S_nB_{i,n+1}^{e_n} - Q_{2,n+1}C_{i,n+1}C_{2,n}S_n \in J_n \text{ for all } i \in [1,4], \text{ and all } n \geq 1$$

Proof. We prove this by considering the polynomials as equivalences. We just need to show:

$$Q_{3,n+1}C_{i,n+1}C_{3,n}S_nB_{i,n+1}^{e_n} \equiv Q_{2,n+1}C_{i,n+1}C_{2,n}S_n \mod J_n \text{ for all } i \in [1,4], \text{ and all } n \geq 1$$

This is done as follows. Fix an arbitrary $i \in [1,4]$ and $n \geq 1$. Now:

$$\begin{aligned}
Q_{3,n+1}C_{i,n+1}C_{3,n}S_nB_{i,n+1}^{e_n} &\equiv Q_{3,n+1}C_{i,n+1}C_{3,n}F_nB_{i,n+1}^{e_n}B_{3,n}^{e_n} && \text{by Lemma 5.2.1}\\
&\equiv Q_{2,n+1}C_{i,n+1}C_{2,n}F_nB_{i,n+1}^{e_n}B_{3,n}^{e_n} && \text{by } (1c)\\
&\equiv Q_{2,n+1}C_{i,n+1}C_{2,n}F_nB_{2,n}^{e_n} && \text{by } (1g)-(1j)\\
&\equiv Q_{2,n+1}C_{i,n+1}C_{2,n}S_n && \text{by Lemma 5.2.1}
\end{aligned}$$

Note that we do use equivalences (1c) and (1g) - (1j) of level $n+1$, but since we are working in J_n this is fine. □

Now it is time for the main result. This is adapted from Proposition 3.4 from the paper by Möller and Mora [8], where only a sketch of the proof is given. Here, I give a full proof of the lemma.

Lemma 5.2.7. We work in the setting presented in Section 5.2.1. Then for all n, we have that any Gröbner basis of J_n must contain an element of degree at least $\frac{e_n}{2} + 4$

Proof. First fix an arbitrary $n \geq 1$ and $i \in [1,4]$. Then by Lemma 5.2.6 we find:

$$Q_{3,n+1}C_{i,n+1}C_{3,n}S_nB_{i,n+1}^{e_n} - Q_{2,n+1}C_{i,n+1}C_{2,n}S_n \in J_n \text{ for all } i \in [1,4], \text{ and all } n \geq 1$$

In particular we have $\Phi = Q_{3,n+1}C_{i,n+1}C_{3,n}S_nB_{i,n+1}^{e_n} \in \mathrm{LT}(J_n)$. We can assume the Gröbner basis is made up exclusively of binomials, as the ideal is generated exclusively by binomials. Because of this there must be a binomial in the Gröbner basis, say $\Psi - \beta$ with $\Psi > \beta$ such that Ψ divides Φ. Now we recall that both terms in every polynomial generating J_n contains either an S or F, because of this, this holds for every polynomial in J_n too. From this we know S_n must be present in Ψ, because none of the other S or F divide Φ. I.e. we have:

$$\Psi - \beta = \eta S_n - \beta$$

with ηS_n divides Φ. Additionally we need β to have total degree equal to, or smaller than the total degree than Ψ. We will investigate the possibilities for β. We do this by considering equivalences once again. We define the path:

$$\eta S_n = \gamma_0 \to \ldots \to \gamma_r = \beta \mod J_n$$

First we note that for any η meeting the requirements, it does not contain any S or F. Additionally it does not contain any $Q_{i,n}$, thus we can conclude the only equivalence applicable to γ_0 is (1a) of level n. We have:

$$\gamma_1 = \eta Q_{1,n}S_{n-1}C_{1,n-1}$$

Now suppose no γ ever returns to having an S or F of level n or higher. Then we will not be able to use $Q_{3,n+1}$, $C_{i,n+1}$ or $B_{i,n+1}$ anywhere in the rest of the derivation. We split into two cases:

1. $\phi(\eta, C_{3,n}) = 0$. In this case the path reduces to:

$$\eta S_n = \eta\gamma_0' \to \ldots \to \eta\gamma_r' = \beta \mod I_n$$

Note we can say it is $\mod I_n$ and not $\mod J_n$ since all equivalences in $J_n \setminus I_n$ require an S or F of level n, which we will never have after γ_0 by assumption in either case. Now we need $|\beta| \leq |\eta S_n|$ for our leading term conditions. Note that because $\phi(\eta, C_{3,n}) = 0$, all variables in η will remain untouched during this path. Furthermore, because of us being forced to start with (1a) of level n, we know γ'_1 contains a $Q_{1,n}$. However the only way to "get rid of" a Q of level n is to use equivalence (1a) or (1b) of level n, in which case we'd have an S or F of level n again, violating our assumption. Thus γ'_l, for all l, contains some kind of S or F and a $Q_{1,n}$, but then $\gamma'_r = \beta$ does too. Thus β contains at least two variables on top of the variables in η, and thus $|\beta| > |\eta S_n|$. This means we can never find a desired β like this.

2. $\phi(\eta, C_{3,n}) = 1$. In this case the path reduces to:

$$\eta S_n = \eta' \gamma'_0 \to \ldots \to \eta \gamma'_r = \beta \mod I_n$$

with $\eta = \eta' C_{3,n}$, and thus $\gamma'_0 = S_n C_{3,n}$.
Now the same reasoning holds true here as in the previous case, with the additional observation that no equivalence in I_n "gets rid of" a C of level n that is present. i.e. β contains at least three variables, an S or F, a C of level n and $Q_{1,n}$, on top of the other variables in η that are not $C_{3,n}$. In conclusion $|\beta| > |\eta S_n|$. This means we can never find a desired β like this.

After ruling out these cases we now know with certainty that, if such a β exist, we must at some point in the path have an S or F of level n or higher. We further know at least one such β will exist (see the polynomial whose leading term we are attempting to divide). Let γ_{l_1} be the smallest l such that γ_l contains an S or F of level n or higher. We observe that in order to get an S of level $n+1$ one must use (1a) of level $n+1$. In particular we see that we must need an S of level n before. Additionally no equivalences containing S or F of levels higher than $n+1$ and n exist respectively Thus we can conclude γ_{l_1} contains specifically an S_n or F_n. Then we once more split into two cases:

1. $\phi(\eta, C_{3,n}) = 0$. In this case the path reduces to:

$$\eta S_n = \eta \gamma'_0 \to \ldots \to \eta \gamma'_{l_1} \mod I_n$$

We can restrict ourselves to working $\mod I_n$ for the same reasons as before. And because this entire subpath is $\mod I_n$ we are allowed to exclude η from it, as none of its potential terms can be used in an equivalence $\mod I_n$. However, now suppose $\gamma'_{l_1} = \xi S_n$, with $\xi \neq 1$ (otherwise we would have a repetition), then we would have the equivalence:

$$S_n \equiv \xi S_n \mod I_n \implies S_n C_{3,n} \equiv \xi S_n C_{3,n} \mod I_n$$

which contradicts Lemma 5.2.5. For similar reasons if $\gamma'_{l_1} = \xi F_n$ then $\xi = B_{3,n}^{e_n}$ is the only choice. This would also contradict Lemma 5.2.5 because we can obtain the equivalence:

$$S_n \equiv \xi F_n = F_n B_{3,n}^{e_n} \mod I_n$$

which implies the equivalence:

$$S_n C_{2,n} \equiv \xi F_n C_{2,n} = F_n C_{2,n} B_{3,n}^{e_n} \mod I_n$$

In conclusion this case can not occur, and thus we know. $\phi(\eta, C_{3,n}) = 1$

2. $\phi(\eta, C_{3,n}) = 1$. In this case we would have to find a path of the form:

$$S_n C_{3,n} = \gamma'_0 \to \ldots \to \gamma'_{l_1} \mod I_n$$

being able to work $\mod I_n$ for the same reasons as before. But now we know by Lemma 5.2.5 the only choice for γ'_{l_1} is $F_n C_{3,n} B_{3,n}^{e_n}$.

Indeed we find

$$\gamma_{l_1} = \eta_1 F_n C_{3,n} B_{3,n}^{e_n}$$

with η_1 such that $\eta_1 S_n C_{3,n}$ must divide Φ. More specifically η_1 must divide $Q_{3,n+1} C_{i,n+1} B_{i,n+1}^{e_n}$

We now move on from γ_{l_1}. Recall that none of the other possible variables in η can play a role if we were to use (1f) of level n, meaning we would only be able to return to $S_nC_{3,n}$ or $F_nC_{3,n}B_{3,n}^{e_n}$. Thus we must use some other equivalence. The only possibility is (1c). This can only be used if η contains $Q_{3,n+1}$, but since we have ruled out all other possibilities this must be the case. We find:

$$\gamma_{l_1+1} = \eta_2 Q_{2,n+1} F_n C_{2,n} B_{3,n}^{e_n}$$

with η_2 such that η_2 must divide $C_{i,n+1}B_{i,n+1}^{e_n}$.

We now could use (1f) of level n, however, by the same reasons as before, there must be a minimal l_2 such that γ_{l_2} contains an S or F of level n. Now note that in the subpath from γ_{l_1+1} to γ_{l_2}, all present F or S will be of level strictly less than n. Thus $C_{2,n}$ and $B_{3,n}^{e_n}$ can only be affected by (1h) and (1i) of level n respectively, however, they would need a $B_{2,n}$ or $C_{3,n}$ respectively in order to use these equivalences. But neither of these variables can ever come up in this subpath. We conclude that we can simply look at the path:

$$F_n = \gamma'_{l_1+1} \to \ldots \to \gamma'_{l_2} \mod I_n$$

But, by similar reasons to before, we already know γ'_{l_2} must be F_n itself in order to not contradict Lemma 5.2.5. And because we don't want any repetition we conclude we must use an equivalence other than (1f) of level n on γ_{l_1+1}.

Our only option avoiding repetition is then one of (1g) - (1j), depending on the choice of i. However, the only way to use one of these equivalences is for η to contain $C_{i,n+1}$ and $B_{i,n+1}^k$, for some $k \in [1, e_n]$. We now finally have narrowed down the list of possible Ψ to just:

$$\Psi = Q_{3,n+1}C_{i,n+1}C_{3,n}S_nB_{i,n+1}^k$$

for some $k \in [1, e_n]$.
We have:

$$\gamma_{l_1+2} = C_{i,n+1}Q_{2,n+1}F_nC_{2,n}B_{3,n}^{e_n-1}B_{i,n+1}^{k-1}B_{2,n}$$

Now suppose we repeatedly apply (1g) - (1j) exactly q times, with $q \in [1, k]$. We have:

$$\gamma_{l_2} = \gamma_{l_1+1+q} = C_{i,n+1}Q_{2,n+1}F_nC_{2,n}B_{3,n}^{e_n-q}B_{i,n+1}^{k-q}B_{2,n}^q$$

Then we can only apply either (1f) of level n or (1b) of level $n+1$.
First I show why this last case will lead to a dead end.

Suppose we do apply (1b) of level $n+1$, then, as the next step, we have to apply (1f) of level n. Now either there is a minimal $l_3 > l_2$ such that γ_{l_3} contains an S or F of level n, or the rest of the derivation to β never contains any S or F of level n. Let $\gamma_{l_3} = \gamma_r$ in this latter case. Then in the subpath:

$$\gamma_{l_2} \to \ldots \to \gamma_{l_3} \mod J_n$$

we can limit ourselves to:

$$F_nC_{3,n}B_{3,n}^{e_n-q} = \gamma'_{l_2} \to \ldots \to \gamma'_{l_3} \mod I_n$$

This is because no variable of level $n+1$ will be used, and $B_{2,n}$ requires a $C_{2,n}$ to be used, which will never appear. However, in the case γ'_{l_3} did contain an S or F of level n, then we would either have a repetition, or a contradiction with Lemma 5.2.5 (I won't go into the details, but the reasoning is just as the other times Lemma 5.2.5 was used to obtain a contradiction). Thus $\gamma'_{l_3} = \gamma'_r \implies \gamma_{l_3} = \gamma_r$. However, we now know $\beta = C_{i,n+1}Q_{3,n+1}B_{i,n+1}^{k-q}B_{2,n}^q\xi$ for some ξ with $|\xi| \geq 2$. We know this about ξ, because ξ must contain some S or F as well as a C of level n. But then:

$$|\Psi| = \left|Q_{3,n+1}C_{i,n+1}C_{3,n}S_nB_{i,n+1}^k\right| = k+4 < k+5 = \left|C_{i,n+1}Q_{3,n+1}B_{i,n+1}^{k-q}B_{2,n}^q\xi\right| = |\beta|$$

This contradicts the requirement that Ψ is the leading term of $\Psi - \beta$, thus this scenario is impossible.

Instead assume we apply (1f) of level n. Now just as in the case we just ruled out we will do the following: Either there is a minimal $l_3 > l_2$ such that γ_{l_3} contains an S or F of level n, or the rest of the derivation to β never contains any S or F of level n. Let $\gamma_{l_3} = \gamma_r$ in this case. Then in the subpath:

$$\gamma_{l_2} \to \ldots \to \gamma_{l_3} \mod J_n$$

we can limit ourselves to:

$$F_n C_{2,n} B_{2,n}^q = \gamma'_{l_2} \to \ldots \to \gamma'_{l_3} \mod I_n$$

This is because no variable of level $n+1$ will be used, and $B_{3,n}$ requires a $C_{3,n}$ to be used, which will never appear. If $q = e_n$, then in particular also $q \leq k \leq e_n \implies k = e_n$, meaning

$$\Psi = Q_{3,n+1} C_{i,n+1} C_{3,n} S_n B_{i,n+1}^{e_n} = \Phi \tag{4}$$

This is the trivial option for Ψ. We will return to this case in the end, for now we continue looking for potential options with lower degree.

Let us instead assume $q < e_n$, then we know $\gamma'_{l_3} = \gamma'_r \implies \gamma_{l_3} = \gamma_r = \beta$ else we would either have a repetition, or a contradiction with Lemma 5.2.5 (for similar reasons as before). It is now important to note that γ'_r will still contain $C_{2,n}$, as it can only be changed by an equivalence of level $n+1$. Now we define:
$M \subset [1, e_n]$ (which may be empty) such that if $m \in M$ then there exists an α such that $\phi(\alpha, S_n) + \phi(\alpha, F_n) = 0$, $|\alpha| \leq 2m - e_n + 1$ and:

$$\alpha C_{2,n} \equiv C_{2,n} F_n B_{2,n}^m \tag{5}$$

Note that $|\alpha| \geq 1$, since it must contain an S or F. Because of this we will have if $m \in M$ then

$$1 \leq |\alpha| \leq 2m - e_n + 1 \implies m \geq \frac{e_n}{2}$$

If we have $q < m$ for all $m \in M$, then, by (5) the only equivalences we can reach (and use) are of the form:

$$\alpha C_{2,n} \equiv C_{2,n} F_n B_{2,n}^j$$

for $j \leq q$ with $|\alpha| \geq 2j - e_n + 1$.

Then we know $j \geq \frac{e_n}{2}$, and find:

$$\begin{aligned} |\beta| &= \left| C_{i,n+1} Q_{2,n+1} B_{3,n}^{e_n - q} B_{i,n+1}^{k-q} B_{2,n}^{q-j} \gamma'_{l_3} \right| \\ &= |\alpha| + 3 + e_n - q + k - q + q - j \geq 2j - e_n + 4 + e_n + k - q - j = j + k - q + 4 \geq \frac{e_n}{2} + 4 \end{aligned}$$

Here we used $k \geq q \geq j \geq \frac{e_n}{2}$ and $|\alpha| \geq 2j - e_n + 1$. So indeed, regardless of what equivalences are possible (outside of the ones purposefully excluded) the degree of β is already larger than or equal to $\frac{e_n}{2} + 4$, so if we want Ψ to be the leading term, it must too have degree of at least $\frac{e_n}{2} + 4$.

Instead now assume there is at least one $m \in M$ such that $q \geq m$. This then means $k \geq q \geq \frac{e_n}{2}$. Which means:

$$|\Psi| = \left| Q_{3,n+1} C_{i,n+1} C_{3,n} S_n B_{i,n+1}^k \right| \geq \left| Q_{3,n+1} C_{i,n+1} C_{3,n} S_n B_{i,n+1}^{\frac{e_n}{2}} \right| = \frac{e_n}{2} + 4$$

In conclusion, if we want $|\Psi| \geq |\beta|$ we must have:

$$\Psi = Q_{3,n+1} C_{i,n+1} C_{3,n} S_n B_{i,n+1}^k \text{ with } k \geq q \geq \frac{e_n}{2}$$

Which means:

$$|\Psi| \geq \frac{e_n}{2} + 4$$

which is exactly what we needed to show. □

Regardless of n, all elements in J_n have degree at most $d+2$. Additionally, I have shown that J_n's Gröbner basis contains an element of at least degree $\frac{e_n}{2}+4 = \frac{d^{2^n}}{2}+4$. Indeed we have double exponential growth.

6 Symmetry

So far one thing has been made clear: generally there are always Gröbner bases that are hard to compute. A question one could then ask is: under what circumstances can we guarantee Gröbner bases won't be hard to compute? I will be looking at one such case, which is the application of symmetry. First I take a look at how the previous examples fare under symmetry, then I discuss some theoretical results I have found, before finally talking about experimental results obtained using Mathematica.

6.1 Breaking the Examples

A good indication of the potential of applying symmetry is how it completely breaks the examples from the last section.

6.1.1 d^2

In order to show the example no longer works under symmetry, we need the following lemma:

Lemma 6.1.1. If we have $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$, such that the sum of the coefficients for any g_i is 0. Then the coefficients of $\sum_{i=1}^{m} f_i g_i$ sum up to 0 too, for any $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$.

Proof. First we just consider one of the $f_i g_i$. This itself is a sum of terms (i.e. monomials with a coefficient) in $k[x_1, \ldots, x_n]$ multiplied by g_i. Now we observe for one of these terms if we multiply g_i with it, then every coefficient in g_i gets multiplied by the same constant. This means that the coefficients still add up to 0. Since this holds for every term in f_i, it will hold for the entirety of f_i too. And indeed, since it holds for all f_i, it will hold for $\sum_{i=1}^{m} f_i g_i$. This all follows from every addition adding a net zero total to the sum of coefficients.
In conclusion, the sum of the coefficients of $\sum_{i=1}^{m} f_i g_i$ is 0. □

Now if we apply symmetry to the example from Section 5.1 we can obtain the following result:

Lemma 6.1.2. Suppose

$$I = \langle \mathrm{Sym}(x, y, z, w)\{f_1, f_2, f_3\}\rangle = \langle \mathrm{Sym}(x, y, z, w)\{x^{n+1} - yz^{n-1}w, xy^{n-1} - z^n, x^n z - y^n w\}\rangle.$$

then the reduced Gröbner basis G of I contains no polynomials of degree larger than n.

Proof. In order to show this I will investigate possible leading terms. Recall the cycle notation for symmetries introduced in Section 2.6.

First we can use symmetries of f_2 to get both x^n and y^n as leading monomials:

$$(x, z, y, w)f_2 = -y^n + zw^{n-1}$$
$$(x, z)f_2 = -x^n + zy^{n-1}$$

With a bit of cancellation we can get z^n as a leading monomial as well:

$$f_2 - (z, w)f_2 = xy^{n-1} - z^n - (xy^{n-1} - w^n) = -z^n + w^n$$

Furthermore, we find the following terms as leading terms:

$$\begin{aligned} f_2 &= xy^{n-1} - z^n \\ (x,y)f_2 &= x^{n-1}y - z^n \\ (z,w,y)f_2 &= xz^{n-1} - w^n \\ (x,z,w,y)f_2 &= x^{n-1}z - w^n \\ (z,w,x)f_2 &= y^{n-1}z - w^n \\ (y,z,w,x)f_2 &= yz^{n-1} - w^n \end{aligned}$$

And using some more cancellation we can also find:

$$\begin{aligned} (y,w)f_2 - (x,y,w)f_2 &= xw^{n-1} - z^n - (yw^{n-1} - z^n) = xw^{n-1} - yw^{n-1} \\ (y,x,w)f_2 - (y,w)f_2 &= wx^{n-1} - z^n - (xw^{n-1} - z^n) = wx^{n-1} - xw^{n-1} \\ (x,y,w,z)f_2 - (z,x)(y,w)f_2 &= yw^{n-1} - x^n - (zw^{n-1} - x^n) = yw^{n-1} - zw^{n-1} \\ (x,w)f_2 - (y,w,x)f_2 &= wy^{n-1} - z^n - (yw^{n-1} - z^n) = wy^{n-1} - yw^{n-1} \\ (x,z)(y,w)f_2 - (z,x)f_2 - (x,z,w)f_2 &= zw^{n-1} - x^n - (y^{n-1}z - x^n) - (y^{n-1}z - w^n) = zw^{n-1} - w^n \\ (x,w)(y,z)f_2 - (y,z)f_2 - (y,z,w)f_2 &= z^{n-1}w - y^n - (xz^{n-1} - y^n) - (xz^{n-1} - w^n) = z^{n-1}w - w^n \end{aligned}$$

In particular, we now observe any term in $\mathrm{Sym}(x,y,z,w)\{f_1,f_2,f_3\}$ is divisible by one of these leading terms, with the exception of w^m for some m. This is because every term is of degree at least n, and contains a power of a variables which is of degree at least $n-1$. Indeed, since I have shown that all terms of degree n such that a variables has a power of $n-1$ can be leading terms (excluding w^n), we have that every term is divisible (excluding a power of w).

Now we just need to show w^m can never be a leading term for any m, and then we will have everything covered. Suppose there is a polynomial that is both a combination of the f_i and has w^m as leading term. Since w is the smallest variable given our ordering, a power of it can only be a leading term if it is a polynomial in $k[w]$. We want to get a polynomial of the form $h = \sum_{i=1}^{m} \alpha_i w^i$ for some m, with at least 1 nonzero α_i. We now note that f_1, f_2 and f_3 are homogeneous, because of this no cancellation can occur between polynomials that contain w^i and w^j for $i \neq j$. We can thus conclude that every term in h can be obtained by itself from a homogeneous combination of polynomials in $\mathrm{Sym}(x,y,z,w)\{f_1,f_2,f_3\}$. I.e:

$$w^m = \sum_{\sigma \in \mathrm{Sym}(x,y,z,w)} p_\sigma \sigma f_1 + q_\sigma \sigma f_2 + r_\sigma \sigma f_3$$

$p_\sigma, q_\sigma, r_\sigma \in k[x,y,z,w]$ homogeneous. More importantly we have that a sum of polynomials whose coefficients sum to 0, results in a polynomial with 1 as the sum of coefficients. However, as seen Lemma 6.1.1 this is impossible. We conclude w^m cannot be a leading term for any m.

Now for all terms shown to be leading terms, there is a polynomial in the reduced Gröbner basis with leading term that divides this term. Suppose there was still some polynomial of degree greater than n in this reduced Gröbner basis, then we must have that all of its terms cannot be divided by the leading terms of any of the other polynomials in the Gröbner basis. However, as discussed earlier, almost every term of degree larger than n that is present in the ideal is divisible by one such leading term. The lone exception being a power of w which we already know can't be a leading term. Thus we conclude that such a polynomial of degree at least $n+1$ does not exist in the Gröbner basis. □

6.1.2 d^{2^n}

Lemma 6.1.3. Recall the scenario presented in Section 5.2.1. We apply symmetry over all variables to the generating polynomials of J_n and call the newly obtained ideals $\tilde{J}_n$. Then, the Gröbner basis of $\tilde{J}_n$ contains no polynomials of degree larger than 2.

Proof. Fix some $n \geq 0$ We can use the polynomials $f_1 = S_n - Q_{1,n}S_{n-1}C_{1,n-1}$ and $f_2 = Q_{1,n}F_{n-1}C_{1,n-1}B_{1,n-1} - Q_{2,n}S_{n-1}C_{2,n-1}$ to get (the squares of) all variables as leading term. This can be seen as follows: Let $x, y_1, y_2, y_3, z_1, z_2, z_3$ be some variables in P_n. Then since the variables inside either polynomials all appear only once, we have the following polynomials in $\tilde{J}_n$

$$\begin{aligned} x - y_1y_2y_3 \\ xz_1z_2z_3 - y_1y_2y_3 \\ x - z_1z_2z_3 \end{aligned}$$

If we now just take:

$$x \cdot (x - z_1z_2z_3) + xz_1z_2z_3 - y_1y_2y_3 - (x - y_1y_2y_3) = x^2 - x$$

Indeed we have x^2 as the leading term. And since it was arbitrary we can get any variable as leading term. □

Remark. It is actually possible to get first powers of most variables as a leading term, but this does not matter for showing how the degree of the Gröbner basis is bounded by 2.

6.2 Theoretical Results

6.2.1 A Look at Leading Terms

When it comes to Gröbner bases, leading terms are hugely important. Indeed, if we can show some ideal I has a polynomial with leading term x^α, then we know any Gröbner basis must contain a polynomial with a leading term that divides x^α. Then, by the definition of the reduced Gröbner basis, we can conclude that the reduced Gröbner basis of I contains only one term in one polynomial that is divisible by x^α. In particular this means we know several higher order terms (those that are divisible by x^α) will not be present in any polynomial in the reduced Gröbner basis. Thus, if we are able to say certain terms are a leading term for a polynomial in I, we can then greatly reduce the amount of possible high-degree polynomials that might be in the reduced Gröbner basis.

Example 6.2.1. For a simple example, take $f = x^2 + y \in k[x, y, z]$, with grevlex order $(x > y > z)$. Then it is trivial to see that x^2, y^2 and z^2 are in $\mathrm{LT}(\mathrm{Sym}(x, y, z)(f))$. Now every term of degree greater than 3 is divisible by either x^2, y^2 or z^2. Because of this we can conclude the reduced Gröbner basis of $\langle \mathrm{Sym}(x, y, z)(f) \rangle$ contains no polynomials of degree higher than 3.

The main goal of this section is thus to try and find as many leading terms as possible in an attempt to rule out higher degree terms from being leading terms.

First I will look at what symmetries can be applied while keeping the same leading term.

Lemma 6.2.2. Let $x^\alpha > x^\beta$ be two monomials in $k[x_1, \ldots, x_n]$ with $|x^\alpha| = |x^\beta|$. We use grevlex ordering with $x_1 > \ldots > x_n$. Define m as the largest integer such that $\alpha_m < \beta_m$. Let $\pi : [1, n] \to [1, n]$ be an injective function such that:

1. $\pi(x_i) \geq x_i$ if $\alpha_i > 0$.
2. $\pi(x_m) \leq x_m$.

Then $\pi(x^\alpha) > \pi(x^\beta)$.

Proof. Suppose a function π meets all the conditions, but $\pi(x^\alpha) < \pi(x^\beta)$. Then there is an i_0 such that $\pi(x_{i_0}^{\alpha_{i_0}}) > \pi(x_{i_0}^{\beta_{i_0}})$ and $\pi(x_i^{\alpha_i}) = \pi(x_i^{\beta_i})$ for all i such that $\pi(x_i) < \pi(x_{i_0})$. We know that $\pi(x_m) \leq x_m$, and since $\alpha_m < \beta_m$ we find $\pi(x_m^{\alpha_m}) < \pi(x_m^{\beta_m})$. This last inequality implies $x_m \geq \pi(x_m) > \pi(x_{i_0}) \geq x_{i_0}$. But now $\alpha_{i_0} > \beta_{i_0}$ and with the assumption that $\alpha_i = \beta_i$ for all $i > m$, we must conclude $\beta \geq \alpha$. This contradicts the assumption that $\alpha < \beta$, and thus we conclude $\pi(x^\alpha) > \pi(x^\beta)$. □

We can now use Lemma 6.2.2 in order to deduce symmetries that preserve the leading term:

Lemma 6.2.3. Let $f \in k[x_1, \ldots, x_n]$. We use grevlex ordering with $x_1 > \ldots > x_n$. Let $x^\alpha = \mathrm{LT}(f)$. Then if we have an injective function $\pi : [1, n] \to [1, n]$ such that:

1. $\pi(x_i) \geq x_i$ if $\alpha_i > 0$.
2. $\pi(x_m) \leq x_m$ for all $m \in \{m \in \mathbb{N} \mid \exists_{x^\beta \text{ term in } f} : |\alpha| = |\beta|,\ \alpha_m < \beta_m, \text{ and } \forall_{i>m}\ \alpha_i \geq \beta_i\ \}$.

Then $\pi(\mathrm{LT}(f))$ is a leading term for a polynomial in $\mathrm{Sym}(n)F$.

Proof. Since π is injective we know it is a symmetry and thus $\pi(f) \in \mathrm{Sym}(n)F$. Then by Lemma 6.2.2 we know $\pi(\mathrm{LT}(f)) > \pi(x^\beta)$ for all x^β terms in f with $\left|x^\beta\right| = \left|\mathrm{LT}(f)\right|$. Since this transformation does not change the total degree, we also have: $\left|x^\beta\right| < \left|\mathrm{LT}(f)\right| \implies \left|\pi(x^\beta)\right| < \left|\pi(\mathrm{LT}(f))\right|$. And of course no terms with total degree larger than $\mathrm{LT}(f)$ exist in the first place. Thus in conclusion the leading term of $\pi(f)$ is $\pi(\mathrm{LT}(f))$. □

In essence we now know that if we can get a symmetry of a term, say $\pi_0(x^\alpha)$ as a leading term, then we can get (most) symmetries such that $\pi(x^\alpha) > \pi_0(x^\alpha)$ as a leading term too. In order to take advantage of this we try to find the "smallest symmetry" that can still be a leading term.

While it is hard to say anything in the general case, under a few assumptions we can get fairly small symmetries as leading terms. Two methods are presented below:

Lemma 6.2.4 (A method to get small leading terms using exclusive variables)**.** Let $f \in k[x_1, \ldots, x_n]$ be a polynomial. We use grevlex ordering with $x_1 > \ldots > x_n$. Let x^α be a term in f such that, if x^β has exactly the same variables with a nonzero power as x^α, we have $|\alpha| > |\beta|$. We use $x_{m_1}, \ldots, x_{m_p}$ to denote the variables present in x^α, ordered such that $\phi(x^\alpha, x_{m_i}) \geq \phi(x^\alpha, x_{m_j})$ if $i > j$. Additionally let x_{m_l} be a variable only present in x^α (and the x^β previously mentioned) with the lowest power. I.e. $\phi(x^\alpha, x_{m_l}) < \phi(x^\alpha, x_{m_i})$ for all $i \in [1, p]$ such that $\phi(x^\beta, x_{m_i}) = 0$ for all other x^β terms in f. Finally let x_q be a variable that is not found in any term, besides x^α, with total degree larger than or equal to that of x^α. x_q need not be present in x^α. Then we can get a symmetry of x^α as leading term.

Proof. We consider two cases:

1. First, we assume $\phi(x^\alpha, x_q) = 0$, i.e. x_q appears in no term in f of relevant total degree. We now create the following symmetry

$$\begin{aligned} \pi(x_{m_{p-i}}) &= x_{n-i} \text{ if } i \in [0, p-l-1] \\ \pi(x_{m_l}) &= x_{n-p+1} \\ \pi(x_{m_{p-i}}) &= x_{n-i+1} \text{ if } i \in [p-l+1, p-1] \\ \pi(x_q) &= x_{n-p} \end{aligned}$$

   This can indeed be extended to a symmetry, as no variable here gets mapped to twice, or gets mapped twice itself. Now take:

$$f' = \pi(f) - (x_{n-p+1}, x_{n-p})\pi(f).$$

   First we note that the variables present in $\pi(x^\alpha)$ are exactly $x_n, x_{n-1}, \ldots x_{n-p+1}$. Next we note that all terms in f with $|\beta| \geq |\alpha|$, outside of x^α, do not contain x_{m_l} and x_q, Thus all terms in $\pi(f)$ with $|\beta| \geq |\alpha|$, other than $\pi(x^\alpha)$, do not contain $\pi(x_{m_l}) = x_{n-p+1}$ and $\pi(x_q) = x_{n-p}$. This means that $\pi(x^\beta) = (x_{n-p+1}, x_{n-p})\pi(x^\beta)$ for all $\beta \neq \alpha$ with $|\beta| \geq |\alpha|$. In particular we find that all these terms get cancelled by themselves in f'. This just leaves $\pi(x^\alpha)$, $(x_{n-p+1}, x_{n-p})\pi(x^\alpha)$ and terms with $|\beta| < |\alpha|$, meaning $\pi(x^\alpha) > \pi(x^\beta)$. Finally, since $x_{n-p} > x_{n-p+1}$, we find that $(x_{n-p+1}, x_{n-p})\pi(x^\alpha) > \pi(x^\alpha)$. In conclusion, $(x_{n-p+1}, x_{n-p})\pi(x^\alpha)$ is the leading term of f'.

2. Now we assume $\phi(x^\alpha, x_q) > 0$ and let $x_q = x_{m_{l_1}}$. We assume w.l.o.g. $l > l_1$, which also means $\phi(x^\alpha, x_{m_l}) \geq \phi(x^\alpha, x_{m_{l_1}})$. We now create the following symmetry:

$$\begin{aligned}
\pi(x_{m_{p-i}}) &= x_{n-i} \text{ if } i \in [0, p-l-1] \\
\pi(x_{m_l}) &= x_{n-p+2} \\
\pi(x_{m_{p-i}}) &= x_{n-i+1} \text{ if } i \in [p-l+1, p-l_1-1] \\
\pi(x_{m_{l_1}}) &= x_{n-p+1} \\
\pi(x_{m_{p-i}}) &= x_{n-i+2} \text{ if } i \in [p-l_1+1, p-1]
\end{aligned}$$

This can indeed be extended to a symmetry, as no variable here gets mapped to twice, or gets mapped twice itself. Now take:

$$f' = \pi(f) - (x_{n-p+2}, x_{n-p+1})\pi(f).$$

First, we note that the variables present in $\pi(x^\alpha)$ are exactly $x_n, x_{n-1}, \ldots x_{n-p+1}$. Next we note that all terms in f with $|\beta| \geq |\alpha|$, outside of x^α do not contain x_{m_l} and $x_{m_{l_1}}$. Thus all terms in $\pi(f)$ with $|\beta| \geq |\alpha|$, other than $\pi(x^\alpha)$, do not contain $\pi(x_{m_l}) = x_{n-p+2}$ and $\pi(x_{m_{l_1}}) = x_{n-p+1}$. This means that $\pi(x^\beta) = (x_{n-p+2}, x_{n-p+1})\pi(x^\beta)$ for all $\beta \neq \alpha$ with $|\beta| \geq |\alpha|$. In particular we find that all these terms get cancelled by themselves in f'. This just leaves $\pi(x^\alpha)$, $(x_{n-p+2}, x_{n-p+1})\pi(x^\alpha)$ and terms with $|\beta| < |\alpha|$, meaning $\pi(x^\alpha) > \pi(x^\beta)$. Since $\phi(x^\alpha, x_{m_l}) \geq \phi(x^\alpha, x_{m_{l_1}})$ we have $x_{n-p+1} > x_{n-p+2}$ and find that $\phi(\pi(x^\alpha), x_{n-p+2}) \geq \phi(\pi(x^\alpha), x_{n-p+1})$. Furthermore we have $\phi(\pi(x^\alpha), x_{n-p+1}) \geq \phi(\pi(x^\alpha), x_{n-p+2})$. Indeed $\pi(x^\alpha)$ and $(x_{n-p+2}, x_{n-p+1})\pi(x^\alpha)$ are nearly identical, the latter just has a larger variable with a potentially larger power, and a smaller variable with a potentially smaller power. From this we conclude $(x_{n-p+2}, x_{n-p+1})\pi(x^\alpha) > \pi(x^\alpha)$. In conclusion $(x_{n-p+2}, x_{n-p+1})\pi(x^\alpha)$ is the leading term of f'.

□

Lemma 6.2.5 (A method to get small leading terms using excess variables)**.** Let $f \in k[x_1, \ldots, x_n]$ be a polynomial. We use grevlex ordering with $x_1 > \ldots > x_n$. Let x^α be a term in f such that, if x^β contains all the variables x^α does, then $|\alpha| > |\beta|$. We use $x_{m_1}, \ldots, x_{m_p}$ to denote the variables present in x^α, ordered such that $\phi(x^\alpha, x_{m_i}) \geq \phi(x^\alpha, x_{m_j})$ if $i > j$. Additionally let there be q variables not found in any term of f : $x_{l_1}, \ldots, x_{l_q}$. We assume x^α has no exclusive variables, otherwise see Lemma 6.2.4.
Now I present the following algorithm, which, on input of a polynomial, term in the polynomial, and ordered tuples of the variables x_{m_i} and x_{l_i} as described above, returns a symmetry of a given term x^α that is a leading term in $\mathrm{Sym}(n)f$:

Algorithm 3: Algorithm for finding small leading term using excess variables

input : $f \in k[x_1, \ldots, x_n]$, x^α term in f, $(x_{m_1}, \ldots x_{m_p}) \subset \{x_1, \ldots, x_n\}$ all variables in x^α ordered as before, $(x_{l_1}, \ldots, x_{l_q}) \subset \{x_1, \ldots, x_n\}$ variables not present in f.

output: $\pi(x^\alpha)$, a small leading term.

1 $F = \{x^\beta \mid x^\beta \neq x^\alpha$ term in f, such that $|\beta| \geq |\alpha|\}$
2 $F' = F$
3 $\pi = (1)$
4 $i = p$
5 $ii = n$
6 $G = \{\}$
7 **while** $i \geq 1$ **do**
8 $RQ =$ False
9 **for** $x^\beta \in F'$ **do**
10 $AV =$ True
11 **for** $j \in [1, i-1]$ **do**
12 **if** $\phi(x^\beta, x_{m_j}) = 0$ **then**
13 $AV =$ False
14 **break**
15 **if** AV **then**
16 $RQ = AV$
17 $F' = F' \setminus \{x^\beta\}$
18 **if** RQ **then**
19 $G = G \cup x_{m_i}$
20 **else**
21 $\pi(m_i) = ii$
22 $ii = ii - 1$
23 $i = i - 1$
24 **if** $p - n + ii > q$ **then**
25 **return** *"Not enough free variables"*
26 $i = p$
27 $ii = ii - 1$
28 **while** $i \geq 1$ **do**
29 **if** $x_{m_i} \in G$ **then**
30 $\pi(m_i) = ii$
31 $ii = ii - 2$
32 $i = i - 1$
33 **return** $\pi(x^\alpha)$

Proof. First it is clear to see that the algorithm does terminate, as there is no recursion. We now show that the term obtained at the end is the leading term of a polynomial in $\mathrm{Sym}(n)f$. Split the set of x_{m_i} into two as follows:

$$x_{m_{1,i}} = x_{m_{j_i}} \text{ with } j_i = \min\{j \mid x_{m_j} \notin G \cup \{x_{m_{1,1}}, \ldots, x_{m_{1,i-1}}\}\}) \qquad \text{for } i \in [1, p_1]$$
$$x_{m_{2,i}} = x_{m_{j_i}} \text{ with } j_i = \min\{j \mid x_{m_j} \notin G^c \cup \{x_{m_{2,1}}, \ldots, x_{m_{2,i-1}}\}\}) \qquad \text{for } i \in [1, p_2]$$

where G is the G in the algorithm after the first while loop has finished. In essence, the $x_{m_{1,i}}$ are the variables for which RQ is not true, ordered just like x_{m_i} was. Similarly the $x_{m_{2,i}}$ are the variables for which RQ is true, also ordered just like x_{m_i} was. Note $p_1 + p_2 = p$
We now know that after the first while loop (up to line 23) we have the following π:

$$\pi(x_{m_{1,i}}) = x_{n-i+1}$$

We will assume l is large enough, otherwise the algorithm returns that no symmetry can be obtained (using this method).

We now create the following π_0:

$$\begin{aligned} \pi_0(x_{m_{1,i}}) &= x_{n-i+1} && \text{for } i \in [1, p_1] \\ \pi_0(x_{m_{2,i}}) &= x_{n-p_1-2i+2} && \text{for } i \in [1, p_2] \\ \pi_0(x_{l_i}) &= x_{n-p_1-2i+1} && \text{for } i \in [1, p_2] \end{aligned}$$

Note that $n \geq p_1 + p_2 + q \geq p_1 + p_2 + p_2$ which means that the smallest possible index for an x is exactly x_1, thus no problems occur with the indexing here. Additionally we still have injectivity, meaning π_0 can be extended to a symmetry.
We can now start creating the polynomial that will have our desired leading term:

$$f_0 = \pi_0(f)$$

We now let:

$$f_i = f_{i-1} - (x_{n-p_1-2i+2}, x_{n-p_1-2i+1}) f_{i-1} = \pi_{i-1} f - \pi_i(f)$$

Consider f_{p_2}. I will show that every term of this polynomial is a symmetry of a term of f which contains all variables $x_{m_{2,i}}$, $i \in [1, p_2]$.

Take some arbitrary $i \in [1, p_2]$. Now note that x_{l_i} is not present in any term of f, and thus $\pi(x_{l_i}) = x_{n-p_1-2i+1}$ is not present in any term of f_0. It also does not get affected by any symmetry applied before f_i, and thus we have x_{n-p_1-2i+1} is not present in any term in f_{i-1}. Because of this any term in f_{i-1} that does not contain x_{n-p_1-2i+2} gets cancelled. In fact terms of this form are the only terms that get cancelled. This is because all terms containing x_{n-p_1-2i+2} before transformation, contain x_{n-p_1-2i+1} after transformation. And these terms cannot cancel any term in f_{i-1} after transformation, since those terms strictly do not contain x_{n-p_1-2i+1}. In particular, we have that any symmetry of any term in f not containing $x_{m_{2,i}}$ does not appear in f_i. Now, for f_j, $j > i$, we again have that at no point x_{n-p_1-2i+1} or x_{n-p_1-2i+2} get affected by one of the symmetries applied. Meaning that for all $j > i$ any symmetry of any term in f not containing $x_{m_{2,i}}$ does not appear in f_j.

We can run through this argument for all i to find that any symmetry of any term in f not containing all of the $x_{m_{2,i}}$, $i \in [1, p_2]$, does not appear in f_{p_2}. Additionally we have that symmetries of x^α are still present in f_{p_2} as they do contain all the $x_{m_{2,i}}$, $i \in [1, p_2]$.

Now suppose there is still another term in f such that a symmetry of this term appears in f_{p_2}. If this term is a symmetry of x^α, no problem. If it is a term such that $|\beta| < |\alpha|$, again no problem. Suppose instead it is a symmetry of a term, x^β in f with $|\beta| \geq |\alpha|$, and $\beta \neq \alpha$. What this means is that x^β contains all the $x_{m_{2,i}}$. We can then further assume $G \neq \{x_{m_1}, \ldots, x_{m_p}\}$, because if this were to be the case, we'd have a contradiction with the maximality of x^α (i.e. x^β contains all the variables x^α does, but is larger). Because of this we know there is a variable that is present in x^α, but not x^β. Let i^* be minimal such that $x_{m_{i^*}}$ is in x^α, but not x^β. Now, since $x_{m_{i^*}}$ is minimal, we know for all $i < i^*$ x_{m_i} is in x^β. But then, according to the algorithm RQ is true for $x_{m_{i^*}}$ (line 12 would be false for all x_{m_i} with x^β, meaning AV will be true, and thus so would RQ while in the $i = i^*$ part of the loop). This would then mean $x_{m_{i^*}}$ is one of the $x_{m_{2,i}}$, meaning it is present in x^β. This is a contradiction, and thus we conclude such a x^β does not exist.

Finally we have shown f_{p_2} contains only symmetries of x^α, and terms with a lower total degree than x^α. We now just need to investigate which symmetry of x^α will be the leading term. Consider $\pi_1(x^\alpha)$, we know this is larger than $\pi_0(x^\alpha)$ because all we do is switch out a smaller variable for a larger one. This same reasoning holds true for all $\pi_i(x^\alpha)$ as each time we swap out a variable in $\pi_{i-1}(x^\alpha)$ for a larger one. Because of this we can conclude $\pi_{p_2}(x^\alpha) > \pi_i(x^\alpha)$ for all $i \in [1, p_2 - 1]$, and thus $\pi_{p_2}(x^\alpha)$ is the leading term of f_{p_2}. If we now consider what π_{p_2} does we find:

$$\begin{aligned} \pi_{p_2}(x_{m_{1,i}}) &= x_{n-i+1} && \text{for } i \in [1, p_1] \\ \pi_{p_2}(x_{m_{2,i}}) &= x_{n-p_1-2i+1} && \text{for } i \in [1, p_2] \end{aligned}$$

which is exactly the π the algorithm outputs. □

An slightly expanded implementation of this algorithm in Mathematica, using adaptations of small bits of code found on StackExchange [9, 10, 11]. This expansion being that it can also output the polynomial of which the obtained term is the leading term. This implementation can be found in Appendix A , along with a function to determine for which terms in a given polynomial the algorithm can work.

Both of these lemmas require some sort of free variable, and only apply to single polynomials. This may make them seem rather weak in the context of all possible ideals. However, the real power of these two lemmas comes from applying them to pre-processed polynomials. E.g. if we work in an ideal generated by $\mathrm{Sym}(n)(\{f_1, \ldots, f_m\}) \subset k[x_1, \ldots, x_n]$, we can take a polynomial combination of the $f = \sum_{i=1}^{m} p_i f_i$. By cleverly choosing the p_i we might be able to cancel terms and/or variables that would otherwise prevent the lemmas from being used, and then apply one of the lemmas to this f.

6.2.2 Degree 1

Degree 1 polynomials, in other words the linear case, was discussed in general in Section 4.2. Because of this, the affect of symmetry in the degree 1 case is not important in and of itself. However, by observing what tricks symmetry allows us to perform in this simple case, we can get a feel for how symmetry might affect Gröbner bases in general. This is what this section is about. Attempting to prove the Gröbner bases are easy to compute, by using options given to us by symmetry.

We consider a set of polynomial $F = \{f_1, \ldots, f_m\} \in k[x_1, \ldots, x_n]$. such that all f_i are of degree at most 1. I.e. we have:

$$f_i = \sum_{j=1}^{n} a_{j,i} x_j + a_{0,i}$$

where $a_i \in k$ for all $i \in [0, m]$. We use grevlex ordering with $x_1 > \ldots > x_n$
W.l.o.g. we assume none of the polynomials is a multiple of another, meaning:

$$f_i - b f_j \neq 0 \text{ for all } i \neq j \in [1, m], \text{ and } b \in k$$

What can we say about Gröbner bases of $I = \langle \mathrm{Sym}(n) F \rangle$ in general?

First if we have $f_i = 1$ for some i, then clearly the reduced Gröbner basis would just be $\{1\}$.

Assume $f_i \neq 1$ for all i, this means there is a j for all i such that $a_{j,i} \neq 0$. If there is just one such j for an i, then we can trivially get any x_i as a leading term. Instead assume there are at least two j for all i such that $a_{j,i} \neq 0$. If for any fixed i all $a_{i,j}$ are equal or 0 for all j (i.e. $a_{i,j} = c$ or $a_{i,j} = 0$ for all j), then up to multiplication with a constant, we either have that the only polynomials in F can be:

$$\sum_{j=1}^{l} x_j$$

$$\sum_{j=1}^{l} x_j + b_i$$

for some $l \in [2, n]$ using symmetry.
Now, if we have that for some l one of both are present, we can get 1 as a leading term and we are done. We have $G = \langle 1 \rangle$. The same holds if we have multiple of the last kind.
If instead we have that for any l only one of the given options is present, then depending on what l

we have, we can get:

$$\sum_{j=1}^{l_0} y_j$$

$$\sum_{j=1}^{l_0} x_j + b_i$$

for some $l_0 \in [2, n]$ by taking linear combinations. Here however we take l_0 to be minimal. Then we will have $G = \langle \sum_{j=1}^{l_0} x_j \rangle$ or $G = \langle \sum_{j=1}^{l_0} x_j + b_i \rangle$.

Now instead assume there is an f_i with j_1, j_2 such that $a_{j_1,i} \neq a_{j_2,i}$. Note that if there is some f_i such that $a_{j,i} = 0$ for some $j \geq 1$, then we can use Lemma 6.2.4. We conclude x_{n-1} can be a leading term, and using Lemma 6.2.3 we know x_i is a leading term in general, for all $i \geq 2$.
Furthermore, using our assumption with j_1, j_2 from before, we can obtain:

$$f_i - b_1(x_{j_1}, x_{j_2}) f_i = x_{j_1} - x_{j_2}$$

Using this we can in particular get the polynomials:

$$x_n - x_i \text{ for all } i \in [1, n-1]$$

by symmetry.
Now suppose we have some polynomial:

$$\sum_{j=1}^{n} a_{j,i} x_j + a_{0,i}$$

We can then do the following:

$$\sum_{j=1}^{n} a_{j,i} x_j + a_{0,i} + \left(\sum_{l=1}^{n-1} a_{l,i}(x_n - x_l) \right) = \sum_{l=1}^{n} a_{l,i} x_n + a_{0,i}$$

which will have x_n as leading term assuming $\sum_{l=1}^{n} a_{l,i} \neq 0$. Meaning we can get all variables as leading terms themselves, and thus $G = \{x_1, \ldots, x_n\}$.
If, on the other hand, there is no polynomial for which this inequality does holds, then we can't get x_n as a leading term like this. If, in this case, we have a polynomial with $a_{0,i} \neq 0$, then we find

$$\sum_{j=1}^{n} a_{j,i} x_j + a_{0,i} + \left(\sum_{l=1}^{n-1} a_{l,i}(x_n - x_l) \right) = a_{0,i}$$

and we conclude $G = \{1\}$. Finally if for all polynomials we additionally have $a_{0,i} = 0$ we then find:

$$\sum_{j=1}^{n} a_{j,i} x_j + a_{0,i} + \left(\sum_{l=1}^{n-1} a_{l,i}(x_n - x_l) \right) = 0$$

for all f_i. This means we can write all f_i as a linear combination of $x_{j_1} - x_{j_2}$ for $j_1, j_2 \in [1, n]$. In particular this means $F \subset \langle \{(x_{j_1} - x_{j_2} \mid j_1, j_2 \in [1, n]\} \rangle$. Using our way to get $x_{j_1} - x_{j_2}$ from before we can conclude $I = \langle \{(x_{j_1} - x_{j_2} \mid j_1, j_2 \in [1, n]\} \rangle$, for which we know a power of x_n can never be the leading term due to Lemma 6.1.1. In conclusion here too the Gröbner basis is of degree 1.

Finally if we have for all i that all $a_{j,i}, j \in [1, n]$ are not zero, then, since there is an f_i with j_1, j_2 such that $a_{j_1,i} \neq a_{j_2,i}$, we can just take:

$$f_i - (x_{j_1}, x_{j_2}) f_i = x_{j_1} - x_{j_2}$$

to end up in the scenario just discussed.

6.2.3 Degree 2

In addition to investigating the linear case, I will also take a look at what we can say about the Gröbner basis of an arbitrary ideal spanned by polynomials of at most degree 2.

I will first look at the case of just two variables, as the general case turns out to be quite complicated already, and the single variable case does not change under symmetry.
We consider a set of polynomials $F = \{f_1, \dots, f_m\} \subset k[x, y]$. such that all f_i are of degree at most 2. We will assume there is at least 1 polynomial in F which is actually of degree 2, otherwise see the section on degree 1 polynomials. We use grevlex ordering with $x > y$
W.l.o.g. we assume none of the polynomials are a multiple of another, meaning:

$$f_i - bf_j \neq 0 \text{ for all } i \neq j \in [1, m], \text{ and } b \in k$$

What can we say about Gröbner bases of $I = \langle \text{Sym}(x, y)F \rangle$ in general?

The way we will be tackling this question is by investigating the possible leading terms. First, trivially, if one of the f_i has a constant as a leading term, this means the ideal is just the entire ring, and thus the Gröbner basis G is of degree 0. If there is some combination of the f_i, say g, such that g is of degree 1 we can perform a trick similar to one we used for the general linear case (i.e. in Section 4.2). Indeed if g is of degree one, we can consider the quotient ring:

$$k[x, y]/\langle g \rangle$$

which will be isomorphic to $k[x]$ (or $k[y]$, but they are in essence the same). Of course for the single variable case the Gröbner basis will just be the gcd, which is bounded by the degree of the polynomials. Because of this, the degree of the Gröbner basis will be bounded by 2 if there is a degree 1 polynomial in F.
We can now assume all polynomials in F are of degree 2. Next, if some combination of the f_i results in a y^2 leading term, then, by Lemma 6.2.3, we can also get x^2 as a leading term. Now every term of degree at least 3 is divisible by one of these two terms, and something that divides them must be a leading term in the Gröbner basis. This allows us to conclude that the Gröbner basis will be of degree at most 2. Finally we can are down to just three cases:

1. We can only get x^2 as a leading term.
2. We can only get xy as a leading term.
3. We can get both x^2 and xy as leading terms.

1. If we can only get x^2 as a leading term, then we can only have f_i of the form:

   $$f_i = x^2 + a_1xy + a_2y^2 + a_3x + a_4y + a_5$$

   Furthermore, we can only have one such polynomial, otherwise we can subtract one from the other and end up with a polynomial with a different leading term (recall we already excluded polynomials that were the same as another up to a constant). Under the symmetry (x, y) we will find the polynomial:

   $$(x, y)f_i = a_2x^2 + a_1xy + y^2 + a_4x + a_3y + a_5$$

   Now if we take:

   $$\begin{aligned} a_2 \cdot f_i - (x, y)f_i &= a_2x^2 + a_1a_2xy + a_2^2y^2 + a_3a_2x + a_4a_2y + a_5a_2 - a_2x^2 - a_1xy - y^2 - a_4x - a_3y - a_5 \\ &= a_1(a_2 - 1)xy + (a_2^2 - 1)y^2 + (a_3a_2 - a_4)x + (a_4a_2 - a_3)y + a_5(a_2 - 1) \end{aligned}$$

   which means $a_2 = \pm 1$, otherwise y^2 would be the leading term (or xy, either way not x^2). Additionally we also need $a_3 = \pm a_4$, we find:

   $$f_i = x^2 + a_1xy \pm y^2 + a_3x \pm a_3y + a_5$$

which is identical under symmetry up to a minus sign (note if $a_2 = 1$, then $a_3 = a_4$ and $a_2 = -1 \implies a_3 = -a_4$. Because of this $\mathrm{Sym}(x, y)F$ is made up of just a single polynomial, for which the Gröbner basis will be this single polynomial too. So in this case we do have a bound of 2 on the degree of the Gröbner basis.

2. If we can only get xy as the leading term, then we can only have f_i of the form:

$$f_i = xy + a_2y^2 + a_3x + a_4y + a_5$$

Just as before we know only one such polynomial will exist. Now, first, $a_2 = 0$, otherwise $(x, y)f_i$ will have x^2 as leading term, which we assumed was not possible. Furthermore if we take:

$$f_i - (x, y)f_i = xy + a_3x + a_4y + a_5 - xy - a_4x - a_3y - a_5 = (a_3 - a_4)(x - y)$$

we find $a_3 = a_4$, in order to not get a different leading term. But now we find:

$$f_i = xy + a_3x + a_3y + a_5$$

Which is identical under symmetry. Indeed again we find $\mathrm{Sym}(x, y)F$ consists of just a single polynomial, and we have that the Gröbner basis is bounded by degree 2.

3. If we only have xy and x^2 as possible leading terms, then we will have f_i of one of the following forms:

$$f_1 = x^2 + a_1xy + a_2y^2 + a_3x + a_4y + a_5$$
$$f_2 = xy + b_2y^2 + b_3x + b_4y + b_5$$

If only one of the two is present, we can use a combination of the polynomial and a symmetry of it to obtain the other case (otherwise we would never get the other leading term). Because of this we can assume both polynomials are present in F. We can then, w.l.o.g., assume $a_1 = 0$, by subtracting f_2 from f_1 if needed. We now consider the S-polynomial $S(f_1, f_2)$:

$$\begin{aligned} S(f_1, f_2) = yf_1 - xf_2 &= a_2y^3 + a_3xy + a_4y^2 + a_5y - b_2xy^2 - b_3x^2 - b_4xy - b_5x \\ &= -b_2xy^2 + a_2y^3 - b_3x^2 + (a_3 - b_4)xy + a_4y^2 - b_5x + a_5y \end{aligned}$$

First, if $b_2 \neq 0$, we will cancel the term xy^2 by applying the division algorithm, resulting in a polynomial with no terms greater than xy^2. Possibly this polynomial is 0, but then we have $\overline{S(f_1, f_2)}^F = 0$, which means we are done as we soon see.

In either case we end up with a polynomial with only y^3 and/or terms of lower degree. If we have y^3 as leading term we are again done, this is because at least one of x^2 and y^3 will divide any given monomial of degree 4. We find the degree of the Gröbner basis is bounded by 3.

Instead assume the resulting polynomial is made up exclusively of terms of degree 2 or lower. In this case, we have three options. Either x^2 is the leading term, xy is the leading term or $\overline{S(f_1, f_2)}^F = 0$. All other cases are not possible, as they would lead to different leading terms. In the first two cases we conclude the polynomial must be a multiple of f_1 or f_2 respectively, otherwise we would be able to get a different leading term. This means $\overline{S(f_1, f_2)}^F = 0$. So we find $\overline{S(f_1, f_2)}^F = 0$ in all three cases, which means $F = \{f_1, f_2\}$ is already a Gröbner basis, with degree at most 2.

In conclusion the degree of the polynomials in the reduced Gröbner basis for degree 2 polynomials with 2 variables is bounded by at most 3.

A similar approach can be used for the 3 variable case. Suppose we have $k[x, y, z]$, with grevlex $x < y < z$ ordering. Then we can first exclude the possibility of degree 1 leading terms. As previously explained, these leading terms would allow us to reduce the problem to a polynomial

ring in 2 variables, which was already covered. Additionally we can exclude the leading term z^2, as Lemma 6.2.4 would tell us that x^2 and y^2 would both be leading terms as well, resulting in a degree bound of 3 on the reduced Gröbner basis (note xyz could still be a leading term in the reduced Gröbner basis). We have now reduced the general case to just the case where we can have any combination of leading terms from x^2, y^2, xy, xz, zy. Following this, we can reason about the form of these polynomials based on what leading terms appear, and likely reach similar conclusions as in the 2 variable case. However, there are some difficulties we run into here. For one, we now have 5 possible leading terms, as opposed to just 2 in the 2 variable case. Considering we can take any combination of these possible leading terms, there are quite a lot of cases to consider. Furthermore, some of these cases will have more than 2 polynomial generating the ideal, which is something we were able to avoid in the 2 variable case. This will lead to more S-polynomials which need to be considered, were we to go down that route.

It may well be possible to get conclusive results on the 3 variable case, and perhaps even beyond, but the amount of cases to consider will grow rapidly.

6.3 Experimental Results

In addition to theoretically investigating what happens under symmetry, I also tried to find examples of ideals that, even under symmetry, would have large Gröbner basis. Largely inspired by the example from Section 5.1, I tried various polynomials, using Mathematica to compute the Gröbner bases. Again, using adaptations of a few bits of code found on Stack Exchange [9, 10]. In this section I present some of the results and observations I made. The full (relevant) results can be found in Appendix B.

6.3.1 Quasi-Polynomial Growth

The first interesting result comes from taking f_2 from the example in Section 5.1 and applying symmetry to it (working in $k[x, y, z]$ as opposed to $k[x, y, z, w]$ in the example). The degree of the resulting Gröbner basis exhibits quasi-polynomial growth of the form:

$$\begin{aligned} 2n-1 \text{ for } n = 0 \mod 3 \\ 2n-2 \text{ for } n = 1 \mod 3 \\ n+1 \text{ for } n = 2 \mod 3 \end{aligned}$$

By investigating the difference between the Gröbner bases for $n = 3, 4, 5$ we can determine why, for $n = 2 \mod 3$, the degree is smaller. Indeed for $n = 5$ no polynomial has a leading term of the form xz^k or yz^k (and this seems to persist for larger n with $n = 2 \mod 3$ as well). Unfortunately I was not able to discover why these terms can only be the leading for certain kinds of n, however it likely is due to certain cancellation steps requiring more than one power of z.

6.3.2 Adding a Constant

Interestingly, when adding a constant (under some constraints soon to be explained) in front of one of the terms of f_2, the Gröbner basis of the ideal under symmetry has a much smaller degree. In particular the degree is exactly $n + 2$. To get an idea of why this happens I present the following lemma and its proof:

Lemma 6.3.1. Let $f_n = cx^{n-1}y - z^n \in k[x, y, z]$, with $c \in k, c^3 \neq 1$ and $c \neq 0$. We consider $I_n = \langle \mathrm{Sym}(x, y, z)(f_n) \rangle$. Then, for any $n \geq 3$ we have $z^{n+2} \in I_n$.

Proof. We take the following combination of symmetries of f_n, using cycle notation:

$$y \cdot (x, y, z)f_n + \frac{1}{c} \cdot x \cdot f_n + \frac{1}{c^2} \cdot z \cdot (x, z, y)f_n = y \cdot (cy^{n-1}z - x^n) + \frac{1}{c}x \cdot (cx^{n-1}y - z^n) + \frac{1}{c^2}z \cdot (cz^{n-1}x - y^n)$$
$$= cy^n z - x^n y + x^n y - \frac{1}{c}xz^n + \frac{1}{c}xz^n - \frac{1}{c^2}zy^n = (c - \frac{1}{c^2})zy^n$$

Now since $c^3 \neq 1$ we have $c - \frac{1}{c^2} \neq 0$, and thus $zy^n \in I$
Next we show $y^{n+1}z - z^{n+2} \in I$:

$$z^2 \cdot f_n - yz \cdot (y,z)f_n = cx^{n-1}yz^2 - z^{n+2} - cx^{n-1}yz^2 + y^{n+1}z = y^{n+1}z - z^{n+2}$$

Combining these two observations we can then conclude $z^{n+2} \in I$. □

In this proof we see why adding a constant can make such a difference, we are able to "loop" around, subtracting symmetries, without all terms cancelling.

6.3.3 $m(n-1)+1$

Playing around with f_2 a bit more ended up giving way to a polynomial whose Gröbner basis (degree) grows at a consistent rate regardless of n. This polynomial being:

$$x^{n-1}y + y^{n-1}x - z^n$$

If we let $I = \langle \mathrm{Sym}(x,y,z)(x^{n-1}y + y^{n-1}x - z^n)\rangle$, then the Gröbner basis of I is of degree $3n-2$. This idea behind this polynomial can be implemented in rings with more variables too, indeed for $k[x,y,z,w]$ we can consider the polynomial:

$$x^{n-1}y + x^{n-1}w + y^{n-1}x + y^{n-1}w + w^{n-1}x + w^{n-1}y - z^n$$

Since the Gröbner basis here becomes hard to compute very quickly (see the 113+ terms with absurdly huge coefficients for $n = 6$ in appendix), I was only able to test up to $n = 10$, but the pattern here does appear to be $4n-3$. Again because of the long computation time I was not able to see if this pattern holds for more than 5 variables, but I can conjecture the following:
If we take

$$f = \sum_{i=1}^{m-1} \sum_{j=1, j\neq i}^{m-1} x_i^{n-1}x_j - x_m^n$$

Then the Gröbner basis of $I = \langle \mathrm{Sym}(m)f\rangle \subset k[x_1,\ldots,x_m]$ contains a polynomial of degree $m(n-1)+1$. It is worth pointing out that for $m = 2, n = 2$ no set of polynomials will have a Gröbner basis with polynomial whose degree exceeds $m(n-1)+1 = 3$, as was seen in Section 6.2.3. Similarly for degree 1 we find $m(n-1)+1 = 1$, which was also shown to be an upperbound on the degree of a reduced Gröbner basis. Of course for higher degrees and more variables things are likely to get more complicated, and I would expect there to be ideals whose Gröbner basis degree exceeds $m(n-1)+1$, but at least for the simpler cases this strategy appears to be relatively good.
This example does illustrate an idea that might lead finding a truly hard to compute example. This idea boils down to "fighting fire with fire". In order to counteract the symmetry from having any affect, we simply "build in" symmetry beforehand in the original polynomial.

7 Conclusion

In conclusion we have seen proof that, in the general case, the degree of the polynomials of a Gröbner basis can grow very fast. However, the results found in this report suggest that, under symmetry, the degree might not be able to grow nearly as quickly. The previously mentioned examples completely fall apart. This is due to the investigated examples being based on all the variables having individual roles. Under symmetry this is lost, as all variables are almost the same. However, the variables are not quite one and the same. This is due to the monomial ordering, which remains unaffected by symmetry.

Further research into the affects of symmetry on Gröbner bases could focus on trying to generalize some of the tricks used in sections 6.2.2 and 6.2.3, or trying to devise better ways to approach these problems. Additionally, a possible proof or counterexample of the $m(n-1)+1$ conjecture presented in Section 6.3.3 could be investigated. Of course, examples that grow even faster could also be found.

In the end, I feel confident that, for an ideal under symmetry, the degree of polynomials in the reduced Gröbner basis will have a lower upper bound, and will not be able to exhibit double exponential growth. I believe this, in part because there are far fewer possible ideals, especially ones with nontrivial Gröbner bases, and in part because the variables lose most of their individuality that was used in constructing the examples discussed.

References

[1] B. Buchberger. '"Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal"'. PhD thesis. University of Innsbruck, 1965.

[2] E.W. Mayr and A.R. Meyer. 'The complexity of the word problems for commutative semigroups and polynomial ideals'. In: *Advances in Mathematics* 46.3 (1982), pp. 305–329. DOI: 10.1016/0001-8708(82)90048-2. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-0001751788&doi=10.1016%5C%2f0001-8708%5C%2882%5C%2990048-2&partnerID=40&md5=9f1331a76c0008e82f2611b198bad0d0.

[3] D. A. Cox, J. B. Little and D. O'Shea. *Ideals, varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Berlin: Springer, 2015. DOI: 10.1007/978-3-319-16721-3. URL: https://doi.org/10.1007/978-3-319-16721-3.

[4] J.-C. Faugère. 'A new efficient algorithm for computing Gröbner bases (F4)'. In: *Journal of Pure and Applied Algebra* 139.1 (1999), pp. 61–88. DOI: 10.1016/S0022-4049(99)00005-5. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-0033143274&doi=10.1016%5C%2fS0022-4049%5C%2899%5C%2900005-5&partnerID=40&md5=303b1d8280d00db7219b92ca186e4f5a.

[5] J.-C. Faugère. 'A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)'. In: *Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC* (2002), pp. 75–83. DOI: 10.1145/780506.780516. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-0036045901&doi=10.1145%5C%2f780506.780516&partnerID=40&md5=55bafd8cb9fc7d36af2b74bcab1e2194.

[6] Alessandro Giovini et al. '"One Sugar cube, Please" or Selection Strategies in the Buchberger Algorithm.' In: Jan. 1991, pp. 49–54. DOI: 10.1145/120694.120701.

[7] D. Lazard. 'Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations'. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 162 LNCS (1983), pp. 146–156. DOI: 10.1007/3-540-12868-9_99. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034440461&doi=10.1007%5C%2f3-540-12868-9%5C_99&partnerID=40&md5=0608ff3c8d114d833e23c2b9920d2425.

[8] H.M. Möller and F. Mora. 'Upper and lower bounds for the degree of Groebner bases'. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 174 LNCS (1984). cited By 60, pp. 172–183. DOI: 10.1007/BFb0032840. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85027674077&doi=10.1007%5C%2fBFb0032840&partnerID=40&md5=0301dd22dd08f962fe3af484f6f1c83d.

[9] StackExchange. *How do I find the degree of a multivariable polynomial automatically?* URL: https://mathematica.stackexchange.com/questions/14925/how-do-i-find-the-degree-of-a-multivariable-polynomial-automatically.

[10] StackExchange. *Symmetric group action on polynomials*. URL: https://mathematica.stackexchange.com/questions/79268/symmetric-group-action-on-polynomials.

[11] StackExchange. *Nested sorting of lists*. URL: https://mathematica.stackexchange.com/questions/182235/nested-sorting-of-lists.

A Implementation of Algorithm in Mathematica

```
SmallSymmetry[f_, \[Alpha]_, X_, polyresult_] :=
 Module[{totdeg, preXm, Xm, Xl, monos, i, ii, iii, j, \[Pi],
   lt, \[FormalX], p, n, q, F, Fprime, remF, G, RQ, AV, h},
  totdeg =
   Exponent[# /. ((# -> \[FormalX] RandomReal[]) & /@ {#}), \
\[FormalX]] &[\[Alpha]];

  (*Verify chosen polynomial + ring combination makes sense*)
  If[\[Not] SubsetQ[X, Variables[f]],
   Return["Chosen polynomial is not in chosen polynomial ring"]];

  (*Set up the ordered tuples of variables*)
  preXm = Variables[\[Alpha]];
  Xl = Complement[X, Variables[f]];
  Xm = {};
  For[i = 1, i <= Length[preXm], i++,
   AppendTo[
    Xm, {preXm[[i]],
     Exponent[# /. ((# -> \[FormalX] RandomReal[]) & /@ \
{preXm[[i]]}), \[FormalX]] &[\[Alpha]]}]];
  Xm = Sort[Xm, #1[[-1]] < #2[[-1]] &];
  Xm = First /@ Xm;

  (*Define several useful constants*)
  q = Length[Xl];
  p = Length[Xm];
  n = Length[X];

  (*Set up the list of relevant terms in f*)
  monos = MonomialList[f];
  F = {};
  For[i = 1, i <= Length[monos], i++,
   If[Exponent[# /. ((# -> \[FormalX] RandomReal[]) & /@ {#}), \
\[FormalX]] &[monos[[i]]] >= totdeg, AppendTo[F, monos[[i]]]]];
  F = Complement[F, {\[Alpha]}];
  Fprime = F;
  (*Verify the chosen monomial is actually a term in f*)
  If[\[Not] MemberQ[monos, \[Alpha]],
   Return["Chosen monomial not a term in f"]];

  (*Initialize several variables for the while loop*)
  \[Pi] = {};
  i = p;
  ii = n;
  G = {};

  (*While loop checking which variables will need to be used for \
cancellation*)
  While[i >= 1,
   RQ = False;
   remF = {};
   For[iii = 1, iii <= Length[Fprime], iii++,
```

```
    AV = True;
    For[j = 1, j <= i - 1, j++,
     (*Check if given variable is present in given term*)
     If[Exponent[# /. ((# -> \[FormalX] RandomReal[]) & /@ \
{Xm[[j]]}), \[FormalX]] &[Fprime[[iii]]] == 0,
      AV = False;
      Break]];
    If[AV,
     RQ = AV;
     (*Remove terms whose cancellation has already been dealt with*)
     AppendTo[remF, Fprime[[iii]]]]];
   If[RQ,
    AppendTo[G, Xm[[i]]],
    AppendTo[\[Pi], {Xm[[i]], X[[ii]]}];
    ii = ii - 1];
   Fprime = Complement[Fprime, remF];
   i = i - 1];

  (*Verify there are enough free variables*)
  If[p - n + ii > q, Return["Not enough free variables"]];
  i = p;
  ii = ii - 1;

  (*Set up resulting polynomial if enabled*)
  If[polyresult, h = f /. Thread[First /@ \[Pi] -> Last /@ \[Pi]]];

  (*While loop assigning the variables used for cancellation their \
mapping*)
  While[i >= 1,
   If[MemberQ[G, Xm[[i]]],
    AppendTo[\[Pi], {Xm[[i]], X[[ii]]}];
    If[polyresult,
     h = (h /. Thread[Xm[[i]] -> X[[ii + 1]]]) - (h /.
         Thread[{Xm[[i]]} -> {X[[ii]]}])];
    ii = ii - 2];
   i = i - 1];
  lt = \[Alpha] /. Thread[First /@ \[Pi] -> Last /@ \[Pi]];
  If[polyresult, {\[Pi], lt, h}, {\[Pi], lt}]]

(*Function that ouputs a list of terms of a polynomial that can be \
used in the algorithm*)
ViableSymmetries[f_] :=
 Module[{monos, terms, vars, n, m, i, ii, iii, AV, \[FormalX], totdeg,
   pos},
  monos = MonomialList[f];
  n = Length[monos];
  terms = {};
  For[i = 1, i <= n, i++,
   vars = Variables[monos[[i]]];
   m = Length[vars];
   totdeg =
    Exponent[# /. ((# -> \[FormalX] RandomReal[]) & /@ {#}), \
\[FormalX]] &[monos[[i]]];
   pos = True;
```

```
    For[ii = 1, ii <= n, ii++,
     AV = True;
     If[ii != i,
      If[Exponent[# /. ((# -> \[FormalX] RandomReal[]) & /@ {#}), \
\[FormalX]] &[monos[[ii]]] >= totdeg,
       For[iii = 1, iii <= m, iii++,
        If[
         Exponent[# /. ((# -> \[FormalX] RandomReal[]) & /@ \
{vars[[iii]]}), \[FormalX]] &[monos[[ii]]] == 0, AV = False]],
       AV = False], AV = False];
     If[AV, pos = False;
      Break]];
    If[pos, AppendTo[terms, monos[[i]]]]];
  terms]
```

B Mathematica Symmetry Experiments

Function definitions:

In[1]:=
```
Remove["Global`*"]
```

In[2]:=
```
groupElementAction[expr_, vars_, perm_] /;
  Length[perm] == Length[vars] && PermutationListQ[perm] :=
 expr /. Thread[vars → Permute[vars, perm]]
```

In[3]:=
```
Symmetries[F_, vars_] := Module[{polynomials, perms, i, j},
  polynomials = {};
  perms = Permutations[Range[Length[vars]]];
  For[i = 1, i ≤ Length[F], i++,
   For[j = 1, j ≤ Length[perms], j++,
    AppendTo[polynomials, groupElementAction[F[[i]], vars, perms[[j]]]]]];
  DeleteDuplicates[polynomials]]
```

In[4]:=
```
IndividualSymmetries[F_, vars_, amount_, order_: "middle"] :=
 Module[{NewF, newvars, varcount, addvars, i, ii},
  NewF = F;
  varcount = Length[vars];
  If[order == "end",
   newvars = vars;
   For[i = 1, i ≤ varcount, i++,
    addvars = {};
    For[ii = 1, ii ≤ amount, ii++,
     AppendTo[addvars, vars[[i]][[ii]]];
    newvars = Join[newvars, addvars];
    NewF = Join[NewF, Symmetries[NewF, Join[{vars[[i]]}, addvars]]]]];
  If[order == "middle",
   newvars = {};
   For[i = 1, i ≤ varcount, i++,
    addvars = {vars[[i]]};
    For[ii = 1, ii ≤ amount, ii++,
     AppendTo[addvars, vars[[i]][[ii]]];
    newvars = Join[newvars, addvars];
    NewF = Join[NewF, Symmetries[NewF, addvars]]]];
  NewF = DeleteDuplicates[NewF];
  {NewF, newvars}
 ]
```

Symmetry in all variables:

quasi-polynomial 2n-1/2n-2/n+1 in GB

Comparison degree input vs degree GB

In[5]:=
```
lst = {};
For[i = 1, i ≤ 50, i++,
 AppendTo[lst, {i, Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[
    GroebnerBasis[Symmetries[{x^(i - 1) y - z^i}, {x, y, z}],
      {x, y, z}, MonomialOrder → DegreeReverseLexicographic][[-1]]]}]]
lst
```

Out[7]=
```
{{1, 1}, {2, 2}, {3, 5}, {4, 6}, {5, 6}, {6, 11}, {7, 12}, {8, 9}, {9, 17}, {10, 18},
 {11, 12}, {12, 23}, {13, 24}, {14, 15}, {15, 29}, {16, 30}, {17, 18}, {18, 35},
 {19, 36}, {20, 21}, {21, 41}, {22, 42}, {23, 24}, {24, 47}, {25, 48}, {26, 27},
 {27, 53}, {28, 54}, {29, 30}, {30, 59}, {31, 60}, {32, 33}, {33, 65}, {34, 66},
 {35, 36}, {36, 71}, {37, 72}, {38, 39}, {39, 77}, {40, 78}, {41, 42}, {42, 83},
 {43, 84}, {44, 45}, {45, 89}, {46, 90}, {47, 48}, {48, 95}, {49, 96}, {50, 51}}
```

Comparison GBs of n = 3, 4, 5

In[8]:=
```
n = 6
GroebnerBasis[Symmetries[{x^(n - 1) * y - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;
GroebnerBasis[Symmetries[{x^(n - 1) y - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;
GroebnerBasis[Symmetries[{x^(n - 1) y - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
```

Out[8]= 6

Out[9]=
$$\{y^5 z - y z^5,\ x^5 z - x z^5,\ y^6 - x z^5,\ x y^5 - z^6,\ x^5 y - z^6,\ x^6 - y z^5,\ y^2 z^5 - x z^6,\ x y z^5 - z^7,\ x^2 z^5 - y z^6,\ x z^9 - y z^9,\ y z^{10} - z^{11}\}$$

Out[11]=
$$\{y^6 z - y z^6,\ x^6 z - x z^6,\ y^7 - x z^6,\ x y^6 - z^7,\ x^6 y - z^7,\ x^7 - y z^6,\ y^2 z^6 - x z^7,\ x y z^6 - z^8,\ x^2 z^6 - y z^7,\ y z^{11} - z^{12},\ x z^{11} - z^{12}\}$$

Out[13]=
$$\{y^7 z - y z^7,\ x^7 z - x z^7,\ y^8 - x z^7,\ x y^7 - z^8,\ x^7 y - z^8,\ x^8 - y z^7,\ y^2 z^7 - x z^8,\ x y z^7 - z^9,\ x^2 z^7 - y z^8\}$$

Adding a constant in front of one of the terms:

In[14]:=
```
c = 2;
lst = {};
For[i = 1, i ≤ 50, i++,
 AppendTo[lst, {i, Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[
    GroebnerBasis[Symmetries[{(c * I) * x^(i - 1) y - z^i}, {x, y, z}],
      {x, y, z}, MonomialOrder → DegreeReverseLexicographic][[-1]]]}]]
lst
```

Out[17]=
```
{{1, 1}, {2, 4}, {3, 5}, {4, 6}, {5, 7}, {6, 8}, {7, 9}, {8, 10}, {9, 11}, {10, 12},
 {11, 13}, {12, 14}, {13, 15}, {14, 16}, {15, 17}, {16, 18}, {17, 19}, {18, 20},
 {19, 21}, {20, 22}, {21, 23}, {22, 24}, {23, 25}, {24, 26}, {25, 27}, {26, 28},
 {27, 29}, {28, 30}, {29, 31}, {30, 32}, {31, 33}, {32, 34}, {33, 35}, {34, 36},
 {35, 37}, {36, 38}, {37, 39}, {38, 40}, {39, 41}, {40, 42}, {41, 43}, {42, 44},
 {43, 45}, {44, 46}, {45, 47}, {46, 48}, {47, 49}, {48, 50}, {49, 51}, {50, 52}}
```

In[18]:=
```
n = 3
GroebnerBasis[Symmetries[{2 x^(n - 1) y - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;
GroebnerBasis[Symmetries[{2 x^(n - 1) y - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;
GroebnerBasis[Symmetries[{2 x^(n - 1) y - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
```

Out[18]= 3

Out[19]= $\{y^2 z - y z^2, x^2 z - x z^2, y^3 - 2 x z^2, 2 x y^2 - z^3, 2 x^2 y - z^3, x^3 - 2 y z^2, y z^3, x z^3, 2 x y z^2 - z^4, z^5\}$

Out[21]= $\{y^3 z - y z^3, x^3 z - x z^3, y^4 - 2 x z^3, 2 x y^3 - z^4,$
$2 x^3 y - z^4, x^4 - 2 y z^3, y z^4, x z^4, y^2 z^3, 2 x y z^3 - z^5, x^2 z^3, z^6\}$

Out[23]= $\{y^4 z - y z^4, x^4 z - x z^4, y^5 - 2 x z^4, 2 x y^4 - z^5,$
$2 x^4 y - z^5, x^5 - 2 y z^4, y z^5, x z^5, y^2 z^4, 2 x y z^4 - z^6, x^2 z^4, z^7\}$

Consistent 2n-2 in GB:

In[24]:=
```
lst = {};
For[i = 1, i ≤ 40, i++,
 AppendTo[lst, {i, Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[
    GroebnerBasis[Symmetries[{x^(i - 1) y - z^i + z^(i - 1) y }, {x, y, z}],
      {x, y, z}, MonomialOrder → DegreeReverseLexicographic][[-1]]]}]]
lst
```

Out[26]= {{1, 1}, {2, 3}, {3, 5}, {4, 6}, {5, 8}, {6, 10}, {7, 12}, {8, 14},
{9, 16}, {10, 18}, {11, 20}, {12, 22}, {13, 24}, {14, 26}, {15, 28}, {16, 30},
{17, 32}, {18, 34}, {19, 36}, {20, 38}, {21, 40}, {22, 42}, {23, 44}, {24, 46},
{25, 48}, {26, 50}, {27, 52}, {28, 54}, {29, 56}, {30, 58}, {31, 60}, {32, 62},
{33, 64}, {34, 66}, {35, 68}, {36, 70}, {37, 72}, {38, 74}, {39, 76}, {40, 78}}

In[27]:=
```
n = 4;
GroebnerBasis[Symmetries[{x^(n - 1) y - z^n + z^(n - 1) y}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;
GroebnerBasis[Symmetries[{x^(n - 1) y - z^n + z^(n - 1) y}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;
GroebnerBasis[Symmetries[{x^(n - 1) y - z^n + z^(n - 1) y}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
```

Out[28]= $\{x^3 z + y^3 z - z^4, y^4 - z^4, x y^3 + x z^3 - z^4, x^3 y + y z^3 - z^4, x^4 - z^4, y z^4 - z^5, x z^4 - z^5, x y z^3, z^6, y^3 z^3\}$

Out[30]= $\{x^4 z + y^4 z - z^5, y^5 - z^5, x y^4 + x z^4 - z^5, x^4 y + y z^4 - z^5, x^5 - z^5, y z^5 - z^6, x z^5 - z^6, x y z^4, z^7, y^4 z^4\}$

Out[32]= $\{x^5 z + y^5 z - z^6, y^6 - z^6, x y^5 + x z^5 - z^6, x^5 y + y z^5 - z^6, x^6 - z^6, y z^6 - z^7, x z^6 - z^7, x y z^5, z^8, y^5 z^5\}$

Consistent 3n - 2 in GB:

In[33]:=
```
lst = {};
For[i = 1, i ≤ 20, i++,
 AppendTo[lst, {i, Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[
    GroebnerBasis[Symmetries[{x^(i - 1) y - z^i + y^(i - 1) x}, {x, y, z}],
      {x, y, z}, MonomialOrder → DegreeReverseLexicographic][[-1]]]}]]
lst
```

Out[35]=
```
{{1, 1}, {2, 4}, {3, 5}, {4, 10}, {5, 13}, {6, 16},
 {7, 19}, {8, 16}, {9, 25}, {10, 28}, {11, 31}, {12, 34}, {13, 37},
 {14, 40}, {15, 43}, {16, 46}, {17, 49}, {18, 52}, {19, 55}, {20, 58}}
```

In[36]:=
```
n = 4;
GroebnerBasis[Symmetries[{x^(n - 1) y + x y^(n - 1) - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;
GroebnerBasis[Symmetries[{x^(n - 1) y + x y^(n - 1) - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;
GroebnerBasis[Symmetries[{x^(n - 1) y + x y^(n - 1) - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
```

Out[37]=
$$\{y^4 - x^3 z - x z^3,\ x^3 y + x y^3 - z^4,\ x^4 - y^3 z - y z^3,$$
$$x^2 y^3 + x^3 z^2 + y^2 z^3,\ x^2 y z^3 - x y^2 z^3 - 2 y^3 z^3 - x y z^4 + x z^5 - y z^5 - z^6,$$
$$x^3 z^3 + y^3 z^3 + x y z^4 + z^6,\ 10 y^3 z^4 + x^2 z^5 + 5 x y z^5 - y^2 z^5 - 3 x z^6 + 3 y z^6 + 5 z^7,$$
$$10 x y^2 z^4 - x^2 z^5 - 5 x y z^5 + y^2 z^5 + 8 x z^6 + 12 y z^6,\ 10 x y^3 z^3 - 2 x^2 z^5 + 2 y^2 z^5 + x z^6 - y z^6 - 5 z^7,$$
$$3 y^2 z^6 + x z^7 + 2 y z^7,\ x y z^6 + z^8,\ 3 x^2 z^6 + 2 x z^7 + y z^7,\ 2 y z^8 + z^9,\ 2 x z^8 + z^9,\ z^{10}\}$$

Out[39]=
$$\{y^5 - x^4 z - x z^4,\ x^4 y + x y^4 - z^5,\ x^5 - y^4 z - y z^4,\ x^2 y^4 + x^4 z^2 + y^2 z^4,$$
$$x^3 z^4 + y^3 z^4 + x y z^5 + z^7,\ 2 x y^4 z^3 - z^8,\ 2 y^4 z^5 + 2 x^2 z^7 + y z^8,\ 2 x y^3 z^5 + 2 x^2 y z^6 - 2 y^2 z^7 + x z^8,$$
$$x^2 y^2 z^5 + x y z^7 + z^9,\ x^2 y^3 z^4 - x y^2 z^6 + x^2 z^7,\ 2 y^3 z^7 + x y z^8 + z^{10},\ 2 x y^2 z^7 - x^2 z^8 + y z^9,$$
$$2 x^2 y z^7 - y^2 z^8 + x z^9,\ 3 y^2 z^9 + x z^{10},\ x y z^9 + 3 z^{11},\ 3 x^2 z^9 + y z^{10},\ y z^{11},\ x z^{11},\ z^{13}\}$$

Out[41]=
$$\{y^6 - x^5 z - x z^5,\ x^5 y + x y^5 - z^6,\ x^6 - y^5 z - y z^5,\ x^2 y^5 + x^5 z^2 + y^2 z^5,$$
$$x^3 z^5 + y^3 z^5 + x y z^6 + z^8,\ x y^3 z^6 + y^4 z^6 - x^2 y z^7 + 2 x y^2 z^7 - 2 x^2 z^8 + 2 y^2 z^8 + y z^9,$$
$$4 y^5 z^6 - 6 x^2 y^2 z^7 - 8 y^4 z^7 - 16 x y^2 z^8 + 2 y^3 z^8 + 13 x^2 z^9 - 5 x y z^9 - 9 y^2 z^9 - x z^{10} - 7 y z^{10} - 3 z^{11},$$
$$4 x^2 y^4 z^5 - 4 x y^5 z^5 - 6 x^2 y^2 z^7 - 4 y^4 z^7 - 8 x y^2 z^8 + 2 y^3 z^8 + 5 x^2 z^9 - 5 x y z^9 - 5 y^2 z^9 - x z^{10} -$$
$$3 y z^{10} + z^{11},\ 10 y^4 z^8 - 3 x^2 y z^9 + 17 x y^2 z^9 - 11 x^2 z^{10} + 3 x y z^{10} + 9 y^2 z^{10} - x z^{11} + 9 y z^{11} + 4 z^{12},$$
$$30 x^2 y^2 z^8 + 18 x^2 y z^9 + 18 x y^2 z^9 + x^2 z^{10} + 17 x y z^{10} + y^2 z^{10} + 11 x z^{11} + 11 y z^{11} + z^{12},$$
$$34 y^3 z^{10} + 29 x^2 z^{11} + 17 x y z^{11} - 29 y^2 z^{11} - x z^{12} + y z^{12} + 17 z^{13},$$
$$204 x y^2 z^{10} - 74 x^2 z^{11} - 102 x y z^{11} + 142 y^2 z^{11} + 77 x z^{12} + 161 y z^{12} - 221 z^{13},$$
$$204 x^2 y z^{10} + 142 x^2 z^{11} - 102 x y z^{11} - 74 y^2 z^{11} + 161 x z^{12} + 77 y z^{12} - 221 z^{13},$$
$$9 y^2 z^{12} - 2 x z^{13} - 7 y z^{13} - 9 z^{14},\ x y z^{12} + 3 z^{14},$$
$$9 x^2 z^{12} - 7 x z^{13} - 2 y z^{13} - 9 z^{14},\ 2 y z^{14} - z^{15},\ 2 x z^{14} - z^{15},\ z^{16}\}$$

Consistent 4n - 3 in GB:

In[42]:=
```
lst = {};
For[i = 1, i ≤ 10, i++,
 AppendTo[lst,
  {i, Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[GroebnerBasis[Symmetries[
       {x^(i - 1) y + x y^(i - 1) + w^(i - 1) x + w^(i - 1) y + x^(i - 1) w + y^(i - 1) w - z^i},
       {x, y, z, w}], {x, y, z, w}, MonomialOrder → DegreeReverseLexicographic][[-1]]]}]]
lst
```

Out[44]= {{1, 1}, {2, 5}, {3, 9}, {4, 11}, {5, 17}, {6, 21}, {7, 25}, {8, 29}, {9, 33}, {10, 37}}

In[45]:=
```
n = 6;
GroebnerBasis[Symmetries[
  {x^(n - 1) y + x y^(n - 1) + w^(n - 1) x + w^(n - 1) y + x^(n - 1) w + y^(n - 1) w - z^n},
  {x, y, z, w}], {x, y, z, w}, MonomialOrder → DegreeReverseLexicographic]
```

Out[46]=
$$\{-w^6 - w^5 x - w x^5 - w^5 y - w y^5 + x^5 z + y^5 z + x z^5 + y z^5 + z^6,$$
$$-w^6 - 2 w^5 x - 2 w x^5 - w^5 y - w y^5 + y^6 - w^5 z + y^5 z - w z^5 + y z^5 + z^6,$$
$$w^5 x + w x^5 + w^5 y + x^5 y + w y^5 + x y^5 - z^6, x^6 - w^5 y - w y^5 - w^5 z - y^5 z - w z^5 - y z^5,$$
$$-w^6 x - w^5 x^2 - w^6 y - 2 w^5 x y - w^5 y^2 - w^6 z + w^5 x z + w^5 y z + 2 w^5 z^2 -$$
$$2 w^2 z^5 - w x z^5 + x^2 z^5 - w y z^5 + 2 x y z^5 + y^2 z^5 + w z^6 + x z^6 + y z^6,$$
$$w^5 x y + w^5 y^2 - w^2 y^5 - w x y^5 - w^5 x z + x y^5 z - w^5 z^2 + y^5 z^2 + w^2 z^5 + w x z^5 - x y z^5 - y^2 z^5,$$
$$\cdots 113 \cdots, -6\,744\,336\,186\,632\,624\,097\,395\,573\,572\,638\,515\,386\,645\, w^{19} +$$
$$2\,266\,128\,241\,661\,263\,020\,163\,907\,018\,092\,029\,066\,959\, w^{18} x +$$
$$19\,643\,548\,099\,806\,772\,871\,541\,144\,097\,567\,947\,192\,777\, w^{17} x^2 -$$
$$3\,201\,495\,169\,385\,208\,383\,496\,443\,032\,824\,392\,738\,290\, w^{18} y -$$
$$3\,201\,495\,169\,385\,208\,383\,496\,443\,032\,824\,392\,738\,290\, w^{18} z,$$
$$-5\,923\,876\,332\,748\, w^{20} + 63\,962\,726\,320\,257\, w^{19} z, -5\,923\,876\,332\,748\, w^{20} + 63\,962\,726\,320\,257\, w^{19} y,$$
$$-5\,923\,876\,332\,748\, w^{20} + 63\,962\,726\,320\,257\, w^{19} x, w^{21}\}$$

large output | show less | show more | show all | set size limit...

1 and 2 individual symmetries f2 compared to normal symmetries f2

Comparison of the GBs

In[47]:=
```
n = 3;
Syms = IndividualSymmetries[{x y^(n - 1) - z^n}, {x, y, z}, 1];
 JSyms = Syms[[1]];
PSyms = Syms[[2]];
GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic]
Syms = IndividualSymmetries[{x y^(n - 1) - z^n}, {x, y, z}, 2];
 JSyms = Syms[[1]];
PSyms = Syms[[2]];
GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic]
GroebnerBasis[Symmetries[{x y^(n - 1) - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]

n = n + 1;
Syms = IndividualSymmetries[{x y^(n - 1) - z^n}, {x, y, z}, 1];
 JSyms = Syms[[1]];
PSyms = Syms[[2]];
GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic]
Syms = IndividualSymmetries[{x y^(n - 1) - z^n}, {x, y, z}, 2];
 JSyms = Syms[[1]];
PSyms = Syms[[2]];
GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic]
GroebnerBasis[Symmetries[{x y^(n - 1) - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
n = n + 1;

Syms = IndividualSymmetries[{x y^(n - 1) - z^n}, {x, y, z}, 1];
 JSyms = Syms[[1]];
PSyms = Syms[[2]];
GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic]
Syms = IndividualSymmetries[{x y^(n - 1) - z^n}, {x, y, z}, 2];
 JSyms = Syms[[1]];
PSyms = Syms[[2]];
GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic]
GroebnerBasis[Symmetries[{x y^(n - 1) - z^n}, {x, y, z}],
 {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
```

Out[51]=
$$\{z^3 - z[1]^3,\ x[1]\,y[1]^2 - z[1]^3,\ x\,y[1]^2 - z[1]^3,\ y^2\,x[1] - z[1]^3,\ x\,y^2 - z[1]^3,\ x\,z[1]^3 - x[1]\,z[1]^3,\ y^2\,z[1]^3 - y[1]^2\,z[1]^3\}$$

Out[55]=
$$\{z[1]^3 - z[2]^3,\ z^3 - z[2]^3,\ x[2]\,y[2]^2 - z[2]^3,\ x[1]\,y[2]^2 - z[2]^3,\ x\,y[2]^2 - z[2]^3,\ x[2]\,y[1]^2 - z[2]^3,\ x[1]\,y[1]^2 - z[2]^3,\ x\,y[1]^2 - z[2]^3,\ y^2\,x[2] - z[2]^3,\ y^2\,x[1] - z[2]^3,\ x\,y^2 - z[2]^3,\ x[1]\,z[2]^3 - x[2]\,z[2]^3,\ x\,z[2]^3 - x[2]\,z[2]^3,\ y[1]^2\,z[2]^3 - y[2]^2\,z[2]^3,\ y^2\,z[2]^3 - y[2]^2\,z[2]^3\}$$

Out[56]=
$$\{y^2\,z - y\,z^2,\ x^2\,z - x\,z^2,\ y^3 - x\,z^2,\ x\,y^2 - z^3,\ x^2\,y - z^3,\ x^3 - y\,z^2,\ x\,z^3 - y\,z^3,\ x\,y\,z^2 - z^4,\ y\,z^4 - z^5\}$$

Out[61]=
$$\{z^4 - z[1]^4,\ x[1]\,y[1]^3 - z[1]^4,\ x\,y[1]^3 - z[1]^4,\ y^3\,x[1] - z[1]^4,\ x\,y^3 - z[1]^4,\ x\,z[1]^4 - x[1]\,z[1]^4,\ y^3\,z[1]^4 - y[1]^3\,z[1]^4\}$$

Out[65]= $\{z[1]^4 - z[2]^4,\ z^4 - z[2]^4,\ x[2]\,y[2]^3 - z[2]^4,\ x[1]\,y[2]^3 - z[2]^4,$
$x\,y[2]^3 - z[2]^4,\ x[2]\,y[1]^3 - z[2]^4,\ x[1]\,y[1]^3 - z[2]^4,\ x\,y[1]^3 - z[2]^4,$
$y^3\,x[2] - z[2]^4,\ y^3\,x[1] - z[2]^4,\ x\,y^3 - z[2]^4,\ x[1]\,z[2]^4 - x[2]\,z[2]^4,$
$x\,z[2]^4 - x[2]\,z[2]^4,\ y[1]^3\,z[2]^4 - y[2]^3\,z[2]^4,\ y^3\,z[2]^4 - y[2]^3\,z[2]^4\}$

Out[66]= $\{y^3\,z - y\,z^3,\ x^3\,z - x\,z^3,\ y^4 - x\,z^3,\ x\,y^3 - z^4,\ x^3\,y - z^4,$
$x^4 - y\,z^3,\ y^2\,z^3 - x\,z^4,\ x\,y\,z^3 - z^5,\ x^2\,z^3 - y\,z^4,\ y\,z^5 - z^6,\ x\,z^5 - z^6\}$

Out[71]= $\{z^5 - z[1]^5,\ x[1]\,y[1]^4 - z[1]^5,\ x\,y[1]^4 - z[1]^5,$
$y^4\,x[1] - z[1]^5,\ x\,y^4 - z[1]^5,\ x\,z[1]^5 - x[1]\,z[1]^5,\ y^4\,z[1]^5 - y[1]^4\,z[1]^5\}$

Out[75]= $\{z[1]^5 - z[2]^5,\ z^5 - z[2]^5,\ x[2]\,y[2]^4 - z[2]^5,\ x[1]\,y[2]^4 - z[2]^5,$
$x\,y[2]^4 - z[2]^5,\ x[2]\,y[1]^4 - z[2]^5,\ x[1]\,y[1]^4 - z[2]^5,\ x\,y[1]^4 - z[2]^5,$
$y^4\,x[2] - z[2]^5,\ y^4\,x[1] - z[2]^5,\ x\,y^4 - z[2]^5,\ x[1]\,z[2]^5 - x[2]\,z[2]^5,$
$x\,z[2]^5 - x[2]\,z[2]^5,\ y[1]^4\,z[2]^5 - y[2]^4\,z[2]^5,\ y^4\,z[2]^5 - y[2]^4\,z[2]^5\}$

Out[76]= $\{y^4\,z - y\,z^4,\ x^4\,z - x\,z^4,\ y^5 - x\,z^4,\ x\,y^4 - z^5,\ x^4\,y - z^5,\ x^5 - y\,z^4,\ y^2\,z^4 - x\,z^5,\ x\,y\,z^4 - z^6,\ x^2\,z^4 - y\,z^5\}$

Comparison degree of the GBs (input vs GB 1 individual symmetry vs GB standard symmetries)

In[77]:=
```
lst = {};
For[i = 1, i ≤ 20, i++,
 Syms = IndividualSymmetries[{x y^(i - 1) - z^i}, {x, y, z}, 1];
 JSyms = Syms[[1]];
 PSyms = Syms[[2]];
 AppendTo[lst, {i, Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[
    GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic][[-1]]],
   Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[
    GroebnerBasis[Symmetries[{x y^(i - 1) - z^i}, {x, y, z}],
      {x, y, z}, MonomialOrder → DegreeReverseLexicographic][[-1]]]}]]
lst
```

Out[79]= {{1, 1, 1}, {2, 3, 2}, {3, 5, 5}, {4, 7, 6}, {5, 9, 6}, {6, 11, 11}, {7, 13, 12}, {8, 15, 9},
{9, 17, 17}, {10, 19, 18}, {11, 21, 12}, {12, 23, 23}, {13, 25, 24}, {14, 27, 15},
{15, 29, 29}, {16, 31, 30}, {17, 33, 18}, {18, 35, 35}, {19, 37, 36}, {20, 39, 21}}

1 and 2 Individual symmetries (f1,f2,f3) compared to normal (f1,f2,f3)

Comparison of the GBs

In[80]:=
```
Syms = IndividualSymmetries[
    {x y^(n-1) - z^n, x^(n+1) - y * z^(n-1) * w, x^n z - y^n w}, {x, y, z, w}, 1];
JSyms = Syms[[1]];
PSyms = Syms[[2]];
GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic]
Syms = IndividualSymmetries[
    {x y^(n-1) - z^n, x^(n+1) - y * z^(n-1) * w, x^n z - y^n w}, {x, y, z, w}, 2];
JSyms = Syms[[1]];
PSyms = Syms[[2]];
GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic]
GroebnerBasis[{x y^(n-1) - z^n, x^(n+1) - y * z^(n-1) * w, x^n z - y^n w},
 {x, y, z, w}, MonomialOrder → DegreeReverseLexicographic]
```

Out[83]=
$$\{z^5 - z[1]^5,\ x[1]\,y[1]^4 - z[1]^5,\ x\,y[1]^4 - z[1]^5,\ y^4\,x[1] - z[1]^5,$$
$$x\,y^4 - z[1]^5,\ y\,w[1]\,z[1]^4 - w[1]\times y[1]\,z[1]^4,\ z^4\,w[1]\times y[1] - w[1]\times y[1]\,z[1]^4,$$
$$y\,z^4\,w[1] - w[1]\times y[1]\,z[1]^4,\ y^5\,w[1] - w[1]\,y[1]^5,\ w\,y[1]\,z[1]^4 - w[1]\times y[1]\,z[1]^4,$$
$$w\,y\,z[1]^4 - w[1]\times y[1]\,z[1]^4,\ w\,z^4\,y[1] - w[1]\times y[1]\,z[1]^4,\ w\,y\,z^4 - w[1]\times y[1]\,z[1]^4,$$
$$w\,y[1]^5 - w[1]\,y[1]^5,\ w\,y^5 - w[1]\,y[1]^5,\ x\,z[1]^5 - x[1]\,z[1]^5,\ -w[1]\,y[1]^5 + x[1]^5\,z[1],$$
$$-w[1]\,y[1]^5 + x^5\,z[1],\ z\,x[1]^5 - w[1]\,y[1]^5,\ x^5\,z - w[1]\,y[1]^5,\ x[1]^6 - w[1]\times y[1]\,z[1]^4,$$
$$x^6 - w[1]\times y[1]\,z[1]^4,\ z\,w[1]\times y[1]\,z[1]^4 - w[1]\times y[1]\,z[1]^5,\ z\,w[1]\,y[1]^5 - w[1]\,y[1]^5\,z[1],$$
$$y^4\,z[1]^5 - y[1]^4\,z[1]^5,\ z^4\,w[1]\,z[1]^5 - w[1]\,z[1]^9,\ y^4\,w[1]\,y[1]^5 - w[1]\,y[1]^9,$$
$$w\,z[1]^9 - w[1]\,z[1]^9,\ w\,z^4\,z[1]^5 - w[1]\,z[1]^9,\ -w[1]\,y[1]^9 + x[1]^4\,z[1]^6,$$
$$-w[1]\,y[1]^9 + z\,x[1]^4\,z[1]^5,\ y\,w[1]^2\,y[1]^5\,z[1]^3 - w[1]^2\,y[1]^6\,z[1]^3,\ z\,w[1]\,z[1]^9 - w[1]\,z[1]^{10},$$
$$y\,w[1]\,y[1]^9 - w[1]\,y[1]^{10},\ -w[1]\,y[1]^{13} + x[1]^3\,z[1]^{11},\ -w[1]\,y[1]^{13} + z\,x[1]^3\,z[1]^{10},$$
$$-w[1]\,y[1]^{17} + x[1]^2\,z[1]^{16},\ -w[1]\,y[1]^{17} + z\,x[1]^2\,z[1]^{15},\ -w[1]\,y[1]^{21} + x[1]\,z[1]^{21},$$
$$-w[1]\,y[1]^{21} + z\,x[1]\,z[1]^{20},\ -w[1]\,y[1]^{25} + z[1]^{26},\ -w[1]\,y[1]^{25} + z\,z[1]^{25}\}$$

Out[87]=
$$\{z[1]^5 - z[2]^5,\ z^5 - z[2]^5,\ x[2]\,y[2]^4 - z[2]^5,\ x[1]\,y[2]^4 - z[2]^5,\ x\,y[2]^4 - z[2]^5,$$
$$x[2]\,y[1]^4 - z[2]^5,\ x[1]\,y[1]^4 - z[2]^5,\ x\,y[1]^4 - z[2]^5,\ y^4\,x[2] - z[2]^5,\ y^4\,x[1] - z[2]^5,$$
$$x\,y^4 - z[2]^5,\ w[2]\times y[1]\,z[2]^4 - w[2]\times y[2]\,z[2]^4,\ y\,w[2]\,z[2]^4 - w[2]\times y[2]\,z[2]^4,$$
$$w[2]\times y[2]\,z[1]^4 - w[2]\times y[2]\,z[2]^4,\ w[2]\times y[1]\,z[1]^4 - w[2]\times y[2]\,z[2]^4,$$
$$y\,w[2]\,z[1]^4 - w[2]\times y[2]\,z[2]^4,\ z^4\,w[2]\times y[2] - w[2]\times y[2]\,z[2]^4,$$
$$z^4\,w[2]\times y[1] - w[2]\times y[2]\,z[2]^4,\ y\,z^4\,w[2] - w[2]\times y[2]\,z[2]^4,$$
$$w[2]\,y[1]^5 - w[2]\,y[2]^5,\ y^5\,w[2] - w[2]\,y[2]^5,\ w[1]\times y[2]\,z[2]^4 - w[2]\times y[2]\,z[2]^4,$$
$$w[1]\times y[1]\,z[2]^4 - w[2]\times y[2]\,z[2]^4,\ y\,w[1]\,z[2]^4 - w[2]\times y[2]\,z[2]^4,$$
$$w[1]\times y[2]\,z[1]^4 - w[2]\times y[2]\,z[2]^4,\ w[1]\times y[1]\,z[1]^4 - w[2]\times y[2]\,z[2]^4,$$
$$y\,w[1]\,z[1]^4 - w[2]\times y[2]\,z[2]^4,\ z^4\,w[1]\times y[2] - w[2]\times y[2]\,z[2]^4,$$
$$z^4\,w[1]\times y[1] - w[2]\times y[2]\,z[2]^4,\ y\,z^4\,w[1] - w[2]\times y[2]\,z[2]^4,\ w[1]\,y[2]^5 - w[2]\,y[2]^5,$$
$$w[1]\,y[1]^5 - w[2]\,y[2]^5,\ y^5\,w[1] - w[2]\,y[2]^5,\ w\,y[2]\,z[2]^4 - w[2]\times y[2]\,z[2]^4,$$
$$w\,y[1]\,z[2]^4 - w[2]\times y[2]\,z[2]^4,\ w\,y\,z[2]^4 - w[2]\times y[2]\,z[2]^4,\ w\,y[2]\,z[1]^4 - w[2]\times y[2]\,z[2]^4,$$
$$w\,y[1]\,z[1]^4 - w[2]\times y[2]\,z[2]^4,\ w\,y\,z[1]^4 - w[2]\times y[2]\,z[2]^4,\ w\,z^4\,y[2] - w[2]\times y[2]\,z[2]^4,$$
$$w\,z^4\,y[1] - w[2]\times y[2]\,z[2]^4,\ w\,y\,z^4 - w[2]\times y[2]\,z[2]^4,\ w\,y[2]^5 - w[2]\,y[2]^5,$$
$$w\,y[1]^5 - w[2]\,y[2]^5,\ w\,y^5 - w[2]\,y[2]^5,\ x[1]\,z[2]^5 - x[2]\,z[2]^5,\ x\,z[2]^5 - x[2]\,z[2]^5,$$
$$-w[2]\,y[2]^5 + x[2]^5\,z[2],\ -w[2]\,y[2]^5 + x[1]^5\,z[2],\ -w[2]\,y[2]^5 + x^5\,z[2],$$
$$-w[2]\,y[2]^5 + x[2]^5\,z[1],\ -w[2]\,y[2]^5 + x[1]^5\,z[1],\ -w[2]\,y[2]^5 + x^5\,z[1],$$
$$z\,x[2]^5 - w[2]\,y[2]^5,\ z\,x[1]^5 - w[2]\,y[2]^5,\ x^5\,z - w[2]\,y[2]^5,\ x[2]^6 - w[2]\times y[2]\,z[2]^4,$$
$$x[1]^6 - w[2]\times y[2]\,z[2]^4,\ x^6 - w[2]\times y[2]\,z[2]^4,\ w[2]\times y[2]\times z[1]\,z[2]^4 - w[2]\times y[2]\,z[2]^5,$$
$$z\,w[2]\times y[2]\,z[2]^4 - w[2]\times y[2]\,z[2]^5,\ w[2]\,y[2]^5\,z[1] - w[2]\,y[2]^5\,z[2],$$
$$z\,w[2]\,y[2]^5 - w[2]\,y[2]^5\,z[2],\ y[1]^4\,z[2]^5 - y[2]^4\,z[2]^5,\ y^4\,z[2]^5 - y[2]^4\,z[2]^5,$$
$$w[2]\,z[1]^4\,z[2]^5 - w[2]\,z[2]^9,\ z^4\,w[2]\,z[2]^5 - w[2]\,z[2]^9,\ w[2]\,y[1]^4\,y[2]^5 - w[2]\,y[2]^9,$$
$$y^4\,w[2]\,y[2]^5 - w[2]\,y[2]^9,\ w[1]\,z[2]^9 - w[2]\,z[2]^9,\ w[1]\,z[1]^4\,z[2]^5 - w[2]\,z[2]^9,$$
$$z^4\,w[1]\,z[2]^5 - w[2]\,z[2]^9,\ w\,z[2]^9 - w[2]\,z[2]^9,\ w\,z[1]^4\,z[2]^5 - w[2]\,z[2]^9,$$
$$w\,z^4\,z[2]^5 - w[2]\,z[2]^9,\ -w[2]\,y[2]^9 + x[2]^4\,z[2]^6,\ -w[2]\,y[2]^9 + x[2]^4\,z[1]\,z[2]^5,$$
$$-w[2]\,y[2]^9 + z\,x[2]^4\,z[2]^5,\ w[2]^2\,y[1]\,y[2]^5\,z[2]^3 - w[2]^2\,y[2]^6\,z[2]^3,$$
$$y\,w[2]^2\,y[2]^5\,z[2]^3 - w[2]^2\,y[2]^6\,z[2]^3,\ w[2]\times z[1]\,z[2]^9 - w[2]\,z[2]^{10},$$
$$z\,w[2]\,z[2]^9 - w[2]\,z[2]^{10},\ w[2]\times y[1]\,y[2]^9 - w[2]\,y[2]^{10},\ y\,w[2]\,y[2]^9 - w[2]\,y[2]^{10},$$
$$-w[2]\,y[2]^{13} + x[2]^3\,z[2]^{11},\ -w[2]\,y[2]^{13} + x[2]^3\,z[1]\,z[2]^{10},\ -w[2]\,y[2]^{13} + z\,x[2]^3\,z[2]^{10},$$
$$-w[2]\,y[2]^{17} + x[2]^2\,z[2]^{16},\ -w[2]\,y[2]^{17} + x[2]^2\,z[1]\,z[2]^{15},\ -w[2]\,y[2]^{17} + z\,x[2]^2\,z[2]^{15},$$
$$-w[2]\,y[2]^{21} + x[2]\,z[2]^{21},\ -w[2]\,y[2]^{21} + x[2]\times z[1]\,z[2]^{20},\ -w[2]\,y[2]^{21} + z\,x[2]\,z[2]^{20},$$
$$-w[2]\,y[2]^{25} + z[2]^{26},\ -w[2]\,y[2]^{25} + z[1]\,z[2]^{25},\ -w[2]\,y[2]^{25} + z\,z[2]^{25}\}$$

Out[88]=
$$\{x\,y^4 - z^5,\ -w\,y^5 + x^5\,z,\ x^6 - w\,y\,z^4,\ -w\,y^9 + x^4\,z^6,$$
$$-w\,y^{13} + x^3\,z^{11},\ -w\,y^{17} + x^2\,z^{16},\ -w\,y^{21} + x\,z^{21},\ -w\,y^{25} + z^{26}\}$$

Comparison degree of GB (input vs GB 1 individual symmetry vs GB no symmetries)

In[89]:=
```
lst = {};
For[i = 1, i ≤ 20, i++,
 Syms = IndividualSymmetries[
   {x y^(i - 1) - z^i, x^(i + 1) - y * z^(i - 1) * w, x^i z - y^i w}, {x, y, z, w}, 1];
 JSyms = Syms[[1]];
 PSyms = Syms[[2]];
 AppendTo[lst, {i, Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[
    GroebnerBasis[JSyms, PSyms, MonomialOrder → DegreeReverseLexicographic][[-1]]],
   Exponent[# /. ((# → x RandomReal[]) & /@ Variables[#]), x] &[
    GroebnerBasis[{x y^(i - 1) - z^i, x^(i + 1) - y * z^(i - 1) * w, x^i z - y^i w},
      {x, y, z, w}, MonomialOrder → DegreeReverseLexicographic][[-1]]]}]]
lst
```

Out[91]=
```
{{1, 2, 2}, {2, 5, 5}, {3, 10, 10}, {4, 17, 17}, {5, 26, 26},
 {6, 37, 37}, {7, 50, 50}, {8, 65, 65}, {9, 82, 82}, {10, 101, 101},
 {11, 122, 122}, {12, 145, 145}, {13, 170, 170}, {14, 197, 197}, {15, 226, 226},
 {16, 257, 257}, {17, 290, 290}, {18, 325, 325}, {19, 362, 362}, {20, 401, 401}}
```