The involutive GVW algorithm and the computation of Pommaret bases

Master Thesis

Thomas Izgin

Date of birth: 30th July 1994
Adress: Kurze Erlen 18, 34132 Kassel
Matriculation Number: 33311724

supervised by
Prof. Dr. Werner M. Seiler
Dr. Daniel Robertz

UNIKASSEL
VERSITÄT

Faculty 10 - Mathematics and Natural Sciences

January 15, 2020

Contents

1 Acknowledgment

I would like to express my deep and sincere gratitude to my research supervisors, Prof. Dr. Werner M. Seiler and Dr. Daniel Robertz. I thank Dr. Robertz for giving me the opportunity to do parts of the research at the University of Plymouth and providing invaluable guidance throughout the beginning of my research. The discussions with him have deeply inspired me. Moreover, he has taught me the methodology to carry out the research and to present the research works as clearly as possible. It was a great privilege and honour to research under his guidance. I would also like to thank Prof. Seiler for all the time he spent in mathematical discussions with me and for his very helpful ideas concerning issues that came up at the end of this thesis. In almost every discussion with him, I have grown beyond myself. He mentored and inspired me most of my time at the University of Kassel. It was a huge honour for me to be one of his students. I also want to thank him for the keen interest shown to complete this thesis successfully.
I am extending my thanks to Prof. Dr. Amir Hashemi for his support during my research work and the deep discussions related to his papers on this topic. Also, I want to thank him for his critical questions concerning my provided proofs, and his ideas concerning some aspects of the developed algorithm.
I am extremely grateful to my parents for their love, caring and sacrifices for educating and preparing me for my future. I am very much thankful to my fiancee for her love, understanding and continuing support to complete this research work. Finally, my thanks go to all the people who have supported me to complete the research work directly or indirectly.

2 Introduction

Gröbner bases provide a powerful tool for a wide variety of problems in commutative algebra, algebraic geometry and many other areas of science and engineering. For example, it can be interpreted as a generalization of the Gaussian elimination to the polynomial case [12]. 1965, Buchberger introduced the theory of Gröbner bases together with an algorithm to compute them [2]. Later, he presented two criteria to improve his algorithm finding superfluous reductions a priori. Since then, many mathematicians like Lazard, Gebauer and Möller, Faugère, Gao, Volny and Wang steadily worked on finding more such criteria or new methods to compute Gröbner bases more efficiently. Thereby, Lazard used techniques from linear algebra [12]. Gebauer and Möller used syzygies to find superfluous reductions. Moreover, Möller et al. extended their work and created the first signature-based algorithm to compute Gröbner bases [15]. Faugère has found a signature-based algorithm, called F5, that is many times more efficient than the previous algorithms when compared by benchmarks [5]. Now, many papers were published trying to simplify the F5 algorithm. The goal, of course, is also to develop an algorithm that is faster than F5 on benchmark systems. Indeed, Gao, Wang and Volny invented the so-called G2V algorithm that seems to be faster than F5 on benchmark systems according to [6] (two to ten times faster to be more precise). Based on G2V, the GVW algorithm was created which again seems to be faster than G2V [7]. Both G2V and GVW not only compute a Gröbner basis of an ideal but also one for its syzygy module. Thus, the algorithm is also a candidate for computing resolutions. Moreover, there are various papers about adapting the GVW algorithm to different mathematical applications or to make it more efficient. For instance, in [13], the authors are interested in adapting the GVW algorithm to principal ideal domains. For efficiency, in [14], the authors use an approach from linear algebra to implement the GVW algorithm with the help of matrix operations. There, they attack one major weakness of the GVW algorithm: all performed reductions must obey a certain restricting rule which leads to the fact that some elements that may be reduced according to other theories are not allowed to be reduced anymore. Thus, the algorithm becomes more inefficient as these elements will lead to more elements that need to be considered. However, the authors in [14] suggest a substituting method to create sparser matrices for signature-based algorithms by storing equivalent but sparser polynomials. They also demonstrate the efficiency of their algorithm. There are also so-called Hibert-driven signature-based algorithms which use the Hilbert

function to make the algorithm more efficient [17]. Moreover, there are approaches to deal with inhomogeneous ideals, too, introducing the concept of *mutant pairs* [18].
Another major part of this thesis is dealing with involutive bases, which are Gröbner bases with additional combinatorial properties. They originate from the works of Janet on the algebraic analysis of partial differential equations [11]. Zharkov and Blinkov introduced the notion of involutive polynomial bases using related works of Pommaret [20]. Later, Gerdt and Blinkov introduced involutive divisions [9]. Of special interest are Pommaret bases as one can read of many properties of an ideal like dimension, depth and Castelnuovo-Mumford regularity [16]. These properties remain unchanged after coordinate transformations, which is very important from a computational point of view as Pommaret bases do not always exist [16],[10]. However, Hashemi, Schweinfurter and Seiler have shown in [10] that a finite Pommaret basis of a *homogenous ideal* for the *degree reverse lexicographical order* exists after finitely many coordinate transformations of a certain type. Gerdt pointed out the special relationship between the Janet and Pommaret divisions in [8]. From further works on the relationship, we know that a Janet basis is also a Pommaret basis if it exists (see [16, Thm 4.3.15]). Thus, Seiler presents two approaches for computing a Pommaret basis of homogeneous ideals for the degree reverse lexicographical order: One can compute a Janet basis which always exists as the Janet division is Noetherian [16, Lem 3.1.19]. If a Pommaret basis exists, we already have computed it. Otherwise, he suggests to perform a coordinate transformation and compute a Janet basis of the transformed system and iterate this procedure. The second approach is to compute a Pommaret basis in a direct way and check during the algorithm whether a finite Pommaret basis exists, i.e. if the ideal is in *quasi-stable position*. If it is not quasi-stable, one may interrupt the algorithm, perform a coordinate transformation and start over again [16, S. 130].
Binaei, Hashemi and Seiler published in [1] a *semi-involutive*[1] version of the GVW algorithm and proved the termination by relating it to Gerdt's algorithm [1, Thm 6]. However, the proof is only given for Noetherian divisions, and thus, not for the Pommaret division. Also, their claim in [1, Thm 5] itself has flaws which we will point out in this thesis.
Moreover, we will develop a semi-involutive version of the GVW algorithm, but also a *full involutive variant*, where we will compute a (weak) Pommaret basis of the syzygy module. For both variants, we will give a proof of correctness for the Pommaret division and Janet division. In the case of the Pommaret division, we also give a proof of termination using coordinate transformations and a bound for

[1] i.e. they aimed to compute an involutive basis of an ideal and a Gröbner basis of its syzygy module.

the regularity of the ideal; and for the Janet division, we refer to results in [1]. Therefore, we can present two ways to compute a Pommaret basis of a homogeneous ideal: In both strategies, we start using the Janet version of the involutive GVW algorithm. From there we get an upper bound q for the regularity of the ideal [16, Cor 5.5.18]. Next, we check if the output is already a Pommaret basis. If not, we perform a coordinate transformation. As transformed syzygies are still syzygies, we can use them to make the algorithm in the next run more efficient because syzygies can be used for detecting superfluous reductions. Nevertheless, we can go in two different ways from there. First, we could iterate the Janet version. Secondly, we can use one of our Pommaret versions of the GVW algorithm (going only at most to the degree bound $q + 2$). However, we will introduce criteria where the algorithm may stop earlier with an error message that the ideal (or, in the full involutive case, its syzygy module) is not quasi-stable. Then, we perform a coordinate transformation and start over. Thus, this thesis is organized as follows:

In the next chapter, we give the theoretical fundamentals we use for the theory of Gröbner bases, syzygy modules, involutive bases and the GVW algorithm. Then, we will develop an involutive version of the GVW algorithm, first discussing the more complex Pommaret case. There, we also introduce an *index of safety* which supports us finding a suitable coordinate transformation for the restart. In the subsequent section, we gain a Janet version and prove its correctness. Afterwards, we give some remarks on implementation and introduce the index of safety. There, we also discuss the benefits and issues of the usage of a POT- or TOP-lift and present some statistics from the implementation of the algorithm in Maple 18. Lastly, we resume our obtained results and give an outlook for future works that may be based on the presented theory.

3 Theoretical Fundamentals

In this chapter, we will introduce the main tools for the following theory about the involutive GVW algorithm and its properties. First, we go into some of the details for the theory of Gröbner bases. Afterwards, we spend some time in recalling the original GVW algorithm. Furthermore, we will discuss some of the properties of the GVW algorithm in subsection 3.4.1 that were not mentioned in [6] and [7].

3.1 Gröbner Bases

Gröbner bases are the fundamental tool to describe the following theory. Thus, our first task is to present the corresponding notions and to introduce the used notations. The theory we present in this and the next section about Gröbner bases and syzygies can be found in [4] and [3].

Throughout the whole thesis, let $R \coloneqq K[x_1, \ldots, x_n]$ be a ring of polynomials in n variables and K a field with $\operatorname{char}(K) = 0$.
Furthermore, let $f_1, \ldots, f_m \in R$ and $F \coloneqq \{f_1, \ldots, f_m\}$. Moreover, we introduce $I \coloneqq \langle F \rangle = \left\{ \sum_{i=1}^{m} u_i f_i \,\middle|\, u_1, \ldots, u_m \in R \right\}$ as the *ideal* of F. Also, we call a product $x^\mu \coloneqq \prod_{i=1}^{n} x_i^{\mu_i} \in R$ a *term*, where $\mu_1, \ldots, \mu_n \in \mathbb{N}_0$. We define the *degree* of x^μ as $\deg(x^\mu) \coloneqq |\mu| = \sum_{i=1}^{m} \mu_i$. For $c \in K$, we call cx^μ a *monomial*. We denote by $\mathbb{T}_n$ the set of all terms of R. For $0 \neq f \coloneqq \sum_{i=1}^{k} c_i t_i \in R$ with $c_i \in K$ and $t_i \in \mathbb{T}_n$ we call $\operatorname{supp}(f) \coloneqq \{t_i \mid c_i \neq 0\}$ the *support* of f. If f is only a term x^μ, the *support* is defined as $\operatorname{supp}(x^\mu) \coloneqq \{x_i \mid \mu_i > 0\}$.
Next, we introduce the notion of *term orders*.

Definition 3.1.1
A *term order* on R is a total order $\prec$ on $\mathbb{T}_n$ such that

(i) $\forall\, r \in \mathbb{T}_n : 1 \preceq r$ and

(ii) $\forall\, r, s, t \in \mathbb{T}_n : s \prec t \Rightarrow rs \prec rt$.

$\prec$ is called *degree compatible*, if in addition

(iii) $\forall\, s, t \in \mathbb{T}_n : \deg(s) < \deg(t) \Rightarrow s \prec t$ holds.

For a given term order $\prec$ on R and $f \in R\backslash\{0\}$ we write $\mathrm{lt}_\prec(f) \coloneqq \max_\prec\{supp(f)\}$ for the *leading term* of f. The coefficient of $\mathrm{lt}_\prec(f)$ is called *leading coefficient* and is denoted by $\mathrm{lc}_\prec(f)$. The so-called *leading monomial* is the product of the two, i.e. $\mathrm{lm}_\prec(f) \coloneqq \mathrm{lc}_\prec(f) \cdot \mathrm{lt}_\prec(f)$. Furthermore, if $\mathrm{lt}_\prec(f) = x^\mu$ we write $\mathrm{le}_\prec(f) \coloneqq \mu$ for the *leading exponent*.
Moreover, we define the set $\mathrm{lt}_\prec(N) \coloneqq \{\mathrm{lt}_\prec(f) \mid f \in N \setminus \{0\}\}$ for a finite subset $\emptyset \neq N \subseteq R$. Also, we denote by $\mathrm{lt}_\prec(I) \coloneqq \langle \mathrm{lt}_\prec(f) \mid f \in I \setminus \{0\}\rangle$ the *leading ideal* of I. Lastly, we may note that if $\prec$ is known from the context we leave it out in the index.

One very important example of a degree compatible term order is the *degree reverse lexicographic* term order $\prec_{\mathrm{degrevlex}}$: We say $x^\mu \prec_{\mathrm{degrevlex}} x^\nu$, if $|\mu| < |\nu|$ applies or if $|\mu| = |\nu|$ and the first non-vanishing entry in $\mu - \nu$ is positive.

Next, we introduce the notion of Gröbner bases. There are several possible definitions, however, the following is the one most used in this work.

Definition 3.1.2
A finite set $G \subseteq I$ is called *Gröbner basis* of I for a term order $\prec$, if $\mathrm{lt}_\prec(I) = \langle \mathrm{lt}_\prec(G)\rangle$.

Buchberger showed one equivalent statement that can be achieved computationally. Before we can go to his theorem (see proposition 3.1.5), we first have to introduce some more notions.

Definition 3.1.3
Let $p_1, \ldots, p_r, g \in R$ and $r \in \mathbb{N}$. We set $P \coloneqq \{p_1, \ldots, p_r\}$.

(i) g is *reducible* by $p_i \in P$, if $\mathrm{lt}_\prec(p_i) \mid \mathrm{lt}_\prec(g)$. Otherwise g is called *irreducible* by p_i. We call g reducible by P, if g is reducible by some $p_i \in P$. Otherwise g is called irreducible by P.

(ii) If g is reducible by p_i, a *reduction step* is given by $h_1 \coloneqq g - \frac{\mathrm{lm}_\prec(g)}{\mathrm{lm}_\prec(p_i)} p_i$. We also write $g \to_{p_i} h_1$ for the reduction step.

(iii) g *reduces to* h *by* P, if there is a sequence $i_1, \ldots, i_s \in \{1, \ldots, r\}$ of indices such that
$$g \to_{p_{i_1}} h_1 \to_{p_{i_2}} h_2 \to_{p_{i_3}} \ldots \to_{p_{i_s}} h_s = h$$
and h is irreducible by P. We denote the reduction steps by $g \to_P^+ h$ and call h a *normal form* of g by P[1].

Now we will shortly recall the notion of S-polynomials which were first introduced by Buchberger.

[1] A normal form is unique if and only if P is a Gröbner basis.

Definition 3.1.4
Let $f, g \in R \setminus \{0\}$ and $t = \operatorname{lcm}(\operatorname{lt}_\prec(f), \operatorname{lt}_\prec(g))$. Then

$$S(f,g) \coloneqq \frac{t}{\operatorname{lm}_\prec(f)} f - \frac{t}{\operatorname{lm}_\prec(g)} g$$

is the *S-polynomial* of f and g.

Proposition 3.1.5 ***(Buchberger)***
Let $G \subseteq R$ be finite and $I = \langle G \rangle$. Then G is a Gröbner basis of I for a term order $\prec$ if and only if $S(f,g) \to_G^+ 0$ for every $f, g \in G$ with $f \neq g$.

This proposition results in the following algorithm: The basic idea is to reduce S-polynomials of any two distinct elements in F and add a normal form to F, if it is not zero. Then, the S-polynomial will reduce to zero by the updated F. However, one now has to look at more S-polynomials that are introduced by the normal form that entered F. Therefore, proof of termination is not trivial. The main idea is to produce an ascending chain of ideals which must become stationary as R is *Noetherian*.

The Buchberger Algorithm	
Input:	A finite subset $F = \{f_1, \ldots, f_m\} \subseteq R$, $\prec$ on R
Output:	A Gröbner basis G for $I = \langle F \rangle$ and $\prec$
Step 1:	$G \leftarrow F$
Step 2:	$S \leftarrow \{\{g_1, g_2\} \mid g_1, g_2 \in G \text{ with } g_1 \neq g_2\}$
Step 3:	**while** $S \neq \emptyset$ **do**
Step 4:	Choose a pair $\{g_1, g_2\} \in S$.
Step 5:	$S \leftarrow S \setminus \{g_1, g_2\}$ and calculate a normal form $\bar{g}$ of $S(g_1, g_2)$ by G.
Step 6:	**if** $\bar{g} \neq 0$ **then**
Step 7:	$S \leftarrow S \cup \{\{g, \bar{g}\} \mid g \in G\}$, $G \leftarrow G \cup \{\bar{g}\}$
Step 8:	**end if**
Step 9:	**end while**
Return:	G

In general, a Gröbner basis is not unique. However, a Gröbner basis G with the properties $\operatorname{supp}_\prec(g) \not\subseteq \langle \operatorname{lt}_\prec(G \setminus \{g\}) \rangle$ and $\operatorname{lc}_\prec(g) = 1$ for all $g \in G$ is called *reduced* Gröbner basis and is indeed unique. A reduced Gröbner basis can be computed with the help of *autoreductions*. In this regard, $g \in G$ is reducible by $G \setminus \{g\}$ if any element in its support is divisible by $\operatorname{lt}_\prec(G \setminus \{g\})$. The corresponding reduction step will then eliminate the appropriate term in the support of g. And

G is *autoreduced* if no $g \in G$ is reducible. Apart from autoreductions, we only consider reductions eliminating leading terms. Sometimes they are referred to as *top-reductions*. Performing only such reduction steps we can achieve a *head autoreduced* version of G.

3.2 Syzygies

In this section, we want to introduce syzygies and the term orders of our interest. The *syzygy module* of $F = \{f_1, \ldots, f_m\}$ is defined as

$$H \coloneqq Syz(F) \coloneqq \left\{ (u_1, \ldots, u_m) \in R^m \;\middle|\; \sum_{i=1}^{m} u_i f_i = 0 \right\}.$$

An element $\boldsymbol{u} \in H$ is called *syzygy* of F. As syzygies are vectors, we need to extend our notions of reduction steps and term orders to higher dimensions. First, we recall the notion of (vector) terms. Let $\boldsymbol{e}_i$ with $1 \leq i \leq m$ be the unit vectors in R^m. Then we call $x^\nu \boldsymbol{e}_j$ a *(vector) term*, where $x^\mu \in \mathbb{T}_n$. The set of all such terms is denoted by $\mathbb{T}_n^m$. We define $\deg(x^\mu \boldsymbol{e}_i) \coloneqq \deg(x^\mu)$.

Definition 3.2.1
A *term order* on R^m is a total order $\prec$ on $\mathbb{T}_n^m$ with

(i) $\forall x^\mu \in \mathbb{T}_n \setminus \{1\}, \boldsymbol{t} \in \mathbb{T}_n^m : \boldsymbol{t} \prec x^\mu \boldsymbol{t}$

(ii) $\forall x^\mu \in \mathbb{T}_n, \boldsymbol{s}, \boldsymbol{t} \in \mathbb{T}_n^m : \boldsymbol{s} \prec \boldsymbol{t} \Rightarrow x^\mu \boldsymbol{s} \prec x^\mu \boldsymbol{t}$

$\prec$ is called *degree compatible*, if in addition

(iii) $\forall\, \boldsymbol{s}, \boldsymbol{t} \in \mathbb{T}_n^m : \deg(\boldsymbol{s}) < \deg(\boldsymbol{t}) \Rightarrow \boldsymbol{s} \prec \boldsymbol{t}$ applies.

Next, we say that a vector term $x^\mu \boldsymbol{e}_i$ is divisible by another vector term $x^\nu \boldsymbol{e}_j$ if $i = j$ and $x^\nu \mid x^\mu$. With this notion, the extension of reduction steps for vector polynomials is straight forward and will be skipped in this section. However, it can be found in [4], [3]. In this thesis, we will focus on so-called POT- and TOP-lifts[2]. In the next example, we will specify the variant which we will use.

Example 3.2.2
Let $\prec$ be a term order on $\mathbb{T}_n$. Then we define

$$x^\mu \boldsymbol{e}_i \prec_{POT} x^\nu \boldsymbol{e}_j \Leftrightarrow i < j \quad \text{or} \quad (i = j \quad \text{and} \quad x^\mu \prec x^\nu)$$

[2]These are abbreviations for "position over term" and "term over position".

and

$$x^\mu \boldsymbol{e}_i \prec_{TOP} x^\nu \boldsymbol{e}_j \Leftrightarrow x^\mu \prec x^\nu \quad \text{or} \quad (x^\mu = x^\nu \quad \text{and} \quad i < j).$$

Also, we want to mention the *Schreyer order*. Let $S \coloneqq \{s_1, \ldots, s_k\} \subseteq R$ be finite and *ordered* set of polynomials. Then

$$x^\mu \boldsymbol{e}_i \prec_S x^\nu \boldsymbol{e}_j \Leftrightarrow \Big(\mathrm{lt}_\prec(x^\mu f_i) \prec \mathrm{lt}_\prec(x^\nu f_j)\Big) \quad \text{or} \quad \Big(\mathrm{lt}_\prec(x^\mu f_i) = \mathrm{lt}_\prec(x^\nu f_j) \ \text{ and } \ j < i\Big)$$

defines the Schreyer order.

3.3 Involutive Bases

In this section, we briefly recall the notion of involutive bases and introduce in particular the Pommaret and Janet division. This section is based on [16]. First, we define the notion of *involutive cones*.

Definition 3.3.1
An *involutive division* L is defined on $(\mathbb{N}_0^n, +)$, if for every finite subset $B \subseteq \mathbb{N}_0^n$ and every set $N_{L,B}(v) \subseteq \{1, \ldots, n\}$ of *multiplicative indices* of $v \in B$ and the set $L(v, B) \coloneqq \{\mu \in \mathbb{N}_0^n \mid \forall j \notin N_{L,B}(v) : \mu_j = 0\}$ the following two conditions for the *involutive cone* $C_{L,B}(v) \coloneqq v + L(v, B)$ are satisfied:

(i) If two involutive cones intersect each other, then one of them must contain the other.

(ii) For any subset $B' \subseteq B$ we have $N_{L,B}(v) \subseteq N_{L,B'}(v)$ for all $v \in B'$.

For $\mu, \nu \in \mathbb{N}_0^n$, we say μ is an *involutive divisor* of ν, written as $\mu \mid_{L,B} \nu$, if $\nu \in C_{L,B}(\mu)$ applies. The *involutive span* of $B \subseteq \mathbb{N}_0^n$ is

$$\langle B \rangle_L \coloneqq \bigcup_{v \in B} C_{L,B}(v). \tag{3.3.1}$$

Furthermore, we denote by $\bar{N}_{L,B}(v)$ the set of *non-multiplicative indices* of $v \in B$.

We want to point out a special type of involutive divisions, namely the *global* divisions, that are independent of the set B.
Now, one can relate involutive divisibility to the common notion of divisibility by

$$\mu \mid_{L,B} \nu \Leftrightarrow\colon x^\mu \mid_{L,B} x^\nu \quad \text{and} \quad x^\mu \mid_{L,B} x^\nu \Rightarrow x^\mu \mid x^\nu.$$

Given the set of multiplicative indices, we can introduce the set of *multiplicative variables* of $g \in G \subseteq R$ for a term order $\prec$ and a finite set G:

$$X_{L,G,\prec}(g) \coloneqq \{x_i \mid i \in N_{L,\mathrm{le}_\prec(G)}(\mathrm{le}_\prec g)\},$$

where $\mathrm{le}_\prec(G) \coloneqq \{\mathrm{le}_\prec(g) \mid 0 \neq g \in G\}$. The finite product of multiplicative variables is called *multiplicative term*. The involutive span of G is denoted by

$$\langle G\rangle_{L,\prec} \coloneqq \sum_{g\in G} K[X_{L,G,\prec}(g)] \cdot g \subseteq \langle G\rangle.$$

Definition 3.3.2
Let L be an involutive division on $(\mathbb{N}_0^n, +)$.

(i) A subset $B \subseteq \mathbb{N}_0^n$ is a *weak involutive basis* of B for L, if $\langle B\rangle_L = \langle B\rangle$ holds. In particular, B is called *strong involutive basis*, if in addition the union in (3.3.1) is disjoint. We call any set $B \subseteq B' \subseteq \mathbb{N}_0^n$ with $\langle B'\rangle_L = \langle B\rangle$ a *(weak) involutive completion* of B.

(ii) A set $G \subseteq I$ is called *weak/strong involutive basis* of I, if $\mathrm{le}_\prec(G)$ is a weak/strong involutive basis of $\mathrm{le}_\prec(I) \coloneqq \langle \mathrm{le}_\prec(f) \mid f \in I \setminus \{0\}\rangle$, where we additionally require for a strong basis that two distinct elements of G never possess the same leading exponents.

Since we have introduced involutive divisions in general, it is easy to extend our notions of reduction steps etc. from the previous sections to the involutive case. Thus, we will instead discuss the two major divisions which are important for this thesis.

Example 3.3.3
It will turn out that the *Pommaret division* is global. Therefore, it is more convenient for our purpose to define it through terms. For a term $x^\mu \coloneqq \prod_{j=k}^n x_j^{\mu_j}$ with $\mu_j \in \mathbb{N}_0$ and a $\mu_k \neq 0$ we define the *class* of x^μ as $cls(x^\mu) \coloneqq k$. Then the set $X_P(x^\mu) = \{x_i \mid i \leq cls(x^\mu)\}$ is the set of multiplicative variables of x^μ for the *Pommaret division*.

For the *Janet division*, we first introduce certain subsets of the given set $B \subseteq \mathbb{N}_0^n$:

$$(d_k, \ldots, d_n) \coloneqq \{v \in B \mid v_i = d_i, k \leq i \leq n\}.$$

Thus all elements in $(d_k, \ldots, d_n)$ have the same "k-tail". Now, the index n is multiplicative for $v \in B$, if $v_n = \max_{\mu\in B}\{\mu_n\}$. An index $k < n$ is multiplicative for v, if $v_k = \max_{\mu\in(v_{k+1},\ldots,v_n)}\{\mu_k\}$.

It is straight forward to see that the Janet division is not global, and thus more complex to use and implement than the Pommaret division. Still, it has some advantages over the Pommaret division. Nevertheless, the more interesting division for us is the Pommaret division since it provides us several theoretically interesting values. For example, from a Pommaret basis one can read off the dimension, depth and Castelnuovo-Mumford regularity of the ideal as mentioned in the introduction. But as we pointed out, a Pommaret basis does not always exists, whereas a Janet basis does. But because the two divisions are linked in some sense (see [8], [16]), there are ways to use Janet bases to compute Pommaret bases (as one can read in the introduction).

3.4 The GVW algorithm

In this section, we aim to compute a Gröbner basis of $I = \langle F \rangle$ for $\prec_1$, and of $Syz(F)$ for $\prec_2$ under some assumptions on the relation between the two term orders. This section is obtained from [6] and [7]. The fundamental object we are working on is the set M, defined in:

Definition 3.4.1
We set

$$M \coloneqq \{(\boldsymbol{u}, v) \in R^m \times R : \boldsymbol{u}\boldsymbol{f}^T = v\},$$

where $\boldsymbol{u} = (u_1, \ldots, u_m)$ and $\boldsymbol{f} = (f_1, \ldots, f_m)$ are row vectors in R^m.

Note, that $(\boldsymbol{u}, 0)$ represents a syzygy $\boldsymbol{u}$. In general, $\boldsymbol{u}$ encodes how to get v out of F.

Lemma 3.4.2
$M = \langle (\boldsymbol{e}_i, f_i) : 1 \leq i \leq m \rangle$ is a R-submodule of $R^m \times R$, where $\boldsymbol{e}_i$ denotes the i-th unit vector of R^m.

Because we operate on M, the term orders $\prec_1$ and $\prec_2$ must be compatible in some sense:

Definition 3.4.3
Let $\prec_1$ be a term order on R and $\prec_2$ one R^m. We say $\prec_2$ is *compatible* to $\prec_1$ if for arbitrary terms x^μ, x^ν in R the equivalence

$$x^\mu \prec_1 x^\nu \Leftrightarrow x^\mu \boldsymbol{e}_i \prec_2 x^\nu \boldsymbol{e}_i \ \forall 1 \leq i \leq m$$

holds.

Remark 3.4.4
From now on we use compatible term orders $\prec_1$ and $\prec_2$ on R and R^m, respectively. In particular, for $v \in R$ and $\boldsymbol{u} \in R^m$ we have the property

$$\mathrm{lt}_{\prec_2}(v \cdot \boldsymbol{u}) = \mathrm{lt}_{\prec_1}(v) \cdot \mathrm{lt}_{\prec_2}(\boldsymbol{u}),$$

coinciding with the law of a product of two polynomials in R. Hence, there will be no mistakes generated when we leave out the indices for the sake of simplicity. Furthermore, we write $\mathrm{lt}(v) = 0$, if $v = 0$ and $\mathrm{lt}(\boldsymbol{u}) = 0$, if $\boldsymbol{u} = \boldsymbol{0}$.

Next we define reduction steps on M and introduce two classes of reduction steps that will play a major role for this thesis.

Definition 3.4.5
Let $p_1 = (\boldsymbol{u}_1, v_1), p_2 = (\boldsymbol{u}_2, v_2) \in R^m \times R$. We say p_1 is *reducible* by p_2 if

(i) $v_1 \neq 0 \neq v_2$ and $\mathrm{lt}(v_2) \mid \mathrm{lt}(v_1)$,

(ii) $\mathrm{lt}(t\boldsymbol{u}_2) \preceq \mathrm{lt}(\boldsymbol{u}_1)$ with $t = \frac{\mathrm{lt}(v_1)}{\mathrm{lt}(v_2)}$.

We set $c \coloneqq \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)}$. Then a *reduction step* of p_1 by p_2 is given by a reduction step in the v-part performed on M, i.e.

$$s \coloneqq p_1 - ctp_2 = (\boldsymbol{u}_1 - ct\boldsymbol{u}_2, v_1 - ctv_2) = \left(\boldsymbol{u}_1 - \tfrac{\mathrm{lm}(v_1)}{\mathrm{lm}(v_2)}\boldsymbol{u}_2, v_1 - \tfrac{\mathrm{lm}(v_1)}{\mathrm{lm}(v_2)}v_2\right). \quad (3.4.1)$$

Moreover, we call $\mathrm{lt}(\boldsymbol{u}_1)$ the *signature* of p_1. If the signature of p_1 stays the same after a reduction step, the reduction is called *regular*, and *super* otherwise.
Also, we call p_1 regular/super reducible by $N \subseteq R^m \times R$, if p_1 is regular/super reducible by some $p \in N$. Furthermore, we denote by $\mathrm{Sig}(N)$ the set of all signatures of elements in N.

Lemma 3.4.6
A reduction step of p_1 by p_2 defined in (3.4.1) is super if and only if

$$\mathrm{lt}(t\boldsymbol{u}_2) = \mathrm{lt}(\boldsymbol{u}_1) \quad \text{and} \quad \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)} = \frac{\mathrm{lc}(\boldsymbol{u}_1)}{\mathrm{lc}(\boldsymbol{u}_2)}.$$

Definition 3.4.7
Let p_1, $p_2 \in R^m \times R$ with $v_2 = 0$ (so $\boldsymbol{u}_2$ is a syzygy). We say p_1 is *reducible by a syzygy* $p_2 = (\boldsymbol{u}_2, 0)$ if

$$\boldsymbol{u}_1 \neq \boldsymbol{0} \neq \boldsymbol{u}_2 \quad \text{and} \quad \mathrm{lt}(\boldsymbol{u}_2) \mid \mathrm{lt}(\boldsymbol{u}_1).$$

A *reduction step* of p_1 by p_2 is given by a reduction step of $\boldsymbol{u}_1$ by $\boldsymbol{u}_2$ performed on M, i.e.

$$h \coloneqq p_1 - \tfrac{\mathrm{lm}(\boldsymbol{u}_1)}{\mathrm{lm}(\boldsymbol{u}_2)}p_2 = \left(\boldsymbol{u}_1 - \tfrac{\mathrm{lm}(\boldsymbol{u}_1)}{\mathrm{lm}(\boldsymbol{u}_2)}\boldsymbol{u}_2, v_1\right).$$

Such a reduction step always reduces the signature of p_1, and hence, a reduction by a syzygy is always called super.

Remark 3.4.8
We want to note, that for any super reduction $\mathrm{lt}(\boldsymbol{u}_2) \mid \mathrm{lt}(\boldsymbol{u}_1)$ applies. Moreover, it is worth mentioning that a syzygy, by definition, is only reducible by a syzygy.

Now, as we are only discussing regular and super reductions, it is straight forward to see, that we save information about the signature the longer the more regular

reductions we perform before we perform a super reduction as the signature is invariant under regular reduction steps. Hence, our goal will be to first compute a *regular normal form*, i.e. the result of only regular reductions until no regular reduction is possible anymore. A regular normal form does not have to be unique as we are, in general, not reducing regular with respect to a Gröbner basis in the v-part. Having a regular normal form, the u-part encodes the "history" of our reductions, and the signature contains the information where we started the reduction steps.
Next, we want to "lift" the notion of a Gröbner basis to M.

Definition 3.4.9
A finite subset $G \subseteq M$ is called *strong Gröbner basis* of M, if every non-zero pair in M is reducible by G.

Now we present an important proposition that justifies the notion of a strong Gröbner basis. As we will give a very similar proof for the involutive version in chapter 4 we will skip it in this section. Nevertheless, it can be found in [6], [7].

Proposition 3.4.10
Let $G = \{(\boldsymbol{u}_1, v_1), \ldots, (\boldsymbol{u}_k, v_k)\}$ be a strong Gröbner basis of M. Then

(i) $G_0 \coloneqq \{\boldsymbol{u}_i \mid v_i = 0,\ 1 \leq i \leq k\}$ is a Gröbner basis of $Syz(F)$.

(ii) $G_1 \coloneqq \{v_i \mid 1 \leq i \leq k\}$ is a Gröbner basis of $I = \langle F \rangle$.

With that proposition we are interested in knowing if one can calculate a strong Gröbner basis efficiently. Indeed, Gao et al. presented an algorithm to compute a strong Gröbner basis as we are going to see. In particular, in the next chapter we aim to lift the theorems to involutive divisions.

Definition 3.4.11
Let $N \subseteq R^m \times R$ and $p = (\boldsymbol{u}_1, v_1) \in M$.

- p is called *eventually super reducible* by N, if a regular normal form of p is super reducible. As p can be regular irreducible, we call p also eventually super reducible, if it only is super reducible and not regular reducible at all.
- p is called *covered* by $q = (\boldsymbol{u}_2, v_2) \in N$ if $\mathrm{lt}(\boldsymbol{u}_2) \mid \mathrm{lt}(\boldsymbol{u}_1)$ and $\frac{\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec \mathrm{lt}(v_1)$ holds. We also may just say that p is covered by N.

If p is covered by q, this means that $\frac{\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_2)}q$ has the same signature as p but a smaller v-part. Hence, we have found a way to reduce p indirectly to a pair with smaller v-part and we may not have to look at p anymore. But this is a claim

worth proving. Indeed, the next theorem asserts that this is a good way to look at it. But before we present it, lets introduce one last notion.

Definition 3.4.12
Let $p_1 = (\boldsymbol{u}_1, v_1),\ p_2 = (\boldsymbol{u}_2, v_2) \in R^m \times R$ and $v_1 \neq 0 \neq v_2$.

For $i, j \in \{1, 2\}$ we set $t_i \coloneqq \mathrm{lt}(v_i)$ and $t_{ij} \coloneqq \mathrm{lcm}(t_i, t_j)$. Furthermore, we define

$$T \coloneqq \max_{\prec}\{\tfrac{t_{12}}{t_1}\mathrm{lt}(\boldsymbol{u}_1), \tfrac{t_{12}}{t_2}\mathrm{lt}(\boldsymbol{u}_2)\}.$$

Without loss of generality, let $T = \frac{t_{12}}{t_1}\mathrm{lt}(\boldsymbol{u}_1)$. Now, if for $c = \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)}$

$$\mathrm{lt}(\tfrac{t_{12}}{t_1}\boldsymbol{u}_1 - c\tfrac{t_{12}}{t_2}\boldsymbol{u}_2) = T \tag{3.4.2}$$

applies, we denote by $\frac{t_{12}}{t_1}p_1$ the *J-pair* of p_1 and p_2. Moreover, a reduction step is given by

$$\tfrac{t_{12}}{t_1}p_1 - c\tfrac{t_{12}}{t_2}p_2 = (\tfrac{t_{12}}{t_1}\boldsymbol{u}_1 - c\tfrac{t_{12}}{t_2}\boldsymbol{u}_2,\ \tfrac{1}{\mathrm{lc}(v_1)}S(v_1, v_2)), \tag{3.4.3}$$

and is regular by definition (see (3.4.2)). Here, $S(v_1, v_2)$ is the S-polynomial of v_1 and v_2 from definition 3.1.4.

So instead of calling the pair in (3.4.3) J-pair, Gao et al. suggest to go one step back in the reduction process and calling $\frac{t_{12}}{t_1}p$ a J-pair. Doing so, we have two things worth pointing out: First, we do not have to look at all S-polynomials as some of them may did not come from a regular reduction step and hence, will not satisfy (3.4.2). Moreover, by definition we can use the property that a J-pair is at least once regular reducible. This will be important for the proof of the next theorem. However, we will provide a proof for the involutive J-criteria in the next chapter. Thus, we just refer to [7] for the proof in this section. Also, it might be interesting to mention it at this point that our involutive J-pairs in general will not be involutive regular reducible at least once. Hence, we will be forced to give a proof for the involutive case where we cannot use that involutive J-pairs are involutive regular reducible by definition.
But let us first focus on the given case. From the next theorem, we will be able to generate an algorithm for computing a strong Gröbner basis.

Theorem 3.4.13 ***(J-criteria)***
Let $G \coloneqq \{(\boldsymbol{u}_1, v_1), \ldots, (\boldsymbol{u}_k, v_k)\} \subseteq M$ be a finite subset of M such that $\langle Sig(G)\rangle = \mathbb{T}_n^m$. Then the following statements are equivalent

(i) G is a strong Gröbner basis of M

(ii) Every J-pair of elements in G is eventually super reducible by G

(iii) Every J-pair of elements in G is covered by G

The corresponding algorithm is the following[3].

GVW algorithm	
Input:	$F = \{f_1, \ldots, f_m\} \subseteq R$, compatible term orders on R and R^m, A head autoreduced set H_0 of syzygies of F, where $H_0 = \emptyset$ is allowed, too.
Output:	A Gröbner basis V of $I = \langle f_1, \ldots, f_m \rangle$ and a Gröbner basis H of $Syz(F)$
Variables:	U is an ordered set of $\boldsymbol{u}_i$ of pairs $(\boldsymbol{u}_i, v_i) \in M$ V is an ordered set of v_i with $(\boldsymbol{u}_i, v_i) \in M$ H is the set of syzygies found so far JP is a set of J-pairs $t(\boldsymbol{u}_i, v_i)$ of $(\boldsymbol{u}_i, v_i)$ and $(\boldsymbol{u}_j, v_j)$ for a $j \neq i$ and a corresponding term t.
Step 1:	$U \leftarrow \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m\}$, $V \leftarrow \{f_1, \ldots, f_m\}$, $H \leftarrow H_0$
Step 2:	Compute the J-pairs of $(\boldsymbol{e}_1, f_1), \ldots, (\boldsymbol{e}_m, f_m)$ and fill JP.
Step 3:	**while** $JP \neq \emptyset$ **do**
Step 4:	Take the J-pair $t(\boldsymbol{u}_i, v_i)$ with smallest signature from JP, $JP \leftarrow JP \setminus \{t(\boldsymbol{u}_i, v_i)\}$
Step 5:	**if** $t(\boldsymbol{u}_i, v_i)$ is not covered by $(U, V) \cup (H, 0)$ **then**
Step 6:	Compute a regular normal form $(\boldsymbol{u}, v)$ of $t(\boldsymbol{u}_i, v_i)$ by (U, V)
Step 7:	**if** $v = 0$ **then**
Step 8:	$H \leftarrow H \cup \{\boldsymbol{u}\}$.
Step 9:	**else**
Step 10:	$U \leftarrow U \cup \{\boldsymbol{u}\}$, $V \leftarrow V \cup \{v\}$
Step 11:	Compute new J-pairs of $(\boldsymbol{u}, v)$ and $(\boldsymbol{u}_j, v_j)$ for $1 \leq j \leq \lvert U \rvert - 1$ and add them to JP
Step 12:	**end if**
Step 13:	**end if**
Step 14:	**end while**
Return:	V und H

[3] We have already included some optimization. For instance, if a J-pair is reducible by a syzygy it is also covered by it, and hence, can be discarded (the proof is really short and does not differ much from the involutive case – see lemma 4.1.1).

This algorithm is correct and terminates according to [7]. It is worth mentioning, that in the thesis from Volny (see [19]), the covered-criteria (statement c) of the J-criteria) was not discovered, yet. There, one had only the equivalence of (i) and (ii) from theorem 3.4.13. Therefore, it is generic that some J-pairs were first regular reduced and then discarded as the computed regular normal forms were found to be super reducible. However, this cannot happen with this version of the algorithm as a J-pair that is not covered is not eventually super reducible either[4]. Still, facing the problem of calculating unnecessary regular normal forms in Volny's thesis, he presents an idea to minimize the computational effort: In a first run, one only keeps the signatures rather than the whole u-part. This is sufficient for deciding whether or not a pair is regular or super reducible. So, the work in the u-part is minimized. With a second run of the algorithm, one knows already which J-pair reductions are superfluous and hence will avoid them[5]. Indeed, as we have the output of the first run, it will be enough to compute all u-parts of pairs with signatures less than the ones of syzygies from the output[6]. Still, this would mean to compute the v-parts again. So, this strategy may only pay off if many J-pairs are discarded, relatively speaking. If we knew the greatest signature of a syzygy a priori, it would make sense for our algorithm to keep only the signature once we have exceeded the greatest syzygy-signature. However, it might not be easy to give a *good* bound for leading terms of a Gröbner basis. For involutive bases on the other hand, it is a feasible task as we will discuss in the next chapter.
But first we enter the next subsection, where we will discuss if the algorithm will provide a minimal Gröbner basis of I or $Syz(F)$, respectively.

3.4.1 Minimal Gröbner Basis with the GVW algorithm

Very briefly saying, the basic idea of the GVW algorithm is to compute J-pairs and append regular normal forms to $G \coloneqq (U, V) \cup (H, 0)$, as they are covered by it. The covered-criteria allows us to avoid some unnecessary reduction steps. However, the covered J-pairs may were superfluous for the computation of V in the first place, and only important for the computation of $Syz(F)$ (see the next example). So, one should not think that the covered-criteria will necessarily save calculations for computing V. Also, because of $\langle \mathrm{Sig}(G) \rangle = \mathbb{T}_n^m$, we are forced to keep (a regular autoreduced version of) F contained in G. Hence, in general the strong Gröbner basis will not produce a minimal Gröbner basis for I. Moreover, the

[4] This is given by the fact that a J-pair is regular reducible at least once by definition and therefore the non involutive variant of lemma 4.1.2 can be applied.

[5] We will not discuss the details as they are not important for our case where we have the covered criteria.

[6] It might be worth mentioning that the strategy induced by step 4 is called *strategy of smallest signature.*

signature may not allow the reduction to ordinary normal forms. For example let $S(f_1, f_2) = xf_3$ for the elements in $F \coloneqq \{f_1, f_2, f_3\}$. If we choose now a POT-Lift, xf_3 may not be regular reducible by f_3 and will be inserted to V. Indeed, even regular autoreductions may not change this fact as the following example shows.

Example 3.4.14
Let K be a field and $R = K[x, y, z]$. We define $f_1 = xy + z$, $f_2 = x^2$, $f_3 = z$ and $F = \{f_1, f_2, f_3\}$. We take $\prec_{\text{degrevlex}}$ on R and a POT-Lift of it as a compatible term order on R^3, where $\boldsymbol{e}_i \prec \boldsymbol{e}_j$ for $i < j$ is the convention we use. We follow the strategy of smallest signature like suggested in [7] and will only keep the signatures instead of the whole u-part. Also, the J-pair of p_i and p_j is denoted by J_{ij}, and we start with $p_k = (\boldsymbol{e}_k, f_k)$ for $k = 1, 2, 3$. We set $G \coloneqq \{p_1, p_2, p_3\}$. All reduction steps we will perform are regular. So, we will truncate our notion of regular reduction steps for this example.
We have to look at $J_{12} = (y\boldsymbol{e}_2, yx^2)$ first. It reduces by p_1 to $(y\boldsymbol{e}_2, xz)$ which is not regular reducible by G. Hence, we will call it p_4 and insert it to G. Next, we have to look at $J_{14} = (y^2\boldsymbol{e}_2, xyz)$ which reduces by p_1 to $(y^2\boldsymbol{e}_2, z^2)$. This pair is also not regular reducible by the current G. So, we call it p_5 and add it to G, which still is regular autoreduced. Fortunately, the next J-pair $J_{24} = (xy\boldsymbol{e}_2, x^2z)$ is reducing by p_2 to a syzygy with signature $xy\boldsymbol{e}_2$. This syzygy covers all next J-pairs J_{i5} for $i = 1, 2, 3, 4$. Hence, the next J-pair to consider is $J_{34} = (x\boldsymbol{e}_3, xz)$ which reduces by p_4 to a syzygy with signature $x\boldsymbol{e}_3$. Lastly, this syzygy will cover the last two J-pairs J_{13} and J_{23} so that, due to theorem 3.4.13, we obtain with

$$G = \{(\boldsymbol{e}_1, f_1), (\boldsymbol{e}_2, f_2), (\boldsymbol{e}_3, f_3), (y\boldsymbol{e}_2 - x\boldsymbol{e}_1, xz), (y^2\boldsymbol{e}_2 - z\boldsymbol{e}_1, z^2), (\boldsymbol{s}_1, 0), (\boldsymbol{s}_2, 0)\}$$

a strong Gröbner basis of M, where $\boldsymbol{s}_1 = (xy - z)\boldsymbol{e}_2 - x\boldsymbol{e}_1$ and $\boldsymbol{s}_2 = x\boldsymbol{e}_3 - y\boldsymbol{e}_2 + x\boldsymbol{e}_1$ are calculated by keeping track of the whole u-part during the computations above. But obviously, we will not get a minimal Gröbner basis of I. In particular, we started with a Gröbner basis of I and the algorithm created new elements for it in order to compute $Syz(F)$.

However, we are able to show that H is a minimal Gröbner basis of $Syz(F)$ if we make the signatures in the algorithm monic.

Corollary 3.4.15
The GVW algorithm returns a minimal Gröbner basis H for $Syz(F)$ if the leading coefficients of the signatures are 1. This still holds if during the algorithm regular head autoreductions are performed using the strategy of smallest signature.

Proof. Assume, for a proof by contradiction, that $\boldsymbol{u}_1, \boldsymbol{u}_2 \in H$ and $\boldsymbol{u}_1$ is reducible by $\boldsymbol{u}_2$, i.e. $\mathrm{lt}(\boldsymbol{u}_2) \mid \mathrm{lt}(\boldsymbol{u}_1)$. Then $\mathrm{lt}(\boldsymbol{u}_2) \preceq \mathrm{lt}(\boldsymbol{u}_1)$. Because of the strategy of smallest signatures $\boldsymbol{u}_1$ has entered H later than $\boldsymbol{u}_2$ if it is a regular normal form of a J-pair.

Indeed, $\boldsymbol{u}_2$ cannot enter after $\boldsymbol{u}_1$ through regular head autoreductions, either, as at the time we consider $\boldsymbol{u}_1$, regular autoreductions will only effect elements with greater signature than $\mathrm{lt}(\boldsymbol{u}_1)$. Assume first, that $\boldsymbol{u}_1$ is the u-part of a regular normal form of a J-pair. Now, since $\boldsymbol{u}_2$ was in H first, the J-pair corresponding to $\boldsymbol{u}_1$ is covered by $(\boldsymbol{u}_2, 0)$ and hence would have been discarded.
Next assume that $\boldsymbol{u}_1$ came from regular autoreductions and not from a J-pair. Then $\mathrm{lt}(\boldsymbol{u}_2) \prec \mathrm{lt}(\boldsymbol{u}_1)$. Hence, $\boldsymbol{u}_1$ must be the u-part of a regular normal form of a $(\boldsymbol{e}_i, f_i)$. Then $\mathrm{lt}(\boldsymbol{u}_2) \mid \mathrm{lt}(\boldsymbol{u}_1) = \boldsymbol{e}_i$, which implies $\mathrm{lt}(\boldsymbol{u}_2) = \boldsymbol{e}_i$. This would mean that we have computed a regular normal form of $(\boldsymbol{e}_i, f_i)$ twice in two different ways, which will not happen during the algorithm as we are replacing $(\boldsymbol{e}_i, f_i)$ by the computed regular normal form during regular autoreductions. □

4 Involutive GVW algorithm

In this chapter we will develop an involutive version of the GVW algorithm. For this purpose, we first adjust some of the definitions made in the previous chapter. Here, we will be able to prove a "full" involutive version of the GVW algorithm, i.e. one where also the division in the u-part is involutive. We will then prove the termination and present the *semi-involutive* GVW algorithm, where we use the classical division on the u-part and an involutive one in the v-part. We will show that the full involutive version for the Pommaret division will provide us weak Pommaret bases of I and $Syz(F)$ whereas the semi-involutive variant only produces a Gröbner basis for $Syz(F)$, in theory. However, we will prove the termination of the semi-inv. variant only for the case where we focus on finding the Pommaret basis of I and then stop the computation (a Gröbner basis of $Syz(F)$). Still, there might be a proof for the general case.
Thus, in our implementation one can choose whether or not the whole u-part shall be computed. If a Gröbner basis H of $Syz(F)$ is computed during the algorithm, iteration of the algorithm with H in the v-part will eventually produce a weak involutive basis after adapting the algorithm for module inputs. Also, the criteria we will provide are stronger in the semi-involutive variant, which implies a faster termination of the algorithm.
Recall, that we are looking at an ideal $I \coloneqq \langle f_1, \dots, f_m \rangle \trianglelefteq K[x_1, \dots, x_n]$ and the set $M \coloneqq \{(\boldsymbol{u}, v) \mid \boldsymbol{u}^T \boldsymbol{f} = v\}$, where $\boldsymbol{f}$ is the vector with entries f_i. Furthermore we set $\prec_1 = \prec_{\text{degrevlex}}$ on $\mathbb{T}_n$ and choose a compatible term $\prec_2$ of *type* ω, i.e. between any two terms there are only finitely many terms.
For the whole chapter, let $G \subseteq M$ be a finite set and $B_u \times B_v \subseteq \mathbb{N}_0^m \times \mathbb{N}_0^m$, where B_u is the set of exponents of signatures in G and B_v the set of leading exponents of elements in the v-part of G.

Definition 4.0.1
We write $p_i := (\boldsymbol{u}_i, v_i)$ for $i = 1, 2$. Let in particular $p_1 \in M$ and $p_2 \in G$. Finally, let L be an involutive division.

a) p_1 is *involutively covered by* p_2 if

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_{L, B_u} \mathrm{lt}(\boldsymbol{u_1}) \quad \text{and} \quad \frac{\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_2)} \mathrm{lt}(v_2) \prec \mathrm{lt}(v_1).$$

We say that p_1 is *involutively covered by* $G \subseteq M$ if it is involutively covered by some element in G.

b1) p_1 is called *involutively regular reducible by* p_2 if the following conditions hold:

(i) $v_1 \neq 0 \neq v_2$,

(ii) $\mathrm{lt}(v_2) \mid_{L,B_v} \mathrm{lt}(v_1)$ and

(iii) for $(\boldsymbol{u}, v) \coloneqq p_1 - \frac{\mathrm{lm}(v_1)}{\mathrm{lm}(v_2)} p_2$ we have $\mathrm{lt}(\boldsymbol{u}) = \mathrm{lt}(\boldsymbol{u}_1)$.

Moreover, we say that p_1 is *involutively super reducible by* p_2 if the conditions $(i), (ii)$, and

(iii') $\mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_1)$ and $\mathrm{lt}(\boldsymbol{u}) \prec \mathrm{lt}(\boldsymbol{u}_1)$ are satisfied.

b2) If p_2 is a syzygy, i.e. $v_2 = 0$, then p_1 is called *involutively super reducible by* p_2 if

$$\boldsymbol{u}_1 \neq \mathbf{0} \neq \boldsymbol{u}_2 \quad \text{and} \quad \mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_1).$$

For an involutive super reduction we perform a reduction of the u-part, analogously to the previous chapter.

b3) p_1 is called *involutively reducible by* p_2 if it is reducible in the sense of b1) or b2). Moreover, p_1 is involutively reducible by G if it is involutively reducible by some element in G.

c) A pair $p \in M$ is called *eventually involutively super reducible* by $G \subseteq M$ if there is a chain – a length of zero is allowed – of involutive regular reduction steps by G leading to an *involutive regular normal form*[1] of p which in turn is involutively super reducible by G.

d) We write $p_2 \mid_{L,B} p_1$ if $\mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_1)$ and $\mathrm{lt}(v_2) \mid_{L,B_v} \mathrm{lt}(v_1)$.

Remark
Note that in b1)(iii') the condition $\mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_1)$ is essentially. Therefore, in contrast to the previous chapter, the conditions b1)(i)-(ii) and

$$\frac{\mathrm{lm}(v_1)}{\mathrm{lm}(v_2)} \mathrm{lt}(\boldsymbol{u}_2) \preceq \mathrm{lt}(\boldsymbol{u}_1)$$

do *not* imply involutive reducibility. In particular, it can happen that from this conditions we face a super reduction which is not involutive, i.e. we have $p_2 \mid p_1$ but not $p_2 \mid_{L,B} p_1$. Furthermore, from now on we may write the abbreviation "inv." whenever we should write "involutive(ly)".

[1] This means that no more involutive regular reduction steps are possible.

Next, we translate the definition of a strong Gröbner basis to the involutive case.

Definition 4.0.2
A finite set $G \subseteq M$ is called *strong L-basis* of M, if any non-zero pair $p = (\boldsymbol{u}, v) \in M$ is inv. reducible by G.

Gao et al. achieved a computational access to obtain a strong Gröbner basis based on S-polynomials which are associated with a criterion for computing Gröbner bases (see definition 3.4.12). In our case, the involutive pendant is encoded in [16, Def. 4.1.1, Prop. 4.1.4]. Hence, we get the following definition for involutive J-pairs.

Definition 4.0.3
Let $p \coloneqq (\boldsymbol{u}, v) \in G$ and $v \neq 0$. Let $\bar{X}_{L,B_v}(v)$ be the set of non-multiplicative variables of $\mathrm{lt}(v)$. Then every element of the set

$$\{x_k p \mid x_k \in \bar{X}_{L,B_v}(v)\}$$

is called *involutive J-pair of* p. Furthermore, every term that is multiplicative for $\mathrm{lt}(\boldsymbol{u})$ and $\mathrm{lt}(v)$ is called a *multiplicative term* for p.

4.1 Involutive J-Criteria (I) for the Pommaret Division

With the notions from the last section we now can go to our first theorem. It will later be discussed however that this version will not be our basis for the implementation. For the purpose of a better reading flow we first prove some lemmas.

First, we want to recall small lemmas combining some notions used in the definitions above. Furthermore, some of these lemmas are just the involutive version of results in [7].

Lemma 4.1.1
A pair $(\boldsymbol{u}, v) \in M$ with $v \neq 0$ that is inv. super reducible by a syzygy $(\boldsymbol{u}_1, 0) \in G$ is also inv. covered by it.

Proof. It applies $\mathrm{lt}(\boldsymbol{u}_1) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u})$ and $\frac{\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u})} \cdot 0 = 0 \prec \mathrm{lt}(v)$. □

Lemma 4.1.2
Let $p \coloneqq (\boldsymbol{u}, v) \in M$ be inv. regular reducible at least once by G. If a regular normal form $(\boldsymbol{u}', v')$ of p is an element of G, then p is inv. covered by $(\boldsymbol{u}', v')$.

Proof. From our assumptions we know that $\mathrm{lt}(\boldsymbol{u}') = \mathrm{lt}(\boldsymbol{u})$ and $\mathrm{lt}(v') \prec \mathrm{lt}(v)$. Therefore, we get $\mathrm{lt}(\boldsymbol{u}') \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u})$ and $\frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}')}\mathrm{lt}(v') = \mathrm{lt}(v') \prec \mathrm{lt}(v)$. □

Lemma 4.1.3
The relations "inv. covered by", "inv. reducible by a syzygy" and "inv. super reducible by a non-syzygy" are transitive on G.

Proof. Let $(\boldsymbol{u}_i, v_i) \in G$ for $i = 1, 2, 3$. Now assume that $(\boldsymbol{u}_j, v_j)$ is inv. covered by $(\boldsymbol{u}_i, v_i)$ for $1 \leq i < j \leq 3$. Then $\mathrm{lt}(\boldsymbol{u}_1) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_3)$ and

$$\frac{\mathrm{lt}(\boldsymbol{u}_2)}{\mathrm{lt}(\boldsymbol{u}_1)}\mathrm{lt}(v_1) \prec \mathrm{lt}(v_2) \quad \text{and} \quad \frac{\mathrm{lt}(\boldsymbol{u}_3)}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec \mathrm{lt}(v_3)$$

This implies

$$\frac{\mathrm{lt}(\boldsymbol{u}_3)}{\mathrm{lt}(\boldsymbol{u}_1)}\mathrm{lt}(v_1) = \frac{\mathrm{lt}(\boldsymbol{u}_3)}{\mathrm{lt}(\boldsymbol{u}_2)}\frac{\mathrm{lt}(\boldsymbol{u}_2)}{\mathrm{lt}(\boldsymbol{u}_1)}\mathrm{lt}(v_1) \prec \frac{\mathrm{lt}(\boldsymbol{u}_3)}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec \mathrm{lt}(v_3).$$

Next, we assume that $(\boldsymbol{u}_j, v_j)$ is inv. super reducible by $(\boldsymbol{u}_i, v_i)$ for $1 \leq i < j \leq 3$. If $v_1 = v_2 = 0$, then $\mathrm{lt}(\boldsymbol{u}_1) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_3)$ and we are done.
So, let's go to the next part of the claim, where we have $v_i \neq 0$ for $1 \leq i < j \leq 3$. Since a syzygy is only inv. reducible by another syzygy we obtain $v_3 \neq 0$, too. By definition, this implies

$$\mathrm{lt}(\boldsymbol{u}_1) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_3)$$

and

$$\mathrm{lt}(v_1) \mid_{L,B_v} \mathrm{lt}(v_2) \mid_{L,B_v} \mathrm{lt}(v_3).$$

In addition, we get

$$\frac{\mathrm{lm}(\boldsymbol{u}_2)}{\mathrm{lm}(\boldsymbol{u}_1)} = \frac{\mathrm{lm}(v_2)}{\mathrm{lm}(v_1)} \quad \text{and} \quad \frac{\mathrm{lm}(\boldsymbol{u}_3)}{\mathrm{lm}(\boldsymbol{u}_2)} = \frac{\mathrm{lm}(v_3)}{\mathrm{lm}(v_2)}.$$

We multiply both sides of the equations with each other and obtain

$$\frac{\mathrm{lm}(\boldsymbol{u}_3)}{\mathrm{lm}(\boldsymbol{u}_1)} = \frac{\mathrm{lm}(v_3)}{\mathrm{lm}(v_1)},$$

and thus, we are done. □

For the next Lemma, we have to extend the spectrum of our notions a bit.

Definition 4.1.4
If for $(\boldsymbol{u}, v) \in M$ there is a $(\boldsymbol{u}', v') \in G$ with $\mathrm{lt}(\boldsymbol{u}') \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u})$, $\mathrm{lt}(v') \mid \mathrm{lt}(v)$, and $\frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}')} = \frac{\mathrm{lt}(v)}{\mathrm{lt}(v')}$, we call $(\boldsymbol{u}, v)$ *pseudo reducible* by $(\boldsymbol{u}', v')$.

Although, the next lemma may not look very interesting, it will be used in later proofs for optimization of the final algorithms for the Pommaret division. Hence, we will only prove it for this division. Now, as the Pommaret division is global, we are not bound by G.

Lemma 4.1.5
Let $(\boldsymbol{u}, v) \in M$ with $v \neq 0$, $G \subseteq M$ finite and $L = P$ be the Pommaret division.

a) If $(\boldsymbol{u}, v)$ is eventually inv. super reducible by G where at least one inv. reduction is regular, then it is inv. covered by G. This stays true for arbitrary involutive divisions L.

b) If $(\boldsymbol{u}, v)$ is inv. covered by some pair $(\boldsymbol{u}', v') \in M$ which in turn is inv. super reducible by G, then $(\boldsymbol{u}, v)$ is inv. covered by G.

c) If $(\boldsymbol{u}, v)$ is pseudo reducible by $(\boldsymbol{u}', v') \in M$ and if $(\boldsymbol{u}', v')$ is inv. covered by G, then $(\boldsymbol{u}, v)$ is inv. covered by G.

Proof. ad a): We calculate an inv. regular normal form $p_1 \coloneqq (\boldsymbol{u}_1, v_1)$ of $(\boldsymbol{u}, v)$. Note that $\mathrm{lt}(\boldsymbol{u}) = \mathrm{lt}(\boldsymbol{u}_1)$ and $\mathrm{lt}(v_1) \prec \mathrm{lt}(v)$ since we only performed regular reductions. According to our assumptions, p_1 is inv. super reducible by some $p_2 \coloneqq (\boldsymbol{u}_2, v_2) \in G$. In the case of $v_2 = 0$, this implies

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u}) \quad \text{and} \quad \frac{\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) = 0 \prec \mathrm{lt}(v).$$

Therefore p is inv. covered by p_2. For $v_2 \neq 0$ it follows that

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_{L,B_u} \mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u}) \quad \text{and} \quad \frac{\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) = \frac{\mathrm{lt}(v_1)}{\mathrm{lt}(v_2)}\mathrm{lt}(v_2) = \mathrm{lt}(v_1) \prec \mathrm{lt}(v).$$

Hence, p is always inv. covered by G.
ad b): If $(\boldsymbol{u}', v')$ is inv. super reducible by a syzygy $(\boldsymbol{u}_2, 0)$, then $(\boldsymbol{u}, v)$ is inv. covered by the same syzygy since $\mathrm{lt}(\boldsymbol{u}_2) \mid_P \mathrm{lt}(\boldsymbol{u}') \mid_P \mathrm{lt}(\boldsymbol{u})$. Hence, we assume as in part a) that $(\boldsymbol{u}_2, v_2)$ is not a syzyzgy. Then $\mathrm{lt}(\boldsymbol{u}_2) \mid_P \mathrm{lt}(\boldsymbol{u}')$ and $\frac{\mathrm{lt}(\boldsymbol{u}')}{\mathrm{lt}(\boldsymbol{u}_2)} = \frac{\mathrm{lt}(v')}{\mathrm{lt}(v_2)}$. Because $(\boldsymbol{u}, v)$ is inv. covered by $(\boldsymbol{u}', v')$ we have $\mathrm{lt}(\boldsymbol{u}') \mid_P \mathrm{lt}(\boldsymbol{u})$ and $\frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}')}\mathrm{lt}(v') \prec \mathrm{lt}(v)$. Hence, we have

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_P \mathrm{lt}(\boldsymbol{u}') \mid_P \mathrm{lt}(\boldsymbol{u}) \quad \text{and} \quad \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) = \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}')\frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v')}}\mathrm{lt}(v_2) = \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}')}\mathrm{lt}(v') \prec \mathrm{lt}(v),$$

and thus, $(\boldsymbol{u}, v)$ is inv. covered by G.
ad c): As p' is inv. covered by G, there exists a pair $(\boldsymbol{u}_2, v_2) \in G$ such that

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_P \mathrm{lt}(\boldsymbol{u}') \quad \text{and} \quad \frac{\mathrm{lt}(\boldsymbol{u}')}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec \mathrm{lt}(v').$$

From $\frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}')} = \frac{\mathrm{lt}(v)}{\mathrm{lt}(v')}$ it follows that

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_P \mathrm{lt}(\boldsymbol{u}') \mid_P \mathrm{lt}(\boldsymbol{u}) \quad \text{and} \quad \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) = \frac{\mathrm{lt}(\boldsymbol{u}')\frac{\mathrm{lt}(v)}{\mathrm{lt}(v')}}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec \frac{\mathrm{lt}(v)}{\mathrm{lt}(v')}\mathrm{lt}(v') = \mathrm{lt}(v).$$

Therefore, we are done. □

The next lemma is very important for both divisions. And of course, we aim to find a computational approach to compute strong L-bases. The following lemma is the first step towards this goal. Later, we will make a few more assumptions to show that the statements indeed are equivalent. Nevertheless, without any further assumptions being made, we obtain the following result already.

Lemma 4.1.6
Let L be an involutive division. Let $G \subseteq M$ be a finite set. Then the implications "$a) \Rightarrow b) \Rightarrow c)$" hold, where

a) G is a strong L-basis of M.

b) Every involutive J-pair of elements of G is eventually inv. super reducible by G.

c) Every involutive J-pair of elements of G is inv. covered by G or inv. super reducible by G.

Proof. We first prove "$a) \Rightarrow b)$". Suppose, G is a strong L-basis. Now let p be an involutive J-pair of an element of G. Since $p \in M$, we know that p is involutive reducible. If the reduction is super, we are done. Otherwise the reduction is regular, and we calculate an inv. regular normal form which lies again in M. Therefore, it is still inv. reducible and now it must be an inv. super reduction. Hence, b) is shown.

Now suppose b) is true. We write again $p \coloneqq (\boldsymbol{u}, v) \in M$ for an arbitrary involutive J-pair. By definition of a J-pair we know $v \neq 0$.
Applying b), we can conclude that p is eventually inv. super reducible by G. If no regular reduction is possible, p is inv. super reducible and c) is true. However, if an inv. regular reduction is possible, we apply lemma 4.1.5 a) and we are done. □

We need one more rather technical lemma before we come to the actual result of this section.

Lemma 4.1.7
Let $L = P$ be the Pommaret division. Let $G \subseteq M$ be a finite set. Suppose that every J-pair in G is inv. covered or inv. super reducible by G.
Let $(\boldsymbol{u}, v) \in M$ be non-zero and suppose there is a pair $p_1 \coloneqq (\boldsymbol{u}_1, v_1) \in G$ with $v_1 \neq 0$ such that

(i) $\mathrm{lt}(\boldsymbol{u}_1) \mid_P \mathrm{lt}(\boldsymbol{u})$ and

(ii) $t\mathrm{lt}(v_1) \coloneqq \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_1)}\mathrm{lt}(v_1)$ is minimal under all elements in G that satisfy condition (i).

Then the following statements are true:

a) tp_1 is not inv. covered by G.

b) If t contains a non-multiplicative variable for $\mathrm{lt}(v_1)$ then there exists a pair $p' \coloneqq (\boldsymbol{u}', v') \in G$ such that $v' \neq 0$ and tp_1 is inv. super reducible by p'.

c) If G is inv. head autoreduced w.r.t. the v-part then tp_1 is not inv. regular reducible by G.

Proof. Since $(\boldsymbol{u}, v) \neq (\mathbf{0}, 0)$ we conclude $\mathrm{lt}(\boldsymbol{u}) \neq \mathbf{0}$. Now lets go into the first statement.

ad a): Assuming that a) is false we will provide a contradiction as follows. We assume that tp_1 is inv. covered by a pair $(\boldsymbol{u}_2, v_2) \in G$. But this implies $\mathrm{lt}(\boldsymbol{u}_2) \mid_P t\mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u})$ and $\frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec t\mathrm{lt}(v_1)$, violating condition (ii).

ad b): By our assumptions t is multiplicative for $\mathrm{lt}(\boldsymbol{u})$ and contains a non-multiplicative variable for $\mathrm{lt}(v_1)$. Let $l \coloneqq \deg(t)$ and x_k be the variable with the largest index occurring in t. Since t contains a non-multiplicative variable, x_k must be non-multiplicative for $\mathrm{lt}(v_1)$, too. Note, that $x_k \mid_P t$. Furthermore, $x_k p_1$ is an inv. J-pair. By our assumptions there are now two possibilities.

In the first case $x_k p_1$ is inv. covered by G. Then there exists $(\boldsymbol{u}_2, v_2) \in G$ such that

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_P x_k\mathrm{lt}(\boldsymbol{u}_1) \quad \text{and} \quad \frac{x_k\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec x_k\mathrm{lt}(v_1).$$

But because $x_k \mid_P t$ is true and t is multiplicative for $\mathrm{lt}(\boldsymbol{u}_1)$, we obtain

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_P t\mathrm{lt}(\boldsymbol{u}_1) \quad \text{and} \quad \frac{t\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec t\mathrm{lt}(v_1),$$

which contradicts a).

Now, for the second case we assume that $x_k p_1$ is inv. super reducible by a pair $p_3 \coloneqq (\boldsymbol{u}_3, v_3) \in G$. If $v_3 = 0$, then $x_k p_1$ is also inv. covered by p_3 because v_1 is non-zero by our assumptions (see lemma 4.1.1). But we have just shown in the

first case that this leads to a contradiction. Therefore, we have $v_3 \neq 0$. Now, by definition we obtain the relations

$$\mathrm{lt}(v_3) \mid_P x_k\mathrm{lt}(v_1) \quad \text{and} \quad \mathrm{lt}(\boldsymbol{u}_3) \mid_P x_k\mathrm{lt}(\boldsymbol{u}_1) \mid_P t\mathrm{lt}(\boldsymbol{u}_1).$$

If in addition to this the relation $\mathrm{lt}(v_3) \mid_P t\mathrm{lt}(v_1)$ is true, we are done since x_kp_1 and tp_1 have the same leading coefficients (because then tp_1 would be inv. super reducible by p_3). So let us suppose that this is not the case, i.e. there must be a non-multiplicative variable for $\mathrm{lt}(v_3)$ left in $\frac{t}{x_k}$. Then, we iterate our arguments, now taking the variable x_h appearing in $\mathrm{supp}(\frac{t}{x_k})$ with the largest index and looking at the J-pair $x_h(\boldsymbol{u}_3, v_3)$. Note that $x_h \mid_P \frac{t}{x_k}$, or equivalently $x_hx_k \mid_P t$ holds (remember that $h \leq k$).
Then, we end up again with a pair $p_4 \coloneqq (\boldsymbol{u}_4, v_4) \in G$ with $v_4 \neq 0$, from which we know that it reduces x_hp_3 inv. super. In particular, we have

$$\mathrm{lt}(v_4) \mid_P x_h\mathrm{lt}(v_3) \mid_P x_hx_k\mathrm{lt}(v_1) \quad \text{and} \quad \mathrm{lt}(\boldsymbol{u}_4) \mid_P x_h\mathrm{lt}(\boldsymbol{u}_3) \mid_P x_hx_k\mathrm{lt}(\boldsymbol{u}_1) \mid_P t\mathrm{lt}(\boldsymbol{u}_1)$$

Repeating this procedure, we finish after at most $l = \deg(t)$ steps, obtaining a pair which satisfies all properties that we have claimed in b).

ad c): We prove this by contradiction. Suppose, that tp_1 is inv. regular reducible by a pair $p_2 \coloneqq (\boldsymbol{u}_2, v_2) \in G$. Hence, $v_2 \neq 0$. Now,we are facing three cases.
Firstly, $t = 1$. This leads to $\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v_1)$, and hence, to a contradiction because G is inv. head autoreduced w.r.t. the v-part.
Also, if $t \neq 1$ is a multiplicative term for $\mathrm{lt}(v_1)$ we have $\mathrm{lt}(v_1) \mid_P t\mathrm{lt}(v_1)$ and still $\mathrm{lt}(v_2) \mid_P t\mathrm{lt}(v_1)$. Therefore, we must have $\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v_1)$ or $\mathrm{lt}(v_1) \mid_P \mathrm{lt}(v_2)$ violating again our assumption in c).
Hence, only one case is possible: $t \neq 1$ contains a non-multiplicative variable for $\mathrm{lt}(v_1)$. But in this case, we can apply b) and obtain a pair p' as described in b). Then, tp_1 cannot be inv. regular reducible by p'. So, we have $p' \neq p_2$. However, we have $\mathrm{lt}(v') \mid_P t\mathrm{lt}(v_1)$ and $\mathrm{lt}(v_2) \mid_P t\mathrm{lt}(v_1)$. This again implies $\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v')$ or vice versa, both violating the condition that G is inv. head autoreduced w.r.t. the v-part. □

Note, that in lemma 4.1.7 we only used the condition "G is inv. head autoreduced w.r.t. the v-part" for the proof of part c). This will be very important for our following work. Because later, it will turn out that we have to drop this condition as we cannot realize it for every input.

Nevertheless, we will prove as the first result of this master thesis an involutive version of the J-criteria (theorem 3.4.13).

Theorem 4.1.8 ***(involutive J-Criteria (I))***
Let P be the Pommaret division. Let $G \subseteq M$ be a finite set and involutively head autoreduced w.r.t. the v-part. Moreover, assume that we have $\langle Sig(G)\rangle_P = \mathbb{T}_n^m$. Then the statements of lemma 4.1.6 are equivalent, i.e. the statements

a) G is a strong P-basis of M.

b) Every involutive J-pair of elements of G is eventually inv. super reducible by G.

c) Every involutive J-pair of elements of G is inv. covered by G or inv. super reducible by G.

Proof. Due to lemma 4.1.6 we only must show the implication "$c) \Rightarrow a)$". And we are doing this by reductio ad absurdum. For this purpose, suppose that G is not a strong P-basis of M and that c) holds. Then – since G is finite – there is only one way for G not to be a strong P-basis: There must exist a pair $(\mathbf{0}, 0) \neq (\boldsymbol{u}, v) \in M$ which is not inv. reducible by G. We take the one with smallest signature. We set $T \coloneqq \mathrm{lt}(\boldsymbol{u})$ and observe that $T \neq \mathbf{0}$ as otherwise v would be 0, too. Now, as $\langle \mathrm{Sig}(G)\rangle_P = \mathbb{T}_n^m$ is true by our assumptions, we can choose a pair $(\boldsymbol{u}_1, v_1) \in G$ with the following two properties:

(i) $\mathrm{lt}(\boldsymbol{u}_1) \mid_P \mathrm{lt}(\boldsymbol{u})$ and

(ii) $t\mathrm{lt}(v_1) \coloneqq \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_1)}\mathrm{lt}(v_1)$ is minimal under all elements in G that satisfy condition (i).

Note, that $v_1 \neq 0$ as otherwise $(\boldsymbol{u}, v)$ would be inv. reducible by a syzygy $(\boldsymbol{u}_1, 0)$ due to condition (i). Hence, we are in the position to apply part c) of lemma 4.1.7, telling us that $t(\boldsymbol{u}_1, v_1)$ is not inv. regular reducible by G. Next, we set $c \coloneqq \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_1)}$ and

$$(\boldsymbol{u}', v') \coloneqq (\boldsymbol{u}, v) - ct(\boldsymbol{u}_1, v_1).$$

First, we observe that $\mathrm{lt}(\boldsymbol{u}') \prec \mathrm{lt}(\boldsymbol{u}) = T$. For the v-part, there are several cases to consider.

If $\mathrm{lt}(v) \neq t\mathrm{lt}(v_1)$, i.e. $v' \neq 0$, we argue as follows: Because $(\boldsymbol{u}', v')$ has a smaller signature than $(\boldsymbol{u}, v)$ it must be inv. reducible by G. For the moment, we reduce by syzygies if possible. Doing so, we only can reduce the signature, and hence, the remainder is still inv. reducible by G. But now, it is inv. reducible by a pair $(\boldsymbol{u}_2, v_2)$ with $v_2 \neq 0$. Also note that v' has not been changed during the reduction process so far.
Since $\mathrm{lt}(v) \neq t\mathrm{lt}(v_1)$, there are two cases.

- If $\mathrm{lt}(v) \prec t\mathrm{lt}(v_1)$ is true, then we have $\mathrm{lt}(v') = t\mathrm{lt}(v_1)$. Hence, we get the relations

$$\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v') = t\mathrm{lt}(v_1) \quad \text{and} \quad \frac{t\mathrm{lt}(v_1)}{\mathrm{lt}(v_2)}\mathrm{lt}(\boldsymbol{u}_2) \preceq \mathrm{lt}(\boldsymbol{u}') \prec T = t\mathrm{lt}(\boldsymbol{u}_1),$$

  which implies that $t(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by G leading to a contradiction to our result above obtained from lemma 4.1.7 c).

- If, on the other hand, $t\mathrm{lt}(v_1) \prec \mathrm{lt}(v)$ is true, then we get $\mathrm{lt}(v') = \mathrm{lt}(v)$. Therefore we obtain

$$\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v') = \mathrm{lt}(v) \quad \text{and} \quad \frac{\mathrm{lt}(v)}{\mathrm{lt}(v_2)}\mathrm{lt}(\boldsymbol{u}_2) \preceq \mathrm{lt}(\boldsymbol{u}') \prec T = \mathrm{lt}(\boldsymbol{u}),$$

  which now implies that $(\boldsymbol{u}, v)$ is inv. regular reducible by G leading once again to a contradiction since $(\boldsymbol{u}, v)$ is not inv. reducible by G due to our assumptions from the beginning of this proof.

Accordingly, there is only one possibility left, i.e. we have $\mathrm{lt}(v) = t\mathrm{lt}(v_1)$. If $t = 1$ or if $t \neq 1$ is a multiplicative term for $\mathrm{lt}(v_1)$, then $\mathrm{lt}(v_1) \mid_P \mathrm{lt}(v)$, $\mathrm{lt}(\boldsymbol{u}_1) \mid_P \mathrm{lt}(\boldsymbol{u})$ and $\frac{\mathrm{lt}(v)}{\mathrm{lt}(v_1)} = \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_1)} = t$ and hence, $(\boldsymbol{u}, v)$ is inv. reducible by $(\boldsymbol{u}_1, v_1) \in G$. But this is not possible. So $t \neq 1$ has at least one non-multiplicative variable for $\mathrm{lt}(v_1)$. Applying part b) of lemma 4.1.7 we obtain a pair $(\boldsymbol{u}_3, v_3) \in G$ such that $t(\boldsymbol{u}_1, v_1)$ is inv. super reducible by $(\boldsymbol{u}_3, v_3)$. But because of $t\mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u})$ and $t\mathrm{lt}(v_1) = \mathrm{lt}(v)$, this implies that $(\boldsymbol{u}, v)$ is involutive reducible by $(\boldsymbol{u}_3, v_3)$ (*not* necessarily inv. super reducible since we might have $\frac{\mathrm{lc}(v)}{\mathrm{lc}(v_1)} \neq \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_1)}$), which is a contradiction to our choice of $(\boldsymbol{u}, v)$. □

Remark 4.1.9
We shall keep in mind that if we can prove lemma 4.1.7 c) under some other assumptions, the proof of theorem 4.1.8 can stay the same. Also, we shall not forget that all elements in M with smaller signature than $tl(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u})$ would inv. reduce to $(\mathbf{0}, 0)$. Hence, the strong L-basis is finished up to this signature. We will later refer to those two facts.

But for now, we will discuss why we should change our preconditions in the first place, and, that we cannot just discard the condition "G is involutive head autoreduced w.r.t. the v-part".

Let us assume that G is at least involutive regular autoreduced. For a term order satisfying $\boldsymbol{e}_1 \prec \boldsymbol{e}_2$ we discuss the ideal $\langle x^2, x\rangle \trianglelefteq K[x]$. Hence, $G \coloneqq \{(\boldsymbol{e}_1, x^2), (\boldsymbol{e}_2, x)\}$ is indeed involutive regular autoreduced with $\langle \mathrm{Sig}(G)\rangle_P = \mathbb{T}_n^m$. However, there are no involutive J-pairs to consider and the modified version of theorem 4.1.8 would tell us that G is a strong P-basis. This is of course not true since there is

no syzygy contained in G. This shows that we cannot drop our assumptions in theorem 4.1.8 so easily. But it shows simultaneously that there is no involutive reduction changing G into an involutive head autoreduced set w.r.t. the v-part. The only possible reduction would increase the signature and, thus, by definition is not involutive. Therefore, there are some ideals for which we cannot fulfill all needed assumptions in theorem 4.1.8. Moreover, we now know that replacing the condition by "G is involutive regular autoreduced" is not enough.
But fortunately, we will find a way around this problem by allowing *some* necessary, yet "forbidden" reductions. Of course, we want to avoid reductions as much as possible. Thus, we will also aim to obtain some criteria how to decide whether or not a forbidden reduction shall be done. Keep in mind that we want to do only regular reductions if possible, because this way we have control over the signature which is very helpful for applying our J-criteria.
We want to point out that this small example is also a counterexample for the theorem 5 in [1], where the authors left out preconditions for the v-part of G. Furthermore, they have used a weaker criterion in statement c) since there, a J-pair can only be discarded if it is covered (remember that they present the semi-inv. version), whereas we can discard inv. super reducible J-pairs, too.

Now, it is of course useful to have some criteria optimizing the test of the statement c) of theorem 4.1.8. We have already found some of these criteria (e.g. lemma 4.1.1), but there are more to discover. We will find some of them in the next section.

4.2 Involutive J-Criteria (II) for the Pommaret Division

To prepare the next result of this thesis, we will introduce some rather technical lemmas in order to avoid an incomprehensible and long proof. In this section we set $L = P$ to be the Pommaret division, if not noted otherwise. Still, we shall note that some of the lemmas remain valid for arbitrary involutive divisions even though we show it only for $L = P$.

Lemma 4.2.1
If $(\boldsymbol{u}, v) \in M$ is inv. regular reducible by $(\boldsymbol{u}_1, v_1) \in G$ and inv. super reducible by $(\boldsymbol{u}_2, v_2) \in G$ with $v_2 \neq 0$, then there is a multiplicative term t for $\mathrm{lt}(\boldsymbol{u}_2)$ and $\mathrm{lt}(v_2)$ such that $\mathrm{lt}(\boldsymbol{u}) = t\mathrm{lt}(\boldsymbol{u}_2)$, $\mathrm{lt}(v) = t\mathrm{lt}(v_2)$ and $t(\boldsymbol{u}_2, v_2)$ is inv. regular reducible by $(\boldsymbol{u}_1, v_1)$.

Proof. Since $(\boldsymbol{u}, v)$ is inv. super reducible by $(\boldsymbol{u}_2, v_2)$ with $v_2 \neq 0$, it follows that there exists a coefficient $c \in K$, a multiplicative term for $\mathrm{lt}(\boldsymbol{u}_2)$ and $\mathrm{lt}(v_2)$ such

that

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_P \mathrm{lt}(\boldsymbol{u}), \quad \mathrm{lt}(v_2) \mid_P \mathrm{lt}(v) \quad \text{and} \quad \frac{\mathrm{lm}(v)}{\mathrm{lm}(v_2)} = \frac{\mathrm{lm}(\boldsymbol{u})}{\mathrm{lm}(\boldsymbol{u}_2)} = ct.$$

In particular, $t\mathrm{lt}(v_2) = \mathrm{lt}(v)$ and $t\mathrm{lt}(\boldsymbol{u}_2) = \mathrm{lt}(\boldsymbol{u})$. Now, because $(\boldsymbol{u}, v)$ is inv. regular reducible by $(\boldsymbol{u}_1, v_1)$, we get $\mathrm{lt}(v_1) \mid_P \mathrm{lt}(v) = t\mathrm{lt}(v_2)$. Thus, there are two possibilities:

- $\frac{t\mathrm{lt}(v_2)}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) = \frac{\mathrm{lt}(v)}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) \prec \mathrm{lt}(\boldsymbol{u}) = t\mathrm{lt}(\boldsymbol{u}_2)$, and hence, $t(\boldsymbol{u}_2, v_2)$ is inv. regular reducible by $(\boldsymbol{u}_1, v_1)$, or

- $\frac{t\mathrm{lt}(v_2)}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) = \frac{\mathrm{lt}(v)}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u}) = t\mathrm{lt}(\boldsymbol{u}_2)$ and

$$\frac{\mathrm{lc}(v)}{\mathrm{lc}(v_1)} \neq \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_1)}. \tag{4.2.1}$$

  We have to prove now, that $\frac{\mathrm{lc}(v_2)}{\mathrm{lc}(v_1)} \neq \frac{\mathrm{lc}(\boldsymbol{u}_2)}{\mathrm{lc}(\boldsymbol{u}_1)}$ in order to show the claim of the lemma.
  Because $(\boldsymbol{u}, v)$ is inv. super reducible by $(\boldsymbol{u}_2, v_2)$, we obtain

$$\frac{\mathrm{lc}(v)}{\mathrm{lc}(v_2)} = \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_2)}. \tag{4.2.2}$$

  Starting from (4.2.1), we know $\mathrm{lc}(v) \neq \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_1)}\mathrm{lc}(v_1)$. Plugging in (4.2.2), we end up with

$$\frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_2)}\mathrm{lc}(v_2) \neq \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_1)}\mathrm{lc}(v_1)$$

  and hence, with

$$\frac{\mathrm{lc}(v_2)}{\mathrm{lc}(\boldsymbol{u}_2)} \neq \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(\boldsymbol{u}_1)},$$

  which is exactly what we needed to show.

□

Lemma 4.2.2
Let L be an arbitrary involutive division. Let $t \in \mathbb{T}_n$, $(\boldsymbol{u}, v) \in G$ and let $t(\boldsymbol{u}, v) \in M$ be inv. regular reducible by $(\boldsymbol{u}_1, v_1) \in G$. If $\mathrm{lt}(v_1) \mid_{L,B_v} \mathrm{lt}(v)$ then $(\boldsymbol{u}, v)$ is inv. regular reducible by $(\boldsymbol{u}_1, v_1)$.

Proof. We know that $t(\boldsymbol{u}, v)$ is inv. regular reducible by $(\boldsymbol{u}_1, v_1)$. This, by definition,

implies $\mathrm{lt}(v_1) \mid_{L,B_v} t\mathrm{lt}(v)$ and

$$\frac{t\mathrm{lt}(v)}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) \prec t\mathrm{lt}(\boldsymbol{u}) \quad \text{or} \quad \left(\frac{t\mathrm{lt}(v)}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) = t\mathrm{lt}(\boldsymbol{u}) \quad \text{and} \quad \frac{\mathrm{lc}(v)}{\mathrm{lc}(v_1)} \neq \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_1)}\right). \tag{4.2.3}$$

In addition we have $\mathrm{lt}(v_1) \mid_{L,B_v} \mathrm{lt}(v)$. Hence, we can write (4.2.3) without "t" and we are done. □

With this lemma we immediately can prove a first proposition aiming towards the next result of this thesis. It collects some properties about the pair $(\boldsymbol{u}_1, v_1)$ from the proof of theorem 4.1.8, some of which are written down already in lemma 4.1.7. Recall, that $t\mathrm{lt}(\boldsymbol{u}_1)$ was the smallest signature belonging to a pair in M which is not inv. reducible by G. Also, we have discussed that we may assume that G is at least inv. regular autoreduced.

Proposition 4.2.3
Let $G \subseteq M$ be inv. regular autoreduced, $(\boldsymbol{u}_1, v_1) \in G$ and t multiplicative for $(\boldsymbol{u}_1, v_1)$. Let $t(\boldsymbol{u}_1, v_1)$ not be inv. covered by G. Moreover, assume that $(\boldsymbol{u}, v) \in M$ inv. reduces to $(\boldsymbol{0}, 0)$ for all $(\boldsymbol{u}, v)$ with $\mathrm{lt}(\boldsymbol{u}) \prec t\mathrm{lt}(\boldsymbol{u}_1)$.

If $t(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by $(\boldsymbol{u}_2, v_2) \in G$ then $t\mathrm{lt}(v_1) = \mathrm{lt}(v_2)$ and $t \neq 1$.

Proof. Let $t(\boldsymbol{u}_1, v_1)$ be inv. regular reducible by $(\boldsymbol{u}_2, v_2)$. Because G is inv. regular autoreduced, we obtain $t \neq 1$.
Since t is multiplicative for $\mathrm{lt}(v_1)$ this implies $\mathrm{lt}(v_1) \mid_P t\mathrm{lt}(v_1)$ and, as $t(\boldsymbol{u}_1, v_1)$ is inv. regular reducible, $\mathrm{lt}(v_2) \mid_P t\mathrm{lt}(v_1)$. Therefore, $\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v_1)$ or vice versa. In the first case, we can apply lemma 4.2.2 and find that already $(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by $(\boldsymbol{u}_2, v_2)$ contradicting the assumption that G is inv. regular autoreduced.
Accordingly, $\mathrm{lt}(v_1) \mid_P \mathrm{lt}(v_2)$ and $\mathrm{lt}(v_1) \neq \mathrm{lt}(v_2)$ must hold. Then, by definition, there exists a multiplicative term $t' \neq 1$ for $\mathrm{lt}(v_1)$ such that $t'\mathrm{lt}(v_1) = \mathrm{lt}(v_2)$. Because of the fact that t' and t are both multiplicative terms for $\mathrm{lt}(v_1)$ and because of the relation

$$t'\mathrm{lt}(v_1) = \mathrm{lt}(v_2) \mid_P t\mathrm{lt}(v_1),$$

we know that $t' \mid_P t$. We now look at $t'(\boldsymbol{u}_1, v_1)$. Since $t(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by $(\boldsymbol{u}_2, v_2)$ and $\mathrm{lt}(v_2) \mid_P t'\mathrm{lt}(v_1)$, we can apply lemma 4.2.2 once again, returning the statement that $t'(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by $(\boldsymbol{u}_2, v_2)$.

Our aim now is to show, that $t' = t$. Then we have shown everything claimed in the proposition. For that we recall that we already know $t' \mid_P t$ and thus, $t' \preceq t$. So, suppose that we have $t' \prec t$. Then $t'\mathrm{lt}(\boldsymbol{u}_1) \prec t\mathrm{lt}(\boldsymbol{u}_1)$. By our preconditions,

this implies that $t'(\boldsymbol{u}_1, v_1)$ reduces inv. to $(\mathbf{0}, 0)$ by G where at least one reduction is inv. regular. Performing first all inv. regular reductions we see that $t'(\boldsymbol{u}_1, v_1)$ is eventually inv. super reducible by G. From lemma 4.1.5 a) we know that $t'(\boldsymbol{u}_1, v_1)$ is inv. covered by a pair $(\boldsymbol{u}_3, v_3) \in G$. Thus, we have $\mathrm{lt}(\boldsymbol{u}_3) \mid_P t'\mathrm{lt}(\boldsymbol{u}_1)$

$$\frac{t'\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_3)}\mathrm{lt}(v_3) \prec t'\mathrm{lt}(v_1). \tag{4.2.4}$$

Because of $t' \mid_P t$ and t is multiplicative for $\mathrm{lt}(\boldsymbol{u}_1)$ we obtain even $\mathrm{lt}(\boldsymbol{u}_3) \mid_P t\mathrm{lt}(\boldsymbol{u}_1)$. Finally, multiplying $\frac{t}{t'}$ to (4.2.4), we receive the fact that even $t(\boldsymbol{u}_1, v_1)$ is inv. covered by $(\boldsymbol{u}_3, v_3) \in G$, and hence, a direct contradiction to our precondition. □

Now, having these results, we can tackle the main theorem. For that, we have to introduce a certain subset of M. The order of the numbering in the following definition might be not intuitive, however becomes meaningful when we later refer to it.

Definition 4.2.4
Let $G \subseteq M$ be finite and inv. regular autoreduced. Then we define the set $BP(G)$ of *bridging pairs* as follows. For any $(\boldsymbol{u}_2, v_2) \in G$ we check if

(i) there exists a pair $(\boldsymbol{u}_1, v_1) \in G$ such that $\mathrm{lt}(v_1) \mid_P \mathrm{lt}(v_2)$, set $t \coloneqq \frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v_1)}$,

(ii) t is a multiplicative term for $\mathrm{lt}(\boldsymbol{u}_1)$,

(iii) $t(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by $(\boldsymbol{u}_2, v_2)$ and

(iv) $t(\boldsymbol{u}_1, v_1)$ is not inv. covered by G.

If and only if all four conditions are satisfied, the pair $t(\boldsymbol{u}_1, v_1)$ is contained in $BP(G)$. Furthermore, we call a bridging pair with smallest signature an *essential pair* for G.

It may seem to be generic that $BP(G)$ is the empty set because there are many conditions the elements in $BP(G)$ have to satisfy. However, it will turn out, that during the computations, this set most likely is not empty and will play a major role. Nevertheless, our goal will be to obtain a set G at the end of the algorithm, where $BP(G) = \emptyset$ is true.
We want also to mention why this notion of bridging pairs is chosen. But this might be more reasonable when we start to formulate the algorithm. Then, we will see, that they are indeed "bridging" in some meaningful sense.

Now, we begin to show our next result. From our previous work we know that all we have to do is to redo part c) of lemma 4.1.7 under the new conditions which we will introduce in the following proposition.

Proposition 4.2.5
Let P be the Pommaret division. Let $G \subseteq M$ be finite and inv. regular autoreduced. Moreover, assume that $BP(G) = \emptyset$. Furthermore, assume that every J-pair of elements in G is inv. covered or inv. super reducible by G.

Let $(\boldsymbol{u}, v) \in M$ be non-zero and suppose there is a pair $p_1 \coloneqq (\boldsymbol{u}_1, v_1) \in G$ with $v_1 \neq 0$ such that

(i) $\mathrm{lt}(\boldsymbol{u}_1) \mid_P \mathrm{lt}(\boldsymbol{u})$ and

(ii) $t\mathrm{lt}(v_1) \coloneqq \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_1)}\mathrm{lt}(v_1)$ is minimal under all elements in G that satisfy condition (i).

Moreover, assume that $(\boldsymbol{u}', v') \in M$ inv. reduces to $(\boldsymbol{0}, 0)$ for all $(\boldsymbol{u}', v')$ with $\mathrm{lt}(\boldsymbol{u}') \prec t\mathrm{lt}(\boldsymbol{u}_1)$. Then tp_1 is not inv. regular reducible by G.

Proof. Let us suppose that tp_1 is inv. regular reducible by $(\boldsymbol{u}_2, v_2) \in G$. Then, applying lemma 4.1.7 a) we know that tp_1 is not inv. covered by G.

For the moment, suppose that t is a multiplicative term for $\mathrm{lt}(v_1)$. With proposition 4.2.3 we can conclude $t\mathrm{lt}(v_1) = \mathrm{lt}(v_2)$ and $t \neq 1$. Hence, we collect the following properties:

- We have $\mathrm{lt}(v_1) \mid_P \mathrm{lt}(v_2)$ and $t = \frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v_1)}$.
- t is multiplicative for $\mathrm{lt}(\boldsymbol{u}_1)$.
- $t(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by $(\boldsymbol{u}_2, v_2)$ and
- $t(\boldsymbol{u}_1, v_1)$ is not inv. covered by G.

Therefore, $t(\boldsymbol{u}_1, v_1) \in BP(G) = \emptyset$ leads to a contradiction. Also note, that indeed $t(\boldsymbol{u}_1, v_1)$ is an essential pair for G since there cannot be any other pair in $BP(G)$ with smaller signature because of the following arguments: All pairs in $BP(G)$ with smaller signature reduce inv. to zero and there is always at least one reduction inv. regular by definition of $BP(G)$. Hence, the pair is eventually inv. super reducible and at least once inv. regular reducible. Applying lemma 4.1.5 a) we know, that the pair would be inv. covered by G contradicting one condition for being an element in $BP(G)$.
Thus, t is not 1 and contains a non-multiplicative variable for $\mathrm{lt}(v_1)$. With lemma 4.1.7 b) there exists a pair $p' \coloneqq (\boldsymbol{u}', v') \in G$ such that $v' \neq 0$ and $t(\boldsymbol{u}_1, v_1)$ is inv. super reducible by p'. Now, applying lemma 4.2.1, we know that there exists a multiplicative term t' for $\mathrm{lt}(v')$ and $\mathrm{lt}(\boldsymbol{u}')$ such that $t\mathrm{lt}(\boldsymbol{u}_1) = t'\mathrm{lt}(\boldsymbol{u}')$ and $t\mathrm{lt}(v_1) = t'\mathrm{lt}(v')$ and such that $t'(\boldsymbol{u}', v')$ is inv. regular reducible by $(\boldsymbol{u}_2, v_2)$, too. t' cannot be 1, as otherwise G would not be inv. regular autoreduced.

Also, $t'(\boldsymbol{u}', v')$ is not inv. covered by G, because it has the same leading terms as $t(\boldsymbol{u}_1, v_1)$. Therefore, we are in the upper case again and we can apply

proposition 4.2.3 and get analogously $t'(\boldsymbol{u}', v') \in BP(G) = \emptyset$, leading to yet another contradiction. □

Now, the actual inv. J-Criteria becomes a corollary. Nevertheless, we will formulate it.

Theorem 4.2.6 ***(Involutive J-Criteria (II))***
Let P be the Pommaret division. Let $G \subseteq M$ be finite and inv. regular autoreduced. Moreover, assume that we have $\langle Sig(G)\rangle_P = \mathbb{T}_n^m$ and that $BP(G) = \emptyset$. Then the following statements are equivalent:

a) G is a strong P-basis of M.

b) Every involutive J-pair of elements of G is eventually inv. super reducible by G.

c) Every involutive J-pair of elements of G is inv. covered by G or inv. super reducible by G.

Proof. According to lemma 4.1.6 we only have to show "$c) \Rightarrow a$". Remark 4.1.9 tells us that for this purpose we only need to show a modified version of lemma 4.1.7 c) and that proposition 4.2.5 is that modified version. □

4.3 Algorithm: Strong P-Basis

Finally, we are able to formulate an algorithm that is suitable for computing a strong P-basis.
In order to not waste too much time on computations we choose the strategy of smallest signature since by this our set G will not change already treated pairs due to inv. regular autoreductions.
Let $JP(G)$ be the set of all inv. J-pairs of a set G. We start with a set

$$G \coloneqq \{(\boldsymbol{e}_i, f_i) \mid 1 \leq i \leq m\}$$

satisfying the precondition $\langle \mathrm{Sig}(G)\rangle_P = \mathbb{T}_n^m$. Since elements in $JP(G) \cup BP(G)$ cannot be syzygies we can extract them from G and collect them in a set H. Next, we will attack $JP(G)$ and $BP(G)$ simultaneously always searching for the element $p \in JP(G) \cup BP(G)$ with smallest signature. Our goal for $p \in JP(G)$ is to add, if not already existing, a pair p_1 to $G \cup H$ such that p is inv. covered by p_1 or inv. super reducible by it. For this, p_1 is set to be an inv. regular normal form of p. Then p is eventually inv. super reducible by p_1 and by applying lemma 4.1.6 we know, that we can discard p from $JP(G)$.

For $p \in BP(G)$ we always take an essential pair because of the strategy of the smallest signature. And this is exactly what we need to do by our proof of Proposition 4.2.5. Then, we calculate one of its inv. regular normal forms and add it to $G \cup H$. Hence, p is now inv. covered by $G \cup H$ (see lemma 4.1.2) and not contained in $BP(G)$ anymore.
Adding an element to G may extend the set $JP(G) \cup BP(G)$ and thus we are interested in finding criteria to discard as much pairs as possible from these sets. Indeed, we have the following lemma.

Lemma 4.3.1
Let $p \in JP(G) \cup BP(G)$.

a) If p is inv. covered by $JP(G) \cup BP(G)$, or

b) if $p \in JP(G)$ is inv. super reducible by $(JP(G) \cup BP(G)) \setminus \{p\}$, or

c) if $p \in BP(G)$ is inv. super reducible by $BP(G) \setminus \{p\}$, or

d) if p is pseudo reducible by $p' \coloneqq (\boldsymbol{u}', v') \in BP(G) \setminus \{p\}$,

then it can be discarded. In particular, for every G there is an unique essential pair.

Proof. Since all these relations are transitive by lemma 4.1.3, we may assume that p is the only element we have to consider.
ad a): Since we will add an element g to $G \cup H$ such that p is inv. covered or inv. super reducible by g we know by lemma 4.1.5 a) and b) that p will be inv. covered by the new $G \cup H$.
ad b): Let p be inv. super reducible by p'. Then, we will provide a g for $G \cup H$ such that p' is inv. covered or – if $p' \in JP(G)$, inv. covered or inv. super reducible – by the new $G \cup H$. Applying lemma 4.1.5 b), we know that p is inv. covered by the new $G \cup H$ or – if $p' \in JP(G)$, inv. covered or inv. super reducible by it. Hence, it can be discarded.
ad c) and d): We will provide a g for $G \cup H$ such that p' is inv. covered by the new $G \cup H$. Hence, by lemma 4.1.5 we are done.

Now, we want to show, that for any signature occurring in $BP(G)$ there will be only one element left in $BP(G)$ after applying a)-d) to each element one by one. To see this, assume that for a given signature, there are to elements $(\boldsymbol{u}_1, v_1) \neq (\boldsymbol{u}_2, v_2) \in BP(G)$ with $\mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u}_2)$. According to a), we must have $\mathrm{lt}(v_1) = \mathrm{lt}(v_2)$ as otherwise one of the two would be inv. covered by the other. Note, that since both elements are bridging pairs, the v-parts are not zero. Now, applying d), we know that the first pair considered would have been discarded. □

Remark 4.3.2
Because we now know, that the essential pair is unique, its notion may become more transparent. Also, if we look back to the proof of the involutive J-criteria, we worked with the essential pair of G. However, when we look at bridging pairs in general, it turns out that we need them to perform a forbidden reduction step. Every time a regular normal form p has a v-part that is not an inv. normal form, we may enter an element to $BP(G)$ with the same leading term in the v-part as p, and with the property that is now inv. regular reducible. Hence, for an inv. irreducible element p with reducible v-part we have introduced a bridging pair with the same leading term in the v-part, allowing us to continue the reduction with inv. regular reduction steps. Also note, the pair p is not important anymore for our inv. bases in the sense that neither its v-part nor its u-part will appear in it. However, its J-pairs might be necessary – and the same holds for the bridging pairs introduced with the help of p.

By the way, it is easy to see, that by theorem 4.2.6, $G \cup H$ is a strong P-basis for M if $BP(G) = \emptyset$ and every element in $JP(G)$ is inv. covered or inv. super reducible by $G \cup H$. However, since we are aiming to compute two Pommaret bases the proof of termination is not trivial. Based on this issue, one may think of dropping the goal to compute a Pommaret basis for $Syz(F)$. This approach, we will follow in the subsection 4.3.2. But for now, we first prove an important proposition which is the involutive version of proposition 3.4.10.

Proposition 4.3.3
Let $G = \{(\boldsymbol{u}_1, v_1), \ldots, (\boldsymbol{u}_k, v_k)\}$ be a strong P-basis of M. Then

(i) $G_0 \coloneqq \{\boldsymbol{u}_i \mid v_i = 0,\ 1 \leq i \leq k\}$ is a weak Pommaret basis of $Syz(F)$.

(ii) $G_1 \coloneqq \{v_i \mid v_i \neq 0,\ 1 \leq i \leq k\}$ is a weak Pommaret basis of $I = \langle F \rangle$.

Proof. For (i), let $\boldsymbol{u} \in Syz(F) \setminus \{\boldsymbol{0}\}$ be a syzygy. Then $(\boldsymbol{u}, 0) \in M$. As G is a strong P-basis of M, $(\boldsymbol{u}, 0)$ is inv. reducible by some $(\boldsymbol{u}_i, v_i) \in G$. Since a syzygy is only inv. reducible by a syzygy, we obtain $v_i = 0$ which implies $\boldsymbol{u}_i \in G_0$. Moreover, the reduction is inv. super, and hence, $\mathrm{lt}(\boldsymbol{u}_i) \mid_P \mathrm{lt}(\boldsymbol{u})$. But this means that G_0 is a weak Pommaret basis of $Syz(F)$.
For the second part of this proof, we look at $v \in I \setminus \{0\}$. Then, v must be a linear combination of F. Therefore, there exists a $\boldsymbol{u} \coloneqq (u_1, \ldots, u_m) \in R^m \setminus \{\boldsymbol{0}\}$, such that $v = \boldsymbol{u}\boldsymbol{f}^T$. This implies $(\boldsymbol{u}, v) \in M$. Of all possible $\boldsymbol{u}$ we choose the one with minimal $\mathrm{lt}(\boldsymbol{u})$.
Now, as G is a strong P-basis of M, $(\boldsymbol{u}, v)$ is inv. reducible by a pair $(\boldsymbol{u}_i, v_i) \in G$. Let us suppose that $v_i = 0$.
Then we obtain by definition $\mathrm{lt}(\boldsymbol{u}_i) \mid_P \mathrm{lt}(\boldsymbol{u})$. The corresponding inv. super reduction leads to an element $(\boldsymbol{u}', v) \in M$ with $\mathrm{lt}(\boldsymbol{u}') \prec \mathrm{lt}(\boldsymbol{u})$ violating the assumption of

$\mathrm{lt}(\boldsymbol{u})$ being minimal.
So, we must have $0 \neq v_i \in G_1$. But as $(\boldsymbol{u}, v)$ is inv. reducible by $(\boldsymbol{u}_i, v_i)$ and $v_i \neq 0$, this gives us $\mathrm{lt}(v_i) \mid_P \mathrm{lt}(v)$. Accordingly, G_1 is a weak Pommaret basis of I. □

Now, we want to note here that this proposition would provide us with a Gröbner basis of $Syz(F)$ if we were in the semi-involutive case. Indeed, it is enough to compute only a generating system of $Syz(F)$ as we could iterate the algorithm to compute a Pommaret basis of $Syz(F)$ starting with the obtained generating system from the first run. Moreover, if we use a semi-involutive variant of our inv. J-criteria potentially more element will be discarded. This is one of the reasons why we will focus on this variant of the GVW algorithm.
But first, we put together the results from this section in an algorithm presented as a pseudo code for the full involutive case. Before we go into the details, we want to mention that we now restrict to homogeneous ideals as the proof of termination is easier to show. However, one may adopt this theory to the affine case through homogenization and dehomogenization arguments.
Before we present the involutive algorithm, we want to point out one notion. If I is homogeneous, $Syz(F)$ is too in some sense:

All we have to do is to introduce another notion of degrees of a vector term. For a term $x^\mu \in \mathbb{T}_n$ we set $\deg_F(x^\mu \boldsymbol{e}_i) \coloneqq \deg(x^\mu) + \deg(f_i)$. In particular, this means for an $(\boldsymbol{u}, v) \in M$ that $\deg_F(\mathrm{lt}(\boldsymbol{u})) = \deg(\mathrm{lt}(v))$ if $v \neq 0$. Thus, if the v-part is homogeneous, the u-part is too.
Also, we want to note an optimization presented in [7]: If $(\boldsymbol{u}_1, v_1) \neq (\boldsymbol{u}_2, v_2) \in G$ are two different elements in G, then $v_2(\boldsymbol{u}_1, v_1) - v_1(\boldsymbol{u}_2, v_2)$ is a so-called *trivial syzygy* that we can add to the syzygies found so far. However, if we decided to only keep signatures rather than the whole u-part it is important to note, that the signatures of the two pairs may cancel each other out, and thus, we know nothing about the u-part of the syzygy. In such a case, we therefore add nothing to G. Furthermore, when trivial syzygies are used in the algorithm, inv. super autoreductions of the set of syzygies found so far is reasonable. Without them, we can avoid such autoreductions due to our arguments in corollary 3.4.15 as long as we do not have to perform coordinate transformations.

InvGVW$(F, H_0, \prec_1, \prec_2, P, q)$ (Pommart Version)	
Input:	A set $F = \{f_1, \ldots, f_m\} \subseteq R$ of homogeneous polynomials, $\prec_1 = \prec_{\text{degrevlex}}$ on R and a compatible term order $\prec_2$ on R^m of type ω, P Pommaret division, a degree bound q for elements in a Pommaret basis of I. An autoreduced set H_0 of syzygies of F, where $H_0 = \emptyset$ is possible.
Output:	A weak Pommaret basis for $I = \langle F \rangle$, that also contains a Pommaret basis as a subset; and a weak Pommaret basis of $Syz(F)$ or an error message that I or $Syz(F)$ is not quasi-stable.
Variables:	G is an ordered set of pairs $(\boldsymbol{u}_i, v_i) \in M$ with $v_i \neq 0$. H is an ordered set of syzygies $(\boldsymbol{u}, 0)$ of F. $JP(G)$ is the set of involutive J-pairs of G. $BP(G)$ is the set of bridging pairs of G.
Step 1:	$G \leftarrow \{(\boldsymbol{e}_i, f_i) \mid 1 \leq i \leq m\}$, $H \leftarrow H_0$, $BP(G) \leftarrow \emptyset$
Step 2:	Perform an inv. regular autoreduction on G. Fill H with obtained syzygies, discard them from G, and fill $BP(G)$ with (new) bridging pairs. Calculate (new) trivial syzygies of G and add them to H. Inv. autoreduce H. Fill $JP(G)$ with (new) inv. J-pairs of G. Remove all elements from $JP(G) \cup BG(G) =: Q$ for which the degree of the v-part is greater than $q + 2$.
Step 3:	**while** $JP(G) \cup BP(G) \neq \emptyset$ **do**
Step 4:	Take elements $p := (\boldsymbol{u}, v) \in JP(G) \cup BP(G) =: Q$ with smallest signature and then with smallest leading term in the v-part. Do the following step for all choices of p
Step 5:	If • p is inv. covered by $G \cup H \cup Q =: S$, or • p is pseudo reducible by $BP(G) \setminus \{p\}$, or • $p \in BP(G)$ is inv. super reducible by $BP(G) \setminus \{p\}$, or • $p \in JP(G)$ is inv. super reducible by $S \setminus \{p\}$, then discard p and go back to step 3.
Step 6:	If there is more than one choice for p left, and one of them is from $BP(G)$, take it and discard the rest. If all are in $JP(G)$ perform an inv. regular reduction step from one of them by another one, replace p by the result of the reduction step and discard all other choices of p.
Step 7:	Calculate an inv. regular normal form $(\boldsymbol{u}', v')$ of p by G
Step 8:	**If** $v' = 0$ **then**
Step 9:	**If** $\min\left\{\deg_F(\mathrm{lt}(\boldsymbol{u}')), \min\limits_{(\boldsymbol{u},v)\in Q}\{\deg_F(\mathrm{lt}(\boldsymbol{u}))\}\right\} > q + 1$ **then**
Step 10:	**return** "$Syz(F)$ is not quasi-stable"
Step 11:	**endif**
Step 12:	$H \leftarrow H \cup \{(\boldsymbol{u}', 0)\}$
Step 13:	**else**
Step 14:	**If** $\mathrm{lt}(v')$ is not inv. reducible by the v-part of G and $\min\left\{\deg(\mathrm{lt}(v')), \min\limits_{(\boldsymbol{u},v)\in Q}\{\deg(\mathrm{lt}(v))\}\right\} > q$ **then**
Step 15:	**return** "I is not quasi-stable"
Step 16:	**endif**
Step 17:	$G \leftarrow G \cup \{(\boldsymbol{u}', v')\}$. Go back to step 2.
Step 18:	**end if**
Step 19:	**end while**
Return:	$\{v_i \mid (\boldsymbol{u}_i, v_i) \in G\}$ and $\{\boldsymbol{u} \mid (\boldsymbol{u}, 0) \in H\}$

4.3.1 Correctness of the GVW algorithm

After presenting the main algorithm, we have to consider of course that we aim to calculate a Pommaret basis which does not exist in general. Schweinfurter et al. have shown in [10], however, that with the help of coordinate transformations, the standard algorithm [16, Algo. 4.5] will terminate for computing a Pommaret basis of an homogeneous ideal and for the degree reverse lexicographic order. But there are many different ways how to decide if a coordinate transformation is needed and if so, which would fit the best (see [16, Prop. 5.3.4],[10, Prop. 3.2]). We will tackle this question later. But for now, we want to prove, that our core algorithm is correct, if it terminates. For the termination with Pommaret bases as the only possible output we will of course have to add some steps with transformations.

Remark 4.3.4
We want to note one property of the involutive GVW algorithm, that follows from the strategy of smallest signatures and the definition of inv. reduction on M: Let us have added $(\boldsymbol{u}, v)$ to $G \cup H$ at some point in the algorithm. As inv. reduction steps are not allowed to increase the signature, and as we build up our strong P-basis from smallest signatures, we know for sure that the strong P-basis is finished up to elements with strictly smaller signature than $\mathrm{lt}(\boldsymbol{u})$[2]. Moreover, if we take a degree compatible term order for the u-part, we can conclude: If $\deg(\mathrm{lt}(\boldsymbol{u})) = k+1$ for some $k \in \mathbb{N}$, we know that we have a *strong P-basis up to the degree* k, i.e. a set $G \cup H$ such that every element in M with a signature of degree less than or equal to k inv. reduces to $(\mathbf{0}, 0)$ by $G \cup H$[3]. But as every Pommaret basis of an homogeneous ideal I has elements with a degree of at most q, and $q+1$ for $Syz(F)$, respectively [16, Cor. 5.5.18], all we need to do is to build a strong P-basis up to the degree $q+1$. If I or $Syz(F)$ are not quasi-stable, we then will find also elements of degree $q+2$ that will increase the involutive span of I or $Syz(F)$ [16, Prop. 5.3.7]. Thus, a first step towards the proof of correctness is to show that the algorithm will produce elements of ascending signature.

Indeed, we will prove that after we have enlarged G by an element $(\boldsymbol{u}, v)$, all new elements that are about to be added to $JP(G) \cup BP(G)$ have a signature greater than $\mathrm{lt}(\boldsymbol{u})$. Indeed, we could show in the next lemma that there are no two elements in $G \cup H$ with same signature, if we follow the algorithm described so far. But since we must allow coordinate transformations this may not be the case anymore after a transformation.

[2]Here, we do not want to discuss if it is even finished up to elements with signature $\mathrm{lt}(\boldsymbol{u})$.
[3]Remember that we are only interested in a strong P-basis for $\prec_1 = \prec_{\mathrm{degrevlex}}$.

Lemma 4.3.5
At some point in the inv. GVW algorithm, consider $p \coloneqq (\boldsymbol{u}, v) \in JP(G) \cup BP(G)$. If we have just entered an inv. regular normal form $p' \coloneqq (\boldsymbol{u}', v')$ of p to $G \cup H$, then after a finite number of loop iterations, we will consider a pair with a signature that is strictly greater than $\mathrm{lt}(\boldsymbol{u}')$.

Proof. At the moment of entering p' to $G \cup H$, there are finitely many elements in $JP(G) \cup BP(G)$ with same signature. Because of step 6, all those elements in $JP(G) \cup BP(G)$ are now inv. covered by the inv. regular autoreduced G or H, and hence can be discarded. Thus, all elements left in $JP(G) \cup BP(G)$ have a greater signature than p'. Therefore, we may assume that the next element we consider has not entered $JP(G) \cup BP(G)$, yet.
Now, if p' is a syzygy, we do not enlarge $JP(G) \cup BP(G)$. If p' is no syzygy, then we perform an inv. regular autoreduction, only changing elements in G with greater or equal signature than p' has. Thus, all new J-pairs that are added to $JP(G)$ have a signature greater than the one from p'. Also, we claim that elements added to $BP(G)$ have a strictly larger signature than p' has. To see this, we consider two cases.

Firstly, assume that v' is not an inv. normal form, i.e. there exists $(\boldsymbol{u}_1, v_1) \in G$ such that $\mathrm{lt}(v_1) \mid_P \mathrm{lt}(v')$ and $\frac{\mathrm{lt}(v')}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) \succeq \mathrm{lt}(\boldsymbol{u}')$ as otherwise G would not be inv. regular autoreduced. Suppose, that $\frac{\mathrm{lt}(v')}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u}')$. So, if we enter $g \coloneqq \frac{\mathrm{lt}(v')}{\mathrm{lt}(v_1)}(\boldsymbol{u}_1, v_1)$ to $BP(G)$, then g is inv. regular reducible by p'. Thus, we must have $\frac{\mathrm{lc}(v')}{\mathrm{lc}(v_1)} \neq \frac{\mathrm{lc}(\boldsymbol{u}')}{\mathrm{lt}(\boldsymbol{u}_1)}$. However, then we know that the reduction $(\boldsymbol{u}', v') - \frac{\mathrm{lm}(v')}{\mathrm{lm}(v_1)}(\boldsymbol{u}_1, v_1)$ is inv. regular, too, and thus, G not inv. regular autoreduced. Hence, we have $\frac{\mathrm{lt}(v')}{\mathrm{lt}(v_1)}\mathrm{lt}(\boldsymbol{u}_1) \succ \mathrm{lt}(\boldsymbol{u}')$.

Secondly, assume that there is a pair $(\boldsymbol{u}_2, v_2) \in G$ such that $\mathrm{lt}(v') \mid_P \mathrm{lt}(v_2)$ and $\frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v')}\mathrm{lt}(\boldsymbol{u}') \succeq \mathrm{lt}(\boldsymbol{u}_2)$. Our candidate for $BP(G)$ is $h \coloneqq \frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v')}(\boldsymbol{u}', v')$. So, what we have to show is $\mathrm{lt}(v_2) \neq \mathrm{lt}(v')$. For this, suppose it is not true, i.e. we have $\mathrm{lt}(v_2) = \mathrm{lt}(v')$.
Therefore, we have in total $\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v')$, and from $\frac{\mathrm{lt}(v_2)}{\mathrm{lt}(v')}\mathrm{lt}(\boldsymbol{u}') \succeq \mathrm{lt}(\boldsymbol{u}_2)$ we obtain $\mathrm{lt}(\boldsymbol{u}') \succeq \frac{\mathrm{lt}(v')}{\mathrm{lt}(v_2)}\mathrm{lt}(\boldsymbol{u}_2)$. Now, if especially $\mathrm{lt}(\boldsymbol{u}') \succ \frac{\mathrm{lt}(v')}{\mathrm{lt}(v_2)}\mathrm{lt}(\boldsymbol{u}_2)$ holds, then $(\boldsymbol{u}', v')$ is inv. regular reducible by $(\boldsymbol{u}_2, v_2)$ leading to a contradiction. Therefore, we have $\mathrm{lt}(\boldsymbol{u}') = \frac{\mathrm{lt}(v')}{\mathrm{lt}(v_2)}\mathrm{lt}(\boldsymbol{u}_2) = \mathrm{lt}(\boldsymbol{u}_2)$. However, the reduction is still inv. regular, if $\frac{\mathrm{lc}(v')}{\mathrm{lc}(v_2)} \neq \frac{\mathrm{lc}(\boldsymbol{u}')}{\mathrm{lc}(\boldsymbol{u}_2)}$. So, the quotients must be equal, too. But then the reduction

$$\frac{\mathrm{lm}(v_2)}{\mathrm{lm}(v')}(\boldsymbol{u}', v') - \frac{\mathrm{lc}(v')}{\mathrm{lc}(v')}(\boldsymbol{u}_2, v_2)$$

cannot be inv. regular, which is a contradiction to the fact that h is indeed inv.

regular reducible by $(\boldsymbol{u}_2, v_2)$ (as we assumed $h \in BP(G)$).

Finally, these two cases let us conclude that since every other element in the inv. regular autoreduced set G, who can lead to new elements in $BP(G)$, have at least the same signature as p', every new element in $BP(G)$ has a greater signature than the one of p'. □

Theorem 4.3.6
Let P be the Pommaret division, $\prec_1 = \prec_{degrevlex}$ and $\prec_2$ a compatible term order of type ω. If the inv. GVW algorithm terminates, it is correct.

Proof. Step 1 guarantees $\langle \mathrm{Sig}(G) \rangle_P = \mathbb{T}_n^m$ at the end as we are not removing any of the start elements from G, and only are able to reduce them inv. regular. Since we are performing an inv. regular autoreduction after every step we have added an element to G (step 2, step 17), our G is inv. regular autoreduced. Now, if the algorithm terminates, we first dicuss the case that $JP(G) = BP(G) = \emptyset$ is true without having removed elements $(\boldsymbol{u}, v)$ with $(\deg_F(\mathrm{lt}(\boldsymbol{u})) =) \deg(\mathrm{lt}(v)) > q + 2$. In the context of the algorithm, this means, that every J-pair of an element in G has been studied in step 5 or 6. Lemma 4.3.1 tells us, that every element in $JP(G)$ removed in step 5 is now inv. covered or inv. super reducible by $G \cup H$. Also, the lemma says that every element removed from $BP(G)$ will be inv. covered by the new $G \cup H$ and hence not be a bridging element anymore. However, we have to argue about step 6 a bit. First, assume that one of the candidates is from $BP(G)$. Then, it will be inv. regular reducible by G and an inv. regular normal form will be added to $G \cup H$. Hence, it will be inv. covered by it and so every other candidate. Now, assume that all candidates are from $JP(G)$. As they have passed step 5, every single one of them must be inv. regular reducible by the any other choice of p. We perform one of the regular reductions. Now, as the obtained pair will be inv. covered or inv. super reducible by the new $G \cup H$, all the candidates for p will be – according to lemma 4.1.2 – inv. covered by the new $G \cup H$. Hence, we end up with a set $G \cup H$ for which $BP(G) = \emptyset$ and every element in $JP(G)$ is inv. covered or inv. super reducible by $G \cup H$. Applying the inv. J-criteria (II), we are done with this part.

Next, we discuss if $Q = \emptyset$ is only the case because all elements that should be contained in Q have a degree in the v-part that is greater than $q + 2$ and therefore have been removed by step 2. Because we have come so far in the algorithm without getting an error message, every element $(\boldsymbol{u}, v)$ with $\deg_F(\mathrm{lt}(\boldsymbol{u})) = \deg(\mathrm{lt}(v)) \leq q+1$ has been considered. So, if no error message stopped the algorithm (as it must be true for this case) I and $Syz(F)$ both are quasi-stable, as the Pommaret bases do not contain elements with a greater degree than $q + 1$ by our thoughts in remark 4.3.4. Hence, the algorithm has provided us a strong P-basis up to the degree $q + 1$. And according to our observations in remark 4.3.4 the output is correct.

If we get the error message that $Syz(F)$ is not quasi-stable this means that we have added a syzygy $(\boldsymbol{u}', 0)$ to H. In particular, the syzygy is not involutive reducible by H as otherwise p would have been inv. covered by H in step 5. So, we have extended the involutive cone of $\mathrm{lt}(H)$. But every Pommaret basis of $Syz(F)$ must consist of elements with $\deg_F(\mathrm{lt}(\boldsymbol{u}')) \leq q+1$ as we have seen above. Because of the strategy of smallest signature, $\mathrm{lt}(\boldsymbol{u}')$ will still be inv. irreducible by any H that we compute during the algorithm as $\mathrm{lt}(\boldsymbol{u}') \prec \mathrm{lt}(\boldsymbol{u})$ for all $\boldsymbol{u} \in H$ that were added after $\boldsymbol{u}'$[4]. Because the signatures of considered pairs are ascending by lemma 4.3.5 and there are only finitely many missing for a strong P-basis up to the degree $q+1$ (we have a term order of type ω), $Syz(F)$ cannot be quasi-stable[5] and the error message is legit.
For the last case, we assume that the algorithm finished with an error message for I. Here, we have similar arguments as for $Syz(F)$. We must have added an element of degree greater than q in the v-part which only can add elements to Q with at least degree $q+1$ in the v-part. However, all elements that are interesting for a Pommaret basis of I are from degree less than $q+1$ (and elements of degree $q+1$ must inv. reduce[6] to zero by a Pommaret basis). However, as our algorithm has computed a strong P-basis up to the degree of the current signature (i.e. the one corresponding to v'), we have already a (weak) Pommaret basis of I computed as all other v-parts have a degree of $q+1$ or greater due to the last component of the if-statement in step 14. Still, we have added an element to G with $\deg(\mathrm{lt}(v')) > q$ which is not inv. reducible by the v-parts of G. Hence, there cannot exist a Pommaret basis of I and the corresponding error message is correct. □

Next, we introduce a notion to connect the GVW algorithm to the standard-algorithm [16, Algo. 4.5].

Definition 4.3.7
Let $G \subseteq M$ be inv. regular autoreduced. Let $p_i \coloneqq (\boldsymbol{u}_i, v_i) \in G$ for $i = 1, 2$. Let $\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v_1)$ and $t \coloneqq \frac{\mathrm{lt}(v_1)}{\mathrm{lt}(v_2)}$. If $tp_2 \in BP(G)$ then we call tp_2 the *proxy* of p_1.

Corollary 4.3.8
Let $\prec_1 = \prec_{\mathrm{degrevlex}}$ be a term order on R and $\prec_2$ a compatible term order on R^m of type ω. Then for every $p \in G$ that has been considered already, the proxy is considered after finitely many steps, too.

Proof. As by lemma 4.3.5, after a finite number of steps, we look at an element with strictly larger signature, and as $\prec_2$ is of type ω, the proxy of p is considered

[4] We can use the same arguments as for the proof of corollary 3.4.15.
[5] Otherwise the algorithm would have computed $Syz(F)$ and $\mathrm{lt}(\boldsymbol{u}')$ could not be inv. irreducible by $Syz(F)$.
[6] Here, we mean the common notion of inv. reducibility without any restrictions by a u-part.

after a finite number of steps. □

Remark 4.3.9
We want to mention that from this corollary one cannot imply immediately that we are computing an inv. normal form of all considered v-parts. Because during the process of the reductions it may be the case that a pair does not possess a proxy because, in the notion of definition 4.3.7, $tp_2 \notin BG(G)$. In such a case, we would stop the reductions. Still, this would mean that the proxy would inv. reduce to $(\mathbf{0}, 0)$ by the final G.

Now the next lemma is the most important one to prove the termination of the semi-involutive case. Still, we will formulate the full involutive variant. Indeed, everything we have discussed would only differ in the division on the u-part. Moreover, if we substitute "$|_{L,B_u}$" by "$|$", one can go through all the proofs and verify that they will stay the same if not become shorter. In fact, some of the proofs get easier as we do not need all of the arguments we needed for justifying why we can write "$|_{P,B_u}$". Nevertheless, as we have introduced the notions for the full involutive case, it is more convenient to present the following lemma also with the same notions.

Lemma 4.3.10
Let $p_i \coloneqq (\boldsymbol{u}_i, v_i)$ be the i-th element that entered $G \cup H$ in step 12 or 17. Then, we have $p_i \nmid_P p_j$ for $i < j$.

Proof. Suppose for $i < j$ we have $p_i \mid_P p_j$, i.e. $\mathrm{lt}(\boldsymbol{u}_i) \mid_P \mathrm{lt}(\boldsymbol{u}_j)$ and $\mathrm{lt}(v_i) \mid_P \mathrm{lt}(v_j)$. Therefore, there exist terms t_1, t_2 such that

$$\mathrm{lt}(v_j) = t_1 lt(v_i) \quad \text{and} \quad \mathrm{lt}(\boldsymbol{u}_j) = t_2 lt(\boldsymbol{u}_i).$$

If $t_1 \prec t_2$, then $t_1 lt(\boldsymbol{u}_i) \prec t_2 lt(\boldsymbol{u}_i) = \mathrm{lt}(\boldsymbol{u}_j)$. Hence, p_j is inv. regular reducible by p_i leading to a contradiction since p_j is an inv. regular normal form.
Thus, $t_2 \preceq t_1$. This implies $t_2 lt(v_i) \preceq t_1 lt(v_i) = \mathrm{lt}(v_j)$. Now, suppose that p_j is an inv. regular normal form of $p \coloneqq (\boldsymbol{u}, v) \in JP(G) \cup BP(G)$. If p was at least once inv. regular reducible, then $\mathrm{lt}(v_j) \prec \mathrm{lt}(v)$ and hence,

$$\mathrm{lt}(\boldsymbol{u}_i) \mid_P \mathrm{lt}(\boldsymbol{u}_j) = \mathrm{lt}(\boldsymbol{u}) \quad \text{and} \quad \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_i)} \mathrm{lt}(v_i) = t_2 lt(v_i) \preceq \mathrm{lt}(v_j) \prec \mathrm{lt}(v).$$

But this means that p should have been discarded in step 5 as it is inv. covered by p_i. Thus, p is not inv. regular reducible, and in particular not an element of $BP(G)$. Therefore, $p \in JP(G)$ cannot be inv. super reducible either, because otherwise it would have been discarded and p_j would not have been calculated. So, we know that p is inv. irreducible, and hence, $p = p_j$.

We are in the case $t_2 \preceq t_1$. Suppose, we have $t_2 \prec t_1$. Then, $t_2 lt(v_i) \prec \mathrm{lt}(v_j) = \mathrm{lt}(v)$ and $t_2 lt(\boldsymbol{u}_i) = \mathrm{lt}(\boldsymbol{u}_j) = \mathrm{lt}(\boldsymbol{u})$. This would mean that p would be inv. covered by $p_i \in G$ and not be entering G in the first place. Accordingly, we have $t_2 = t_1$. But then, p is inv. reducible by p_i contradicting the observation that p is inv. irreducible by G. □

Lastly, we want to present a proof for the termination. For the full involutive case, we can easily argue as we will find out in the next proposition.

Proposition 4.3.11
Let P be the Pommaret division, $\prec_1 = \prec_{\mathrm{degrevlex}}$ and $\prec_2$ a compatible term order of type ω. Then the full involutive GVW algorithm terminates.

Proof. As we can discard all elements of degree greater than $q+2$, there are only finitely many terms left to consider since $T_{\leq q+2} \coloneqq \{t \in \mathbb{T}_n \mid \deg(t) \leq q+2\}$ is a finite dimensional subvector space of R. As the signature is strictly increasing after finitely many pairs that we have to consider (lemma 4.3.5), we cannot look at the same pair infinitely many times. Thus, as we have term orders of type ω, the algorithm will terminate. □

We want to note here that once again; this proof is only that short because we are in the homogeneous case where have an a priori knowledge about the degree of an inv. regular normal form. In the general case, lemma 4.3.10 might be useful. Moreover, as a last remark, we want to point out the following result.

Remark 4.3.12
Because the proxy is considered after finitely many steps by corollary 4.3.7, we indeed compute all necessary inv. normal forms of v-parts: The proxy is defined in such a way that the reduction steps in the v-part can continue, but instead of reducing v_1 by v_2 (assuming that $\mathrm{lt}(v_2) \mid_P \mathrm{lt}(v_1)$), we reduce tv_2 by v_1, where $t = \frac{\mathrm{lt}(v_1)}{\mathrm{lt}(v_2)}$. Nevertheless, the result of the reduction step is the same up to a constant factor. Thus, if the proxy survives step 5 of the algorithm, we go one step further towards an inv. normal form of v_1. However, the algorithm will keep $(\boldsymbol{u}_1, v_1)$ in $G \cup H$, although the v-part is inv. reducible, and hence, v_1 will be not part of a strong Pommaret basis of I. Still, after the algorithm has returned his output, such elements are fairly easy to detect. We only have to look, if the v-part is inv. reducible. Then we know, that his proxy (if it exists) will be considered. Thus, we can just discard v_1 from the output and we will obtain a strong Pommaret basis of I.

4.3.2 Semi-involutive GVW algorithm

At this stage, we are able to prove termination for the semi-involutive case. One can verify all the results we have achieved so far also hold for the semi-involutive case. However, this might not trivially be the case since we do not only have weaker statements but also weaker assumptions. Still, all of the proofs can be just rewritten, only changing the involutive division in the u-part to the common one. In some contexts, one can even leave out arguments that were only necessary for the full involutive case.

Therefore, we must drop the lines 9-11 from the pseudo code because we will no longer have a bound for elements in an involutive bases of $Syz(F)$. Thus, we cannot decide which elements we can neglect from Q. Still, the proof of correctness therefore becomes shorter as we neither have to discuss the case of an error message due to $Syz(F)$, nor the case that $Q = \emptyset$ because we have removed elements from Q by step 2. But this also means that the proof for termination will be more difficult because we cannot argue with finitely many elements that are left to be discussed. On the other hand, we can take in now "Noetherian" arguments. For the corresponding algorithm (dropping lines 9-11 and using the common division on the u-part), we will not be able to prove the termination in this thesis. Instead, we will focus on computing a Pommaret basis of I. For this, we only have to keep the signatures as they are sufficient for applying the J-criteria. However, this should only be done for ideals in quasi-stable position because we cannot gain any information about the transformed syzygies when we only keep the signatures. Thus, if the need of coordinate transformations is not excluded one should still carry the whole u-part.
As we have a degree bound for the v-parts, we can now neglect all elements in Q with a degree greater than $q + 1$. Note, that this implies, that we may have not found all (leading terms of) syzygies of the Gröbner basis of $Syz(F)$, when we interrupt the algorithm at this degree bound. Nevertheless, this is not a problem for our case where we start with the Janet version of the GVW algorithm[7]. This algorithm will provide us a Gröbner basis of $Syz(F)$. So, this weakness of the semi-inv. Pommaret version may only play a role, if one wants to use it without the Janet version.
Now, our semi-inv. algorithm for the Pommaret division arises as follows from the full involutive version:

- Only keep signatures rather than the whole u-part.
- Use the common division for the u-parts.
- Drop lines 9-11.

[7] We will introduce it in section 4.4.

- Return a weak Pommaret basis of I, and syzygies/signatures of syzygies.

Theorem 4.3.13
Let P be the Pommaret division, $\prec_1 = \prec_{degrevlex}$ and $\prec_2$ a compatible term order of type ω. Then the semi-involutive GVW algorithm terminates.

Proof. We prove that the algorithm terminates independently from our choice of using only signatures. So, we assume for this proof that we keep the whole u-part. Suppose that the algorithm does not terminate. Then we obtain in the notion of lemma 4.3.10

$$\begin{aligned} \langle \boldsymbol{u}_1 \rangle &\subseteq \langle \boldsymbol{u}_1, \boldsymbol{u}_2 \rangle \ \subseteq \dots \\ \langle v_1 \rangle_P &\subseteq \langle v_1, v_2 \rangle_P \ \subseteq \dots, \end{aligned}$$

where $p_i \coloneqq (\boldsymbol{u}_i, v_i)$ and at least one "$\subseteq$" at same height is a "$\subsetneq$". As the upper chain must become stationary, the chain of the v-parts must be strictly ascending at some point.
Now assume, that a finite Pommaret basis exists. As the signatures are increasing by lemma 4.3.5 and we have there a term order of type ω, too, we need only finitely many iterations to get beyond the degree $q+1$ in the v-part. Hence, the algorithm has computed a weak Pommaret basis according to remark 4.3.4. Thus, after interrupting the algorithm, our input will be a weak Pommaret basis.
On the other side, if I is not quasi-stable, by [16, Prop. 5.3.7] there must exist an element which has a degree greater than $q+1$ and yet increase the involutive cone of the current $\mathrm{lt}(G)$. This will still be the case after we have considered all elements in V with degree less than $q+1$. Thus, our algorithm will terminate with an error message that I is not quasi-stable. □

Before we discuss the case where we need coordinate transformations we want to give a last remark.

Remark 4.3.14
As the p_i stand for elements that are added to $G \cup H$, we cannot argue, that the lower chain must become stationary in the case that a Pommaret basis exists. On the other hand, all syzygies we find, will be encoded in some $\boldsymbol{u}_j$. But still, we would not be able to argue for the full involutive case that the upper chain must become stationary as not all $\boldsymbol{u}_i$ refer to a syzygy. In fact, we have no good argument for the termination of the full involutive algorithm at this point if we would not neglect all elements from Q with a degree greater than $q+2$, because we have no better argument, yet, that both chains must become stationary besides cutting them off at the degree bound. Thus, this proof is only valid for the semi-inv. case where we only focus on the v-part.

4.3.3 Coordinate Transformations and Index of Safety

Now, we are ready to show a version of the inv. GVW algorithm with coordinate transformations. We will only discuss here the full involutive algorithm, as it is more complex because we have to put $Syz(F)$ in quasi-stable position, too.
From private communication with Matthias Orth it is known that we can transform a not quasi-stable I and $Syz(F)$ step by step simultaneously into quasi-stable position. In general, we then have to restart the algorithm after each step. However, as syzygies will transform into syzygies, we can use them for our J-criteria. Hence, the strength of the inv. GVW algorithm now becomes clear. So, many of the J-pairs might be inv. covered. Also, the set of bridging pairs might not be as big as it would be without the syzygies that we obtained from the transformation of the old syzygies. Thus, we should also work on the problem, where we need to start over after a transformation. In particular, we will introduce an *index of safety* in this chapter.

Remark 4.3.15
Basically, we are using the inv. GVW algorithm trying to compute a Pommaret basis of I and $Syz(F)$. For this, we first calculate a Janet basis of I, obtaining a degree bound q for elements in a Pommaret basis of I (see [16, Cor. 5.5.18]). In fact, we can take the inv. GVW algorithm for the Janet division which we will present in the next section. If the Janet basis is also a Pommaret basis, we are done with I. So let's assume, that it is not a Pommaret basis. Then, because we only increase the leading term of the v-parts via $JP(G)$, we check which inv. J-pairs $x_k p \in JP(G)$ are not inv. reducible by $G \cup H$ and satisfy $\deg(\mathrm{lt}(x_k v)) > q$ or $\deg_F(\mathrm{lt}(x_k \boldsymbol{u})) > q + 1$. If so, we need to perform a coordinate transformation on the u- or v-part. Let us discuss here the v-part, the u-part works similar[8]. Let $j = cls(\mathrm{lt}(v))$. Then we transform by $x_j \mapsto x_j + x_k$. However, this forces us to start our calculations all over again. Also, we may ask ourselves, if we need to perform the transformation directly after finding such an inv. J-pair, or if we can push it back a little until we cannot do anything else but to transform the system. In fact, our algorithm does exactly this: According to steps 9 and 14, we return an error message if and only if I or $Syz(F)$ are not quasi-stable[9]. But in such a case, we perhaps can choose between several coordinate transformations after analyzing Q. So, we have to face the question which of the possible transformations is the best in the context of computational efficiency. Nevertheless, we have to discuss what

[8] Also, we will discuss later in this remark how do deal with an error message for $Syz(F)$ coming from the Pommaret version of the algorithm.
[9] For the argument corresponding to $Syz(F)$, one may look up the arguments in the proof of correctness of the (full) inv. GVW algorithm.

happens after the transformation. There, we just transform F and all syzygies with a suitable coordinate transformation. Then we take it as an input for the Pommaret version of the GVW algorithm. Here of course, one is not forced to take the full involutive variant, however, we will argue our strategy only for the full involutive algorithms. The ideas can easily be adapted for the semi-inv. algorithms. In particular, this means for the pseudo code the following:

Instead of returning an error message for I in step 15, we go through the elements in Q and check if their v-part is divisible by the v-part of a $p = (\boldsymbol{u}, v) \in G$, but involutively irreducible by G. If this is the case, we choose the p with maximal $\mathrm{cls}(\mathrm{lt}(v))$. Then every J-pair of p leads to a candidate for a coordinate transformation as we have described above.
If, on the other hand, an error message for $Syz(F)$ has been returned in step 10, then we go through the signatures of Q and check if they are divisible by some $p' = (\boldsymbol{u}', v') \in G \cup H$, but not inv. reducible by the signatures of all elements in $G \cup H$. Then we take under all p' satisfying this condition the one with maximal $j \coloneqq \mathrm{cls}(\mathrm{lt}(\boldsymbol{u}'))$. For this signature, we have non-multiplicative variables x_k. Therefore, potential coordinate transformations are of the form $x_j \mapsto x_j + x_k$. After gathering all possible coordinate transformations ψ_i, we do the following:

1. Transform $G \cup H$ with ψ_i into $G' \cup H'$.
2. Perform an inv. regular autoreduction of G' and insert obtained syzygies into H'.
3. Compute $Q' \coloneqq JP(G') \cup BG(G')$ for the inv. regular autoreduced G' and sort it first by signature, then by the leading terms of the v-part.
4. Search the position s of the first element in the sorted Q' that cannot be discarded due to our criteria in step 5.

In 4., s is of course dependent of ψ_i, i.e. we better write $s(\psi_i)$. The largest value of $s(\psi_i)$ is called *index of safety*. It is so to speak the latest possible starting point of the algorithm after a coordinate transformation. After we have found the index of safety, we can continue the involutive GVW algorithm at step 7, taking the element in Q' at the position $\max_i \{s(\psi_i)\}$ and neglect all elements from Q' with smaller signature.

Although this strategy is straight forward to see, it might not be the best if it comes to an efficient implementation. For such one, a bigger analysis is needed. For instance, if only a few elements would not be discarded after a coordinate transformation and by accident, there is one with small signature (so the index of safety is small), one could try to analyze when the corresponding transformation is still a better choice then the one related to the index of safety. However, this might be a difficult question to answer.

Remark 4.3.16
It is easy to see that a POT-lift is not of type ω. However, as we have a degree bound for $Syz(F)$ in the full inv. variant as well, we also can use a POT-lift of a term order $\prec_1$ of type ω with the following restriction: We just jump to $\boldsymbol{e}_{i+1}$ if the signature at position i exceeds the degree $q+1$. Then we know, that no element at position i is of interest for our Pommaret bases, and thus can be pushed back for the moment. Thereby, we ensure that between two terms, there are only finitely many other pairs that the algorithm will consider. Whenever we say, we choose a *POT-lift of pseudo type* ω we mean to follow this strategy. It is worth mentioning that our algorithm follows this strategy for a POT-lift input as all elements above the degree $q+2$ are neglected and an error message only occurs if there are no elements $(\boldsymbol{u}, v)$ left with $\deg_F(lt(\boldsymbol{u})) \leq q+1$. Thus, with the POT-lift, we would not go any further in position i than to the degree $q+2$.

We first want to give an example that it is not guaranteed that a finite Pommaret basis of $Syz(F)$ exists only because there is one for I.

Example 4.3.17
$I \coloneqq \langle x, y\rangle \trianglelefteq K[x, y]$, where we respect the ordering of x and y, i.e. we have $G \coloneqq \{(\boldsymbol{e}_1, x), (\boldsymbol{e}_2, y)\}$. With a POT-lift obeying $\boldsymbol{e}_1 \prec_{POT} \boldsymbol{e}_2$, the syzygy module is generated by $x\boldsymbol{e}_2 - y\boldsymbol{e}_1$ and thus, possesses no finite Pommaret basis.

Still, the semi-involutive algorithm here once again shows it benefits. We have to perform no coordinate transformations on the u-part, which would be necessary in the full involutive version. Also, the J-criteria will discard more potentially superfluous elements. But of course, we have also pointed out the disadvantages of the semi-involutive algorithm, where we might not compute the Gröbner basis of $Syz(F)$ completely before interrupting the algorithm.

4.4 Algorithm: Strong J-Basis

The Janet division is not global and therefore we cannot be sure without further investigation that an inv. J-pair will be covered by a final G just because it was covered by a subset of it. And of course, we would build up G with the same strategy as in the Pommaret case, where we neglect inv. covered J-pairs. Fair enough, a J-pair that is inv. covered by the computed inv. regular normal form (which will be added to G) will always be inv. covered by it regardless which other elements are added to G. However, this might not be true for syzygies. In the semi-involutive variant, on the other hand, we have the ordinary division in the u-part which helps us finding superfluous J-pairs. Therefore, it is more convenient to use the semi-inv. variant of the GVW algorithm. Furthermore, we will be able to show that we do not need the concept of bridging pairs. We could go

straight forward to the main theorem of this section. But before we do, we show a small lemma that points out the special relation between the Janet division and reductions on M.

Lemma 4.4.1
Let $G \subseteq M$ be finite. G is inv. autoreduced if and only if the v-parts of G are inv. head autoreduced.

Proof. If the v-parts are inv. head autoreduced, of course, there is no inv. reduction on G possible.

Now, let G be inv. autoreduced. Suppose, there are two pairs $p_i \coloneqq (\boldsymbol{u}_i, v_i) \in G$ for $i = 1, 2$ such that $\mathrm{lt}(v_1) \mid_{J,B_v} \mathrm{lt}(v_2)$. Because $p_i \in G$, we get $\mathrm{lt}(v_1) = \mathrm{lt}(v_2)$[10]. Now, if $\mathrm{lt}(\boldsymbol{u}_1) \neq \mathrm{lt}(\boldsymbol{u}_2)$, then p_1 is inv. regular reducible by p_2 or vice versa. But if the signatures are equal, then the reduction is obviously involutive in the sense of definition 4.0.1. □

Well, as we are performing only inv. regular reductions G might not be inv. autoreduced. But then we could conclude that the v-parts of G are inv. head autoreduced, which is our assumption of the first inv. J-Criteria. But still, we can achieve our goal by assuming that G is inv. regular autoreduced – similar to the assumptions in the second J-Criteria.

Like we did it in the previous chapter, we will present a proof for the full involutive case, however we will use arguments that remain valid for the semi-involutive case. Like in the Pommaret case we first prove a rather technical lemma that corresponds to lemma 4.1.7.

Lemma 4.4.2
Let J be the Janet division. Let $G \subseteq M$ be a finite set. Suppose that every J-pair in G is inv. covered or inv. super reducible by G.
Let $(\boldsymbol{u}, v) \in M$ be non-zero and suppose there is a pair $p_1 \coloneqq (\boldsymbol{u}_1, v_1) \in G$ with $v_1 \neq 0$ such that

(i) $\mathrm{lt}(\boldsymbol{u}_1) \mid_{J,B_u} \mathrm{lt}(\boldsymbol{u})$ and

(ii) $t\mathrm{lt}(v_1) \coloneqq \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_1)}\mathrm{lt}(v_1)$ is minimal under all elements in G that satisfy condition (i).

If t contains a non-multiplicative variable for $\mathrm{lt}(v_1)$ then there exists a pair $p'' \coloneqq (\boldsymbol{u}'', v'') \in G$ such that $v'' \neq 0$ and tp_1 is inv. super reducible by p''.

Proof. ad a): If t contains a non-multiplicative variable for $\mathrm{lt}(v_1)$, this means that there is a $x_k \in \mathrm{supp}(t)$, such that $x_k(\boldsymbol{u}_1, v_1)$ is an involutive J-pair. If this J-pair is

[10] This is a property of the Janet division [16, p. 67].

inv. covered by G, by definition, there is a $(\boldsymbol{u}_2, v_2) \in G$ such that

$$\mathrm{lt}(\boldsymbol{u}_2) \mid_{J,B_u} x_k\mathrm{lt}(\boldsymbol{u}_1) \quad \text{and} \quad \frac{x_k\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}_2)}\mathrm{lt}(v_2) \prec x_k\mathrm{lt}(v_1). \tag{4.4.1}$$

Because t is a multiplicative term for $\mathrm{lt}(\boldsymbol{u}_1)$, x_k is multiplicative, too. Therefore, $\mathrm{lt}(\boldsymbol{u}_1) \mid_{J,B_u} x_k\mathrm{lt}(\boldsymbol{u}_1)$. But as we have $\boldsymbol{u}_1, \boldsymbol{u}_2 \in B_u$, $\mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u}_2)$ must hold. In particular this means $\mathrm{lt}(\boldsymbol{u}_2) \mid_{J,B_u} t\mathrm{lt}(\boldsymbol{u}_1)$ is true. We multiply both sides of the second relation in (4.4.1) with $\frac{t}{x_k}$ which leads to a contradiction of the choice of $(\boldsymbol{u}_1, v_1)$.
Thus, the J-pair is inv. super reducible. Then, there is a $p_3 \coloneqq (\boldsymbol{u}_3, v_3) \in G$ with $v_3 \neq 0$ (as otherwise the inv. J-pair would be inv. covered by it), such that

$$\mathrm{lt}(\boldsymbol{u}_3) \mid_{J,B_u} x_k\mathrm{lt}(\boldsymbol{u}_1),$$

from which $\mathrm{lt}(\boldsymbol{u}_3) = \mathrm{lt}(\boldsymbol{u}_1) \mid_{J,B_u} t\mathrm{lt}(\boldsymbol{u}_1)$ follows. Also, we have

$$\mathrm{lt}(v_3) \mid_{J,B_v} x_k\mathrm{lt}(v_1).$$

If $\mathrm{lt}(v_3) \nmid_{J,B_v} t\mathrm{lt}(v_1)$, we can iterate these arguments, taking now a variable x_h in $\mathrm{supp}(\frac{t}{x_k})$ such that x_hp_3 is an inv. J-pair of p_3. Then there exists a pair $p_4 \coloneqq (\boldsymbol{u}_4, v_4)$ with $v_4 \neq 0$ such that x_hp_3 is inv. super reducible by p_4. This again implies $\mathrm{lt}(\boldsymbol{u}_4) = \mathrm{lt}(\boldsymbol{u}_3) = \mathrm{lt}(\boldsymbol{u}_1) \mid_{J,B_u} t\mathrm{lt}(\boldsymbol{u}_1)$ (as $\boldsymbol{u}_4, \boldsymbol{u}_3 \in B_u$). Furthermore, we have $\mathrm{lt}(v_4) \mid_{J,B_v} x_h\mathrm{lt}(v_3) \mid_{J,B_v} x_hx_k\mathrm{lt}(v_1)$. If even $\mathrm{lt}(v_4) \mid_{J,B_v} t\mathrm{lt}(v_1)$ holds, we are done because x_hp_3 and tp_1 have the same leading coefficients. Eventually, we construct an element $(\boldsymbol{u}'', v'') \in G$ after at most $\deg(t)$ steps such that $v' \neq 0$ and $t(\boldsymbol{u}_1, v_1)$ is inv. super reducible by $(\boldsymbol{u}'', v'')$. □

Theorem 4.4.3 ***(Involutive J-Criteria (III))***
Let J denote the Janet division. Let $G \subseteq M$ be finite and inv. regular autoreduced. Moreover, assume that $\langle Sig(G)\rangle_J = \mathbb{T}_n^m$. Then the following statements are equivalent.

a) G is a strong J-basis of M.

b) Every involutive J-pair of elements of G is eventually inv. super reducible by G.

c) Every involutive J-pair of elements of G is inv. covered by G or inv. super reducible by G.

Proof. Because of lemma 4.1.6 we only have to show "$c) \Rightarrow a)$". Basically, we follow the proof for the Pommaret case. However, this time, many things will be easier.

We give again a proof by contradiction. For this purpose, suppose that G is not a strong J-basis of M and that c) holds. Then – since G is finite – there is only one way for G not to be a strong J-basis: There must exist a pair $(\mathbf{0}, 0) \neq (\boldsymbol{u}, v) \in M$ which is not inv. reducible by G. We take the one with smallest signature. We set $T \coloneqq \mathrm{lt}(\boldsymbol{u})$ and observe that $T \neq \mathbf{0}$ as otherwise v would be 0, too. Now, as $\langle \mathrm{Sig}(G) \rangle_J = \mathbb{T}_n^m$ is true by our assumptions, we can choose a pair $(\boldsymbol{u}_1, v_1) \in G$ with the following two properties:

(i) $\mathrm{lt}(\boldsymbol{u}_1) \mid_{J,B_u} \mathrm{lt}(\boldsymbol{u})$ and

(ii) $t\mathrm{lt}(v_1) \coloneqq \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_1)}\mathrm{lt}(v_1)$ is minimal under all elements in G that satisfy condition (i).

Note, that $v_1 \neq 0$ as otherwise $(\boldsymbol{u}, v)$ would be inv. reducible by a syzygy $(\boldsymbol{u}_1, 0)$ due to condition (i).

We again claim that $t(\boldsymbol{u}_1, v_1)$ is not inv. regular reducible by G. Suppose that this is not true. Then there is a $p_2 \coloneqq (\boldsymbol{u}_2, v_2) \in G$ such that $t(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by p_2. $t = 1$ is impossible since G is inv. regular autoreduced. Also if $t \neq 1$ contains only multiplicative variables for $\mathrm{lt}(v_1)$, we obtain $\mathrm{lt}(v_1) \mid_{J,B_v} t\mathrm{lt}(v_1)$ and $\mathrm{lt}(v_2) \mid_{J,B_v} t\mathrm{lt}(v_1)$, and hence $\mathrm{lt}(v_2) \mid_{J,B_v} \mathrm{lt}(v_1)$ or $\mathrm{lt}(v_1) \mid_{J,B_v} \mathrm{lt}(v_2)$. In either of these both cases we obtain $\mathrm{lt}(v_1) = \mathrm{lt}(v_2)$. Therefore, applying lemma 4.2.2, we know that even p_1 is inv. regular reducible by p_2 which is impossible. Then, $t \neq 1$ must contain a non-multiplicative variable. Lemma 4.4.2 tells us, that there is a $(\boldsymbol{u}'', v'') \in G$ such that tp_1 is inv. super reducible by it. Thus,

$$\mathrm{lt}(\boldsymbol{u}'') \mid_{J,B_u} t\mathrm{lt}(\boldsymbol{u}_1) \quad \text{and} \quad \mathrm{lt}(v'') \mid_{J,B_v} t\mathrm{lt}(v_1) \quad \text{and} \quad \frac{t\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}'')} = \frac{t\mathrm{lt}(v_1)}{\mathrm{lt}(v'')}$$

is true. As seen above, we can conclude $\mathrm{lt}(\boldsymbol{u}'') = \mathrm{lt}(\boldsymbol{u}_1)$. But then we get from $\frac{t\mathrm{lt}(\boldsymbol{u}_1)}{\mathrm{lt}(\boldsymbol{u}'')} = \frac{t\mathrm{lt}(v_1)}{\mathrm{lt}(v'')}$ the equality $\mathrm{lt}(v'') = \mathrm{lt}(v_1)$. Thus $\mathrm{lt}(v_1) = \mathrm{lt}(v'') \mid_{J,B_v} t\mathrm{lt}(v_1)$. But then t must be a multiplicative term for $\mathrm{lt}(v_1)$ contradicting that we have assumed for this case that t contains a non-multiplicative variable for $\mathrm{lt}(v_1)$.

This is telling us that $t(\boldsymbol{u}_1, v_1)$ is not inv. regular reducible by G. Next, we follow the strategy from the Pommaret case, setting $c \coloneqq \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_1)}$ and

$$(\boldsymbol{u}', v') \coloneqq (\boldsymbol{u}, v) - ct(\boldsymbol{u}_1, v_1).$$

First, we observe that $\mathrm{lt}(\boldsymbol{u}') \prec \mathrm{lt}(\boldsymbol{u}) = T$. For the v-part, there are several cases to consider.

If $\mathrm{lt}(v) \neq t\mathrm{lt}(v_1)$, i.e. $v' \neq 0$, then we argue as follows: Because $(\boldsymbol{u}', v')$ has a smaller signature than $(\boldsymbol{u}, v)$ it must be inv. reducible by G. For the moment, we reduce by syzygies if possible. Doing so, we only can reduce the signature, and hence, the remainder is still inv. reducible by G. But now, it is inv. reducible by

a pair $(\boldsymbol{u}_3, v_3)$ with $v_3 \neq 0$. Also note that v' has not been changed during the reduction process so far.
Since $\mathrm{lt}(v) \neq t\mathrm{lt}(v_1)$, there are two cases.

- If $\mathrm{lt}(v) \prec t\mathrm{lt}(v_1)$ is true, then we have $\mathrm{lt}(v') = t\mathrm{lt}(v_1)$. Hence, we get the relations

$$\mathrm{lt}(v_3) \mid_{J,B_v} \mathrm{lt}(v') = t\mathrm{lt}(v_1) \quad \text{and} \quad \frac{t\mathrm{lt}(v_1)}{\mathrm{lt}(v_3)}\mathrm{lt}(\boldsymbol{u}_3) \preceq \mathrm{lt}(\boldsymbol{u}') \prec T = t\mathrm{lt}(\boldsymbol{u}_1),$$

  which implies that $t(\boldsymbol{u}_1, v_1)$ is inv. regular reducible by G leading to a contradiction to our result above.

- If, on the other hand, $t\mathrm{lt}(v_1) \prec \mathrm{lt}(v)$ is true, then we get $\mathrm{lt}(v') = \mathrm{lt}(v)$. Therefore we obtain

$$\mathrm{lt}(v_3) \mid_{J,B_v} \mathrm{lt}(v') = \mathrm{lt}(v) \quad \text{and} \quad \frac{\mathrm{lt}(v)}{\mathrm{lt}(v_3)}\mathrm{lt}(\boldsymbol{u}_3) \preceq \mathrm{lt}(\boldsymbol{u}') \prec T = \mathrm{lt}(\boldsymbol{u}),$$

  which now implies that $(\boldsymbol{u}, v)$ is inv. regular reducible by G leading once again to a contradiction since $(\boldsymbol{u}, v)$ is not inv. reducible by G due to our assumptions from the beginning of this proof.

Accordingly, there is only one possibility left, i.e. we have $\mathrm{lt}(v) = t\mathrm{lt}(v_1)$. If $t = 1$ or if $t \neq 1$ is a multiplicative term for $\mathrm{lt}(v_1)$, then $\mathrm{lt}(v_1) \mid_{J,B_v} \mathrm{lt}(v)$, $\mathrm{lt}(\boldsymbol{u}_1) \mid_{J,B_u} \mathrm{lt}(\boldsymbol{u})$ and $\frac{\mathrm{lt}(v)}{\mathrm{lt}(v_1)} = \frac{\mathrm{lt}(\boldsymbol{u})}{\mathrm{lt}(\boldsymbol{u}_1)} = t$ and hence, $(\boldsymbol{u}, v)$ is inv. reducible by $(\boldsymbol{u}_1, v_1) \in G$. But this is not possible as $(\boldsymbol{u}, v)$ is inv. irreducible by G. So $t \neq 1$ has at least one non-multiplicative variable for $\mathrm{lt}(v_1)$. Applying lemma 4.4.2 we obtain a pair $(\boldsymbol{u}_4, v_4) \in G$ such that $t(\boldsymbol{u}_1, v_1)$ is inv. super reducible by $(\boldsymbol{u}_4, v_4)$. But because of $t\mathrm{lt}(\boldsymbol{u}_1) = \mathrm{lt}(\boldsymbol{u})$ and $t\mathrm{lt}(v_1) = \mathrm{lt}(v)$, this implies that $(\boldsymbol{u}, v)$ is involutive reducible by $(\boldsymbol{u}_4, v_4)$ (*not* necessarily inv. super reducible since we might have $\frac{\mathrm{lc}(v)}{\mathrm{lc}(v_1)} \neq \frac{\mathrm{lc}(\boldsymbol{u})}{\mathrm{lc}(\boldsymbol{u}_1)}$), which is a contradiction to our choice of $(\boldsymbol{u}, v)$. □

Although we have proven the full involutive version of this theorem, from now on we focus on the semi-involutive variant. The proof can easily be adopted. It is also a strength of the Janet version that we do not have to consider a set $BG(G)$. As we have mentioned already in the introduction, Binaei et al. have presented similar theorem in [1], that only differs in the second condition in the statement c) for the Janet division. Although we have discussed that their theorem is not correct (see last paragraph in remark 4.1.9), the proof of termination remains valid for the Janet division. They have related it to Gerdt's algorithm [1, Thm. 6]. Thus, we end up with the following pseudo code, where we mark notions that must be treated differently in the semi-inv. case. For instance, "inv.∗ super reducible" only

differs from the notion we have introduced by the division in the u-part. In the semi-inv. case we of course take the common division rather than the Janet division. The proof of correctness follows immediately from the involutive J-criteria (III).

SemiInvGVW$(F, H_0, \prec_1, \prec_2, J)$ (Janet Version)	
Input:	A set $F = \{f_1, \ldots, f_m\} \subseteq R$ of polynomials, $\prec_1$ on R and a compatible term order $\prec_2$ on R^m, J Janet division, An autoreduced set H_0 of syzygies of F, where $H_0 = \emptyset$ is possible.
Output:	A weak Janet basis for $I = \langle F \rangle$ and a Gröbner basis of $Syz(F)$.
Variables:	G is an ordered set of pairs $(\boldsymbol{u}_i, v_i) \in M$ with $v_i \neq 0$. H is an ordered set of syzygies $(\boldsymbol{u}, 0)$ of F. $JP(G)$ is the set of involutive J-pairs of G.
Step 1:	$G \leftarrow \{(\boldsymbol{e}_i, f_i) \mid 1 \leq i \leq m\}$, $H \leftarrow H_0$
Step 2:	Perform an inv. regular autoreduction on G. Fill H with obtained syzygies, discard them from G. Calculate (new) trivial syzygies of G and add them to H. Autoreduce H. Fill $JP(G)$ with (new) inv. J-pairs of G.
Step 3:	**while** $JP(G) \neq \emptyset$ **do**
Step 4:	Take an element $p := (\boldsymbol{u}, v) \in JP(G)$ with smallest signature and then with smallest leading term in the v-part.
Step 5:	If • p is covered by $G \cup H \cup JP(G) =: S$, or • p is inv.$*$ super reducible by $S \setminus \{p\}$, then discard p and go back to step 3.
Step 7:	Calculate an inv. regular normal form $(\boldsymbol{u}', v')$ of p by G
Step 8:	**If** $v' = 0$ **then**
Step 12:	$H \leftarrow H \cup \{(\boldsymbol{u}', 0)\}$
Step 13:	**else**
Step 17:	$G \leftarrow G \cup \{(\boldsymbol{u}', v')\}$. Go back to step 2.
Step 18:	**end if**
Step 19:	**end while**
Return:	$\{v_i \mid (\boldsymbol{u}_i, v_i) \in G\}$ and $\{\boldsymbol{u} \mid (\boldsymbol{u}, 0) \in H\}$

5 Remarks on Implementation

In this section, we discuss our implementation in Maple 18. For the implementation we use the package "Groebner" to have access to some optimized functions that, for example, a test which of two given terms is larger. First, we want to mention how an element $(\boldsymbol{u}, v) \in G \cup H$ is stored. Assume that $\mathrm{lm}(\boldsymbol{u}) = ct\boldsymbol{e}_i$ for some $c \in K$ and $t \in \mathbb{T}_n$. We store vectors in lists and $(\boldsymbol{u}, v)$ is represented by

$$[[c, t, i, \boldsymbol{u}], [\mathrm{lc}(v), \mathrm{lt}(v), v], \bar{X}_P(\mathrm{lt}(v))]].$$

We have implemented a sort function *FHelp* that sorts elements in G by signature and then by the leading term of the v-part. This helps us to reduce the computational time for inv. regular reductions. As regular reductions cannot increase the signature, we have implemented the function *FindIndex* that finds the largest element (by signature) we have to consider for (inv.) regular reductions.
We have then implemented the full and semi-involutive GVW algorithm for the Pommaret division according to our presented pseudo code with additional coordinate transformations as described in remark 4.3.15. Here we want to point out, that only a TOP-lift variant of the algorithm should be used when coordinate transformations are needed. A POT-lift version would take additional effort and could not be implemented in our code, yet. Also, the algorithm is not yet free from all errors if one takes large systems where coordinate transformations are required. As we wanted to check computationally that no inv. super autoreductions are needed for H, we decided not to insert trivial syzygies to H. Nevertheless, inv. super autoreductions will be necessary when coordinate transformations are needed. And in such cases, these reduction steps will be performed. We have decided to fill $JP(G)$ with all possible J-pairs at once which is very inefficient but an easy way on the other hand to exclude mistakes coming from some strategies of filling $JP(G)$. Nevertheless, other strategies can be implemented fairly easy by just commenting out some lines in the code. Still, this means that we have computed inv. J-pairs of an element in G that may get inv. regular reduced before we have to consider its J-pairs. Thus, we would have spent time in computing the inv. J-pair and finding out that it is inv. covered by the computed inv. regular normal form. This shows that we have an inefficient code. We also have not implemented step 6 from the pseudo-code as it is only a small optimization which seems not to apply very often. However, the implementation of the corresponding function requires for-loops that

may take too much time, relatively speaking. Nevertheless, we have done some optimizations to our code by using the functions *FindIndex* and *FHelp*. Also, it might be useful to only keep the signatures once we have exceeded the degree limit $q+1$ since all following elements are not of interest to us. This might save time for the calculations in the degree $q+2$.

The strength of the implementation is the following. One can choose between a TOP-lift (encoded in $ord = 2$) and a POT-lift ($ord = 1$), the full ($Syzbool = true$) and semi-involutive variant ($Syzbool = false$) and between keeping the whole u-part ($SigOnly = false$) or only the signatures ($SigOnly = true$). Then, one can call the algorithm by the function $StrPBas(F, H_0, Syzbool, q, false)$, where H_0 is an (inv) autoreduced set of syzygies and q a degree bound for elements in a Pommaret basis of I. The last entry is set to be *false* initially. It will be set to be *true* after we have found out, that a coordinate transformation is required. Then we call *StrPBas* recursively with the last parameter, called *RestartBool*, being *true*. After the algorithm has returned a result G and H it should be tested. If $Syzbool = true$ and $SigOnly = false$, i.e. we are in the full involutive case where we keep the whole u-part, the function *TestBasis* computes all non-multiplicative prolongations of any syzygy from H and performs involutive reductions. If and only if all these reductions end with a zero vector the message *"True for syzygy module"* is printed. This pays respect to the fact that the function does not test whether we have found a generating system of $Syz(F)$. If this error message is not printed, H is not a weak Pommaret basis of $Syz(F)$, and thus, this is what will be printed instead. Moreover, *TestBasis* does the same check for G regardless of what choice of parameters we have set (this is meaningful as we always aim to compute a Pommaret basis of I). Here, we print *"Output contains a Pommaret basis for the ideal"*, if and only if all reduction steps return the remainder 0 which takes two things into account: First, we know that we have a generating system as we have started with $(\boldsymbol{e}_i, f_i)$, $1 \leq i \leq m$. Secondly, it contains the result of remark 4.3.12. Indeed, the detection of the negligible elements mentioned in that remark is already implemented at the end of *StrPBas*. Hence, the function returns a (strong) Pommaret basis of I. If G is not a weak Pommaret basis, the algorithm will detect it and print a corresponding message. It is worth mentioning that the non-involutive GVW algorithm may not have a reduced Gröbner basis contained in its output as there is no set $BP(G)$ that ensures that the proxy will be reduced.

5.1 Benchmarks

Although we have presented the proof of termination only for homogeneous inputs, we will present benchmark calculations with affine inputs. Here, we are not comparing with algorithms that only aim to compute a Pommaret basis or a Janet

basis of I as our algorithm does more than this. Also, a comparison would be not fair since our implementation is far away from being completely optimized. Instead, we make some statistics about the different variants that are provided by our implementation. Finally, we can compare it with the Janet version of the semi-involutive variant that has been implemented by Binaei. As only signatures are saved in this implementation, we shall compare the computational time with our algorithm where we choose $SigOnly = true$. And because the algorithm does only aim to compute a Janet basis of I, we only compare zero dimensional ideals, which implies that no coordinate transformation will be required and both algorithms will compute a Pommaret basis.
However, we surely want to investigate with at least a few examples of how our algorithm works when a coordinate transformation is needed. We return the coordinate transformations (from top to bottom), the maximal value for the index of safety[1], the number of syzygies, the number of elements in the Pommaret basis and the used value for q which encodes the Castelnuovo-Mumford regularity $Reg(I)$ in the related examples.
In order to underline the advantage of the algorithm when syzygies are known, we will also restart the computations with $H_0 = H$ as input, where H is a generating system or signatures of the generating system of $Syz(F)$. Thus, we have the following structure of cells:

runtime [s]: $H_0 = \emptyset$	discarded elements	regular normal forms	$\lvert H \rvert$
runtime [s]: $H_0 = H$	discarded elements	regular normal forms	

Therefore, we obtain the following tables for zero dimensional benchmark problems.

POT-lift	Katsura5 (q=6)				Katsura6 (q=7)				Katsura7 (q=8)			
SigOnly=true	8.16	140	93	43	84.63	386	188	83	1241.4	1003	372	156
Syzbool=false	3.53	175	50		36.53	450	105		434.6	1113	216	
SigOnly=false	15.31	144	94	44	200.58	399	191	86				
Syzbool=true	5.03	179	50		53.5	462	105					
SigOnly=false	15.28	140	93	43	203.13	386	188	83				
Syzbool=false	5.13	175	50		53.2	450	105					

[1]Remember that we have an index of safety for every coordinate transformation that we perform.

TOP-lift	Katsura5 (q=6)				Katsura6 (q=7)				Katsura7 (q=8)			
SigOnly=true	7.47	112	83	42	80.06	307	164	80	981.95	778	310	143
Syzbool=false	3.64	153	41		33.97	384	84		370.75	918	167	
SigOnly=false	23.03	111	84	43	364.48	304	167	83				
Syzbool=true	5.66	153	41		55.06	384	84					
SigOnly=false	22.34	112	83	42	338.84	307	164	80				
Syzbool=false	5.47	153	41		53.17	384	84					

POT-lift	Chandra4 (q=4)				Chandra5 (q=5)				Chandra6 (q=6)			
SigOnly=true	0.13	24	26	11	1.05	78	60	26	8.73	224	130	57
Syzbool=false	0.09	28	15		0.84	89	34		6.80	250	73	
SigOnly=false	0.22	24	26	11	1.52	78	60	26	12.80	224	130	57
Syzbool=true	0.16	28	15		1.02	89	34		8.58	250	73	
SigOnly=false	0.20	24	26	11	1.42	78	60	26	12.45	224	130	57
Syzbool=false	0.14	28	15		0.97	89	34		8.48	250	73	

TOP-lift	Chandra4 (q=4)				Chandra5 (q=5)				Chandra6 (q=6)			
SigOnly=true	0.14	24	26	11	1.31	78	60	26	11.23	224	130	57
Syzbool=false	0.14	28	15		1.23	89	34		9.31	250	73	
SigOnly=false	0.25	24	26	11	2.02	78	60	26	19.52	224	130	57
Syzbool=true	0.16	28	15		1.41	89	34		11.98	250	73	
SigOnly=false	0.23	24	26	11	2.16	78	60	26	18.50	224	130	57
Syzbool=false	0.19	28	15		1.30	89	34		12.16	250	73	

One can observe that for the small Chandra benchmark runs, the POT-lift variant is a bit faster. However, for the Katsura runs the opposite is true. For Katsura7 the difference is about 260s. Also, the bigger the example is the bigger is the difference between discarded elements and thus, the amount of saved regular normal form calculations. However, if we compare the number of discarded elements from a POT-lift run with a TOP-lift run we can conclude that with a POT-lift more elements will be discarded. But as the usage of the POT-lift leaded to a larger runtime, it seems to be the case that too many negligible pairs were calculated. This might come from the incremental character of the GVW algorithm when a POT-lift is used. It is also worth mentioning that the semi- and full involutive variants do not differ very much according to their runtimes. However, only keeping the signatures has a major impact on the runtime. Now let us compare the runtimes of our implementation with Binaei's. Remember, that we take the rimes from the first row as this row corresponds to the structure of Binaei's implementation.

	Chandra4	Chandra5	Chandra6	Katsura5	Katsura6	Katsura7
Pommaret	0.13-0.14	1.05-1.31	8.73-11.23	7.47-8.16	80.06-84.63	981.95-1241.4
Janet	0.63	5.34	52.5	43.69	636.09	10155.31

Also, keep in mind, that instead of a POT- or TOP-lift the author chose the Schreyer ordering. For these examples, we can conclude that our implementation is about four to five times as fast as the implementation of Binaei for the smaller examples and five to eight times as fast if it comes to Katsura runs. This is surprising in the sense that for the Pommaret case we have to consider bridging pairs. But the answer may lie in the fact that our J-criteria potentially discards more elements than the J-criteria presented in [1]. Now, one may also think that this comes from the fact that we did not take the degree of the Janet basis as our value of q but instead searched heuristically for the Castelnuovo-Mumford regularity (which was often smaller by 1 for these examples). However, this is not true. For instance, the run for Katsura6 was repeated with $q = 8$ and finished after 91.25s with a TOP-lift. Furthermore, our algorithm only discards elements of degree in the v-part that is greater than $q + 1$ (in the semi-inv. variant). So, this cannot be the reason. Maybe our implementation is that much faster because our term orders on R^m work better for the GVW algorithm, or because we do not compute the whole Gröbner basis of $Syz(F)$ in general. However, this is an open question at this point.

For investigating the performance of our implementation for inputs where coordinate transformations are required, we look at the following four rather small examples.

$$
\begin{aligned}
F_1 &\coloneqq \{y^2, yz + y^2, xz + xy\} \\
F_2 &\coloneqq \{y^3 - xyz, yz^3 + y^4, z^2x + x^2y, x^2 + xy\} \\
F_3 &\coloneqq \{y^3 - xyz + yz^2, yz^3 + y^2x^2, z^2x + x^2y, x^2 + xy + zx\} \\
F_4 &\coloneqq F_3 \cup \{xy - t^2\}
\end{aligned}
$$

The following table summarizes the obtained information from the calculations. Here, we chose *Syzbool=true* and *SigOnly=false* so that transformations of $Syz(F)$ would be detected, too. However, the algorithm never returned an error message for $Syz(F)$. If the maximal index of safety is represented by "[]", this means, that all elements in $JP(G) \cup BG(G)$ could be discarded for the corresponding transformation. Thus, we obtain

TOP-lift	runtime	$\|H\|$	$\|G\|$	$Reg(I)$	transformations	max. index of safety
F_1	0.63	2	3	2	$x \mapsto x+z$ $y \mapsto y+t$	[]
F_2	20.33	7	7	5	$x \mapsto x+t$ $y \mapsto y+z$	2
F_3	19.45	10	7	5	$x \mapsto x+t$ $y \mapsto y+z$	2
F_4	40.25	18	17	6	$y \mapsto y+z$ $x \mapsto x+y$	3

All ideals from the examples could be transformed into a quasi-stable position with two coordinate transformations. The index of safety, however, turned out not to be as big as expected. But this might change for larger examples, where for instance many syzygies have small signatures. Nevertheless, it would take much effort to adjust the algorithm for managing bigger examples.

5.2 Benefits and Issues of Usage of POT- or TOP-lifts

We have focused especially on TOP- and POT-lifts. In this rather small subsection, we want to collect properties of the POT- and TOP-lift in the context of the (semi-)inv. GVW algorithm.
Now, it is well known, that with a POT-lift, the algorithm becomes incremental [7]. Furthermore, as we are performing coordinate transformations on the u-part, too, we have to find the signatures of the transformed pairs. For the u-part, this obviously is easier with a POT-lift than with a TOP-lift as we have to search for the leading term only in one position of the vector in the u-part. However, when using the POT-lift, we may be stuck easier at a signature belonging to a position i, because the POT-lift is not of type ω. Hence, we may go to the degree $q+1$ more often until we jump to elements with a signature at position $i+1$. This means, that we are calculating too many unnecessary pairs, blowing up the set G and hence increasing the costs for any operation on G, especially the calculation of new elements for $JP(G) \cup BP(G)$ for the Pommaret case. A POT-lift, in general, reacts sensitively to these signature-based algorithms as the order of the elements in F have a major impact on the efficiency as we will recall in a moment. Whereas a TOP-lift is more convenient for calculations, it is rather expensive when we have to perform a lot of coordinate transformations. However, it is an open question at this point which of the two lifts performs better according to the index of safety. Lastly, we want to recall one more thing:

It is not guaranteed that a Pommaret basis exists for $Syz(F)$ just because it exists for $\langle F \rangle$, at least if it comes to the POT-lift. A simple example was given in example 4.3.17. In fact, we want to point out that in this example we already started with a Pommaret basis of $\langle F \rangle$, yet our algorithm would return an error message for $Syz(F)$ and the POT-lift. However, one can see that everything would work perfectly fine if we took a POT-lift and just changed the order of our elements in F, so that $G = \{(\boldsymbol{e}_1, y), (\boldsymbol{e}_2, x)\}$ holds. Then $\boldsymbol{e}_1 \prec_{POT} \boldsymbol{e}_2$, however, now the leading term of the syzygy $x\boldsymbol{e}_1 - y\boldsymbol{e}_2$ is $y\boldsymbol{e}_2$. This, on the other hand, points out how sensitive the inv. GVW algorithm reacts to the POT-lift. This is also based on the fact that the algorithm becomes incremental for a POT-lift.

6 Summary and Outlook

In this thesis, we have introduced the main ideas of the original GVW algorithm and then presented a corresponding theory for involutive divisions where we discussed very detailed the algorithm for the Pommaret division. We have developed the theory also presenting the process of finding computational achievable assumptions under which an involutive J-criteria holds. We also gave examples of why none of the made assumptions can be dropped. Moreover, we gave a counterexample for the inv. J-criteria from [1]. We presented for our version some criteria in order to make an implementation more efficient and proved the termination of the full and semi-inv. GVW algorithm. We also pointed out the benefits of both variants and the issues that go along with them. Then we have introduced coordinate transformations and the index of safety that arose naturally from our strategy for the algorithm. After completing the discussion of the Pommaret case, we were able to present a Janet version of the GVW algorithm. Indeed, we have found out that no bridging pairs are required. But even though we have proven a full inv. version, we argued that without further investigations only a semi-inv implementation of the algorithm is meaningful. In the last chapter, we gave remarks on our implementation and presented some benchmark computations along with some examples that tested the functionality of coordinate transformations. However, the computation of the index of safety turned out to be too expansive in relation to its benefits – at least if it comes to such small examples.

With the versions of the inv. GVW algorithm for the Pommaret and Janet version, we gave an algorithm to compute Pommaret bases for homogeneous ideals and the degree reverse lexicographic order together with a compatible term order of type ω or a POT-lift of pseudo type ω. In the last subsection, we collected some properties of these term orders. However, we left out the discussion of the Schreyer ordering which was used in [1] for the implementation.

Still, the given implementation is only a proof of concept and shall not be used for bigger examples. For further investigation of this algorithm and its properties with a POT- or TOP-lift, one may consider the following questions: Is $Syz(F)$ in quasi-stable position for a TOP-lift of $\prec_{\text{degrevlex}}$ if $\langle F \rangle$ is in quasi-stable position? Does the POT-lift lead to a bigger maximal value of the index of safety compared to the one obtained with a TOP-lift?
Furthermore, it might be interesting to find out whether there is a different proof for the termination of the semi-inv. GVW algorithm for the Pommaret division

where the computation of a Gröbner basis of $Syz(F)$ is not interrupted. Lastly, it should be investigated in detail how the Pommaret variant can be adapted for affine inputs. And it might be also interesting to discover why our implementation seems to be much faster than the implementation for the Janet division.
Furthermore, it might be useful to add some of the ideas presented in the introduction to the inv. GVW algorithm. In particular, one could aim to create a Hilbert-driven algorithm that uses the substituting method from [14] and the concept of mutant pairs from [18].

7 Bibliography

[1] Bentolhoda Binaei, Amir Hashemi, and Werner M. Seiler. Computation of Pommaret Bases Using Syzygies. In Werner M. Seiler Vladimir P. Gerdt, Wolfram Koepf and Evgenii V. Vorozhtsov, editors, *International Workshop on Computer Algebra in Scientific Computing*, pages 51–66. Springer, 2018.

[2] Bruno Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. *PhD thesis, Universitat Insbruck*, 1965.

[3] David Cox, John Little, and Donal O'shea. *Using algebraic geometry*, volume 185. Springer Science & Business Media, 2006.

[4] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

[5] Jean Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F 5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83. ACM, 2002.

[6] Shuhong Gao, Yinhua Guan, and Frank Volny IV. A new incremental algorithm for computing Gröbner bases. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 13–19. ACM, 2010.

[7] Shuhong Gao, Frank Volny IV, and Mingsheng Wang. A new framework for computing Gröbner bases. *Mathematics of computation*, 85(297):449–465, 2016.

[8] Vladimir P. Gerdt. On the relation between Pommaret and Janet bases. In E.W. Mayr V.G. Ganzha and E.V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing*, pages 167–181. Springer, 2000.

[9] Vladimir P. Gerdt and Yuri A. Blinkov. Involutive bases of polynomial ideals. *Mathematics and Computers in Simulation*, 45(5-6):519–541, 1998.

[10] Amir Hashemi, Michael Schweinfurter, and Werner M. Seiler. Deterministic genericity for polynomial ideals. *Journal of Symbolic Computation*, 86:20–50, 2018.

[11] Maurice Janet. *Sur les systèmes d'équations aux dérivées partielles*. Univ. de Paris, 1920.

[12] Daniel Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In J.A. Hulzen, editor, *European Conference on Computer Algebra*, volume 162, pages 146–156. Springer, 1983.

[13] Dongmei Li, Jinwang Liu, Weijun Liu, and Licui Zheng. GVW algorithm over principal ideal domains. *Journal of Systems Science and Complexity*, 26(4):619–633, 2013.

[14] Ting Li, Yao Sun, Zhenyu Huang, Dingkang Wang, and Dongdai Lin. Speeding up the GVW algorithm via a substituting method. *Journal of Systems Science and Complexity*, 32(1):205–233, 2019.

[15] H. Michael Möller, Teo Mora, and Carlo Traverso. Gröbner bases computation using syzygies. In *Papers from the international symposium on Symbolic and algebraic computation*, pages 320–328. ACM, 1992.

[16] Werner M. Seiler. *Involution: The formal theory of differential equations and its applications in computer algebra : with 2 tables*, volume Vol. 24 of *Algorithms and computation in mathematics*. Springer, Berlin and Heidelberg, 2010.

[17] Bruno Simões. An Hilbert-Driven Strategy for Signature-Based Gröbner Basis Algorithms. In *Future Vision and Trends on Shapes, Geometry and Algebra*, pages 13–37. Springer, 2014.

[18] Yao Sun, Zhenyu Huang, Dingkang Wang, and Dongdai Lin. An improvement over the GVW algorithm for inhomogeneous polynomial systems. *Finite Fields and Their Applications*, 41:174–192, 2016.

[19] Frank Volny. New algorithms for computing Gröbner bases. *TigerPrints*, 2011.

[20] A. Yu Zharkov and Yu A. Blinkov. Involution approach to investigating polynomial systems. *Mathematics and Computers in Simulation*, 42(4-6):323–332, 1996.

Statutory Declaration

I hereby declare that the thesis submitted is my own unaided work. All direct or indirect sources used are acknowledged as references. The thesis in the same or similar form has not been submitted to any examination body and has not been published. This thesis was not yet, even in part, used in another examination or as a course performance.

Thomas Izgin