JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche
Fakultät

Gröbner Bases and Generalized Sylvester Matrices

DISSERTATION

zur Erlangung des akademischen Grades

Doktorin

im Doktoratsstudium der

Technischen Wissenschaften

Eingereicht von:
Manuela Wiesinger-Widi

Angefertigt am:
Institut für Symbolisches Rechnen (RISC)

Beurteilung:
Prof. Dr. Dr.h.c.mult. Bruno Buchberger (Betreuung)
Prof. Dr. Ernst W. Mayr

Linz, Juli 2015

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Die vorliegende Dissertation ist mit dem elektronisch übermittelten Textdokument identisch.

Linz, Juli 2015,

Manuela Wiesinger-Widi

Kurzfassung

In dieser Arbeit untersuchen wir den Zusammenhang zwischen Gröbnerbasen und verallgemeinerten Sylvestermatrizen. Motiviert durch nützliche Resultate im univariaten Fall mit zwei Input-Polynomen, zeigen wir, wie verallgemeinerte Sylvestermatrizen im multivariaten Fall mit mehreren Input-Polynomen dazu verwendet werden können, eine Gröbnerbasis für die Inputmenge zu berechnen. Teilmatrizen der Sylvestermatrix werden schon seit geraumer Zeit dazu verwendet, die Gröbnerbasenberechnung zu beschleunigen. In dieser Arbeit zeigen wir, wie eine Gröbnerbasis berechnet werden kann, indem man eine große Matrix, bestehend aus bestimmten Shifts der Input-Polynome, konstruiert und diese trianguliert. Bestimme Zeilen dieser triangulierten Matrix bilden eine minimale Gröbnerbasis. Wir geben eine obere Schranke für die Größe dieser Matrix an, die vom größten Grad der Input-Polynome, der Anzahl der Variablen und der Anzahl der Input-Polynome abhängt. Als einen Spezialfall untersuchen wir den univariaten Fall mit mehr als zwei Input-Polynomen und geben schärfere Schranken an als die in der Literatur bekannten.
Im zweiten Teil der Arbeit untersuchen wir als einen wichtigen Spezialfall Binomideale. Wir betrachten den Fall mit zwei multivariaten Input-Binomen. Als ersten Schritt behandeln wir das Membership-Problem und geben obere Schranken für den Grad der Kofaktoren eines potentiellen Elementes in der reduzierten Gröbnerbasis an. Diese Schranken sind schärfer als die Schranken, die man von der Hermannschranke durch Spezialisierung bekommt. Als zweiten Schritt geben wir obere Schranken für die Größe der verallgemeinerten Sylvestermatrix an, die ausreichen, um nach obiger Methode eine Gröbnerbasis für bestimmte Fälle von Binomidealen, abhängig vom Support der zwei Input-Binome, zu berechnen. Diese Schranken sind schärfer als die, die man von der Schranke aus dem ersten Teil der Arbeit durch Spezialisierung bekommt.

Abstract

In this thesis we investigate the connection between Gröbner bases computation and generalized Sylvester matrices. Motivated by useful results in the univariate case with two input polynomials, we show how generalized Sylvester matrices can be used in the multivariate case with several input polynomials to compute a Gröbner basis of the input set. Submatrices of the Sylvester matrix have been used for quite some time to speed up the Gröbner bases computation. In this thesis we show how we can compute a Gröbner basis by constructing one big matrix consisting of certain shifts of the input polynomials and triangularizing this matrix. Certain rows of the triangularized matrix form a minimal Gröbner basis. We give an upper bound on the size of this matrix that depends on the highest degree of the input polynomials, the number of variables and the number of input polynomials. As a special case, we treat the univariate case with more than two input polynomials and give sharper bounds than were previously known in the literature.

In the second part of the thesis we investigate as an important special case binomial ideals. We consider the case of two multivariate input binomials. As a first step we treat the membership problem and give upper bounds on the degree of the cofactors of a potential element in the reduced Gröbner basis. These bounds are sharper than the ones obtained by the Hermann bound after specialization. As a second step we give upper bounds for the size of the generalized Sylvester matrix for computing a Gröbner basis for certain cases of binomial ideals depending on the support of the two input binomials. These bounds are sharper than the ones derived from the bound in the first part of the thesis by specialization.

Acknowledgements

I would like to thank my advisor, Bruno Buchberger, for the opportunity to work at RISC and the DK and for supervising this thesis. I am grateful to my second advisor, Ernst W. Mayr, for many helpful suggestions and to Alexander Maletzky for proof reading big parts of this thesis. Many thanks go to those who have helped me — emotionally and financially — in very difficult times in the last few years.

The research was funded by the Austrian Science Fund (FWF): W1214-N15, project DK1 and it was supported by the strategic program "Innovatives OÖ 2010 plus" by the Upper Austrian Government.

Contents

Notation

We denote the set of natural numbers (including 0) by $\mathbb{N}$, the set of integers by $\mathbb{Z}$, the set of rational numbers by $\mathbb{Q}$, the set of real numbers by $\mathbb{R}$, the set of positive real numbers by $\mathbb{R}^+$ and the set of positive real numbers including 0 by $\mathbb{R}_0^+$. For $k \in \mathbb{N}$ we define

$$\mathbb{N}_k := \{i \in \mathbb{N} \mid 1 \leq i \leq k\}.$$

In this paper we use a special kind of representation for polynomials. Let $\mathbb{K}$ be a field, X a finite set of indeterminates and $n := |X|$. We denote the monoid of terms over X by $[X]$ and the degree of a term t by $\deg(t)$. We define the ring of polynomials over $\mathbb{K}$ and X by $\mathbb{K}[X] := \{f : [X] \to \mathbb{K} \mid \text{supp}(f) \text{ is finite}\}$ where, for any $f : [X] \to \mathbb{K}$, $\text{supp}(f) := \{t \in [X] \mid f(t) \neq 0\}$. For any $f, g \in K[X], u \in [X], c \in \mathbb{K}$,

$$\begin{aligned} f + g : [X] &\to \mathbb{K}, \\ t &\mapsto f(t) + g(t), \end{aligned}$$

$$\begin{aligned} f \cdot g : [X] &\to \mathbb{K}, \\ t &\mapsto \sum_{\substack{v,w \in [X] \\ v\, w = t}} f(v)g(w), \end{aligned}$$

$$u\, f := u^* \cdot f,$$

$$c\, f := c^* \cdot f,$$

where $u^*$and c^* are u and c seen as a polynomials, respectively. Furthermore, for $f \neq 0$

$$\deg(f) := \max(\{\deg(t) \mid t \in \text{supp}(f)\}).$$

The ideal generated by a set $F \subseteq \mathbb{K}[X]$ over $\mathbb{K}[X]$ will be denoted by $\text{ideal}(F)$.

For $F \subseteq \mathbb{K}[X]$ we define $\text{hull}(F)$ to be the set of all polynomials of the form $\sum_{i=1}^{m} c_i\, f_i$ with $m \in \mathbb{N}$, $c_i \in \mathbb{K}$ and $f_i \in F$ for $i \in \mathbb{N}_m$.

in some papers called power products

For a finite sequence s over any set, we denote its length by $\mathrm{len}(s)$ and the i-th element in the sequence by s_i for $i \in \mathbb{N}_{\mathrm{len}(s)}$. If s is a nested sequence, we use notation $s_{i,j}$ for $(s_i)_j$ and $s_{i,j,k}$ for $((s_i)_j)_k$, where $i \in \mathbb{N}_{\mathrm{len}(s)}$, $j \in \mathbb{N}_{\mathrm{len}(s_i)}$ and $k \in \mathbb{N}_{\mathrm{len}((s_i)_j)}$.

Chapter 1

Introduction

1.1 Problem and Previous Work

In his PhD thesis [9], Buchberger introduced the notion of Gröbner bases and gave the first algorithm for computing them. Since then, extensive research has been done in order to reduce the complexity of the computation, the first of them being two criteria given by Buchberger (the product criterion [9, 10] and the chain criterion [12]) to reduce the number of unnecessary S-polynomials. Nevertheless, even for small examples, the computation can be quite time consuming, reflecting the known fact that Gröbner bases computation is intrinsically complex. Still, more theoretical knowledge may improve the concrete complexity of algorithms.

The classical approach for computing a Gröbner basis is introduced by the Buchberger algorithm: We start from the initial set F, execute certain reduction steps (consisting of multiplication of polynomials by terms — called shifts — and subtraction of polynomials). Due to Buchberger's theorem, which says that the computation is finished if all the S-polynomials reduce to zero, we know that after finitely many iterations of this procedure we obtain a Gröbner basis of the ideal generated by F. In two talks [13, 15] and a technical report [14], Buchberger proposed a second approach: We start from F, execute certain shifts of the initial polynomials in F, arrange them as rows in a matrix, triangularize this matrix and from the resulting matrix extract a Gröbner basis by formation of the "contour".

In this thesis we pursue the second approach and seek to improve the theory in order to speed up the Gröbner bases computation. This approach has been studied a couple of times in the past, but never thoroughly. The immediate question is: Can we give an a priori upper bound on the degrees of the necessary shifts such that a triangularization of the matrix built by these shifts yields a Gröbner basis?

In the univariate case, Gröbner bases computation amounts to the computation of a gcd of the input polynomials. Going back to work of Sylvester [62], Habicht [37] and later Collins [19, 20] and Brown and Traub [8, 7] built up the theory of polynomial subresultants, which are determinant polynomials of certain submatrices of the Sylvester matrix, and showed that they are the same as the remainders of the Euclidean algorithm up to certain constant factors. For an overview of this topic see for example [48] and [66].

These results serve as a motivation to find similar connections between Gröbner bases and generalized Sylvester matrices. This topic has been studied by various authors ([47], [49], [50], [45], [36], [61]). Although not intended to compute Gröbner bases as a whole but as an efficient method for solving a system of equations under a special condition, the families of XL ([22, 23, 24]) and later MXL algorithms ([18, 53, 52, 17]) proceed in this linear algebra spirit and have interesting connections with Gröbner bases algorithms ([4, 2]). In his F4 algorithm [31] Faugére uses submatrices of a generalized Sylvester matrix to reduce several S-polynomials at once. His F5 algorithm [32] uses two new criteria based on signatures. Due to these criteria the F5 algorithm does not perform any zero-reductions for a certain class of polynomial systems, called regular sequences, and it is also implemented in the matrix style of F4. By computer experiments Faugére showed that F5 is much faster than previous algorithms. There is a lot of ongoing research in improving the F5 algorithm even further (e.g. [3, 29, 33, 38, 54, 60, 67]). In a similar style as F5 are the algorithms G2V [34] and GVW [35].

However, none of the above papers answers the question of how big a generalized Sylvester matrix should be in order to compute a Gröbner basis by triangularizing this one matrix.

1.2 Outline of the Thesis

In Chapter 2, after introducing the basic notions of Gröbner bases and Sylvester matrices, we investigate the connection between the two. We give a theorem that specifies which shifts of the input polynomials should be put into the Sylvester matrix in order to compute a Gröbner basis by triangularizing this matrix. We also give an upper bound on the size of this matrix. As a special case, we treat the univariate case with more than two input polynomials and give sharper bounds than were previously known in the literature.

In Chapter 3 we investigate the membership problem for binomial ideals and treat the case of two multivariate binomials as a generating set. We give upper bounds on the

degree of the cofactors of a potential element in the reduced Gröbner basis. These bounds are sharper than the ones obtained by the Hermann bound after specializing to the case at hand. We accomplish this by translating the problem to a combinatorial problem.

In Chapter 4 we use the results of Chapter 3 to give an upper bound for the generalized Sylvester matrix for computing a Gröbner basis for certain cases of binomial ideals. Again we treat the case of two multivariate binomials as a generating set. We give sharp bounds for the case where one input binomial is a monomial. We give bounds for the case where both binomials are proper binomials (i.e. their support consists of two terms) and their structure is linearly dependent. We also give bounds for the case where both binomials are proper, their structure is linearly independent and one of the two satisfies a certain property that has to do with the relative position of the terms in the support of the two binomials. These bounds are sharper than the ones derived, by specialization, from the bound in Chapter 2.

Chapter 2

Gröbner Bases Computation by Gaussian Elimination

In [13], [15] and [16] Buchberger proposed to investigate whether it is possible to compute a Gröbner basis of an input set F of polynomials over a field by generating, in a first step, a finite set of shifts of the elements in F (i.e. multiplications of these elements by power products), arranging them in a matrix and, then, triangularizing this matrix.

In this chapter we use results by Hermann and Dubé to give a set of shifts of the input polynomials that depends on the highest degree of the polynomials in F, the number of variables and the number of polynomials in F, for generating such a matrix that suffices for computing a Gröbner basis by triangularization afterwards. We also give a set of shifts to decide in this way whether the system $F = 0$ is solvable or not. This set of shifts is smaller than the set used for Gröbner bases computation.

In Subsection 2.4 we treat the univariate case and give a smaller set of shifts than previously known in the literature. In Chapter 4 we investigate the case of binomial ideals and give degree bounds on the shifts that depend on the support of the input binomials but not on their coefficients.

2.1 Gröbner Bases

Definition 2.1.1 (Admissible order)**.** *A total order $\prec$ on $[X]$ is called* admissible *iff for all $u, v, w \in [X]$*

1. $1 \prec u$

2. *if* $v \prec w$ *then* $u\,v \prec u\,w$.

From now on, we fix an admissible order $\prec$ on $[X]$.

Definition 2.1.2 (Leading term/coefficient/monomial, maxdeg, mindeg)**.** *For any non-zero polynomial* $f \in \mathbb{K}[X]$*, we define the leading term, the leading coefficient and the leading monomial of* f *by* $\mathrm{lt}(f) := \max_\prec(\mathrm{supp}(f))$, $\mathrm{lc}(f) := f(\mathrm{lt}(f))$ *and* $\mathrm{lm}(f) := \mathrm{lc}(f)\,\mathrm{lt}(f)$*, respectively. For a non-empty set* $F \neq \{0\}$ *of polynomials and a subset* U *of* $[X]$ *we define* $\mathrm{lt}(F) := \{\mathrm{lt}(f) \mid f \in F \setminus \{0\}\}$, $U\,F := \{tf \mid t \in U \wedge f \in F\}$ *and, for finite* F, $\mathrm{maxdeg}(F) := \max(\{\deg(f) \mid f \in F \setminus \{0\}\})$ *and* $\mathrm{mindeg}(F) := \min(\{\deg(f) \mid f \in F \setminus \{0\}\})$.

Definition 2.1.3 (Reduction)**.** *Let* $f, g \in \mathbb{K}[X] \setminus \{0\}$ *have the same leading term. The* reduction *of* f *by* g *is defined as* $\mathrm{red}(f, g) = f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)}\,g$.

Definition 2.1.4 (S-polynomial, Polynomial reduction; cf. [9, 10])**.** *Let* $f, f_1, f_2 \in \mathbb{K}[X] \setminus \{0\}$.

1. *The* S-polynomial *of* f_1 *and* f_2 *is defined as*

$$\mathrm{spol}(f_1, f_2) = \mathrm{red}(u_1 f_1, u_2 f_2),$$

   where $u_i = \mathrm{lcm}(\mathrm{lt}(f_1), \mathrm{lt}(f_2))/\,\mathrm{lt}(f_i)$, $i = 1, 2$.

2. *We say* f_1 reduces *by* f_2 *to* h *(and we write* $f_1 \to_{f_2} h$*), if for some term* $u \in \mathrm{supp}(f_1)$, $\mathrm{lt}(f_2)$ *divides* u *and* $h = f_1 - f_1(u)(u/\,\mathrm{lm}(f_2))f_2$*. (If* u *in the definition is the leading term of* f_1*, we say that* f_1 head-reduces *by* f_2 *to* h*.)*
   We say f reduces *to* h *w.r.t. a set of polynomials* F *(written* $f \to_F h$*) if there exists* $h' \in F$ *such that* $f \to_{h'} h$*. For any binary relation* $\to$ *we denote by* $\to^*$ *the reflexive transitive closure of* $\to$.
   The polynomial f *is irreducible w.r.t.* F *iff there is no* $h \in \mathbb{K}[X]$ *such that* $f \to_F h$*. If* $f \to_F^* h$ *and* h *is irreducible w.r.t.* F *then we call* h *a* normal form *of* f *w.r.t.* F.

The relation $\to_F$ is Noetherian (see any textbook on Gröbner bases; e.g. [26]). Therefore, for any $f \in \mathbb{K}[X]$, a normal form of f always exists. However, it does not need to be unique. It turns out, uniqueness is guaranteed, if F is a Gröbner basis. The theory of Gröbner bases was introduced by Buchberger ([9],[10]), the name "Gröbner basis" first appeared in [11]:

Definition 2.1.5 (Gröbner basis)**.** *A set* $G \subseteq \mathbb{K}[X] \setminus \{0\}$ *is a* Gröbner basis *iff it satisfies the following condition:*

$$\textit{For all } u \in \mathrm{lt}(\mathrm{ideal}(G)) \textit{ there exists a } v \in \mathrm{lt}(G) \textit{ such that } v \mid u.$$

We call a Gröbner basis G reduced *iff for every* $g \in G$, $\mathrm{lc}(g) = 1$ *and* g *is irreducible w.r.t.* $G \setminus \{g\}$, *and* head-reduced *iff no* $g \in G$ *can be head-reduced by any polynomial in* $G \setminus \{g\}$. *For a set* $F \subseteq \mathbb{K}[X]$ *we say that* G *is a* (head-/reduced) Gröbner basis of F, *if* G *is a (head-/reduced) Gröbner basis and* $\mathrm{ideal}(G) = \mathrm{ideal}(F)$.

The following are basic facts about Gröbner bases and are contained in any textbook on Gröbner bases (e.g. [26]).

Lemma 2.1.6. *Let* $G \subseteq \mathbb{K}[X]$ *be a Gröbner basis and let* $f, g \in G$, $f \neq g$, *such that* $\mathrm{lt}(g) \mid \mathrm{lt}(f)$. *Then* $G \setminus \{f\}$ *is a Gröbner basis of* G.

Lemma 2.1.7. *Let* $G \subseteq \mathbb{K}[X]$ *be a Gröbner basis and let* $G' \subseteq \mathrm{ideal}(G) \setminus \{0\}$ *be such that* $\mathrm{lt}(G) \subseteq \mathrm{lt}(G')$. *Then* G' *is a Gröbner basis of* G.

Theorem 2.1.8. *Let* $G, G' \subseteq \mathbb{K}[X]$ *be reduced Gröbner bases with* $\mathrm{ideal}(G) = \mathrm{ideal}(G')$. *Then* $G = G'$.

Theorem 2.1.9 (Buchberger [9, 10])**.** *A set* $G \subseteq \mathbb{K}[X] \setminus \{0\}$ *is a Gröbner basis if and only if*

$$\text{for all } f, g \in G,\ \mathrm{spol}(f, g) \to_G^* 0.$$

Algorithm 2.1.10 (Gröbner basis; Buchberger algorithm)**.**
Input: *F, a finite set of non-zero polynomials*
Output: *G, a Gröbner basis for F*
$G \leftarrow F$;
$B \leftarrow \{\{f, g\} \mid f, g \in G, f \neq g\}$;
while $B \neq \emptyset$
  take a pair $\{f, g\}$ *from* B;
  $B \leftarrow B \setminus \{\{f, g\}\}$;
  $h \leftarrow$ *a normal form computed by reduction from* $\mathrm{spol}(f, g)$ *with respect to* G;
  if $h \neq 0$ ***then*** $B \leftarrow B \cup \{\{h, g'\} \mid g' \in G\}$;
    $G \leftarrow G \cup \{h\}$;
  end if;
end while;
Return G;

2.2 Matrices

For a finite, non-empty set $A \subset [X]$ and $f : A \to \mathbb{K}$ we define

$$\mathrm{pol}_A(f) : [X] \ \to \ \mathbb{K},$$

$$t \quad \mapsto \quad \begin{cases} f(t), & \text{if } t \in A, \\ 0, & \text{else,} \end{cases}$$

$$\mathrm{lt}(f) := \mathrm{lt}(pol_A(f))$$

and

$$\mathrm{lc}(f) := f(\mathrm{lt}(f)).$$

Definition 2.2.1 (Matrix)**.** *Let I and $J \subseteq [X]$ be non-empty, finite sets. We call $\mathbb{K}^{I \times J} := \{m : I \times J \to \mathbb{K}\}$ the set of matrices over $\mathbb{K}$ with index sets I and J.*

For $m, m' \in \mathbb{K}^{I \times J}$, we define

$$\begin{aligned} m + m' : I \times J &\to \mathbb{K}, \\ (i,j) &\mapsto m(i,j) + m'(i,j). \end{aligned}$$

For $i \in I$ and $m \in \mathbb{K}^{I \times J}$, we denote the i-th row of m by

$$\begin{aligned} m(i) : J &\to \mathbb{K}, \\ j &\mapsto m(i,j), \end{aligned}$$

and we say that $r : J \to \mathbb{K}$ is a row in m, if there exists an $i' \in I$ such that $r = m(i')$.

Let $m \in \mathbb{K}^{I \times J}$, $c \in \mathbb{K}$ and r, r', r'' be rows in m. We define

$$\begin{aligned} c\,r : J &\to \mathbb{K}, \\ j &\mapsto c\,r(j), \end{aligned}$$

$$\begin{aligned} r' + r'' : J &\to \mathbb{K}, \\ j &\mapsto r'(j) + r''(j). \end{aligned}$$

In the sequel we assume that if F is a finite set, F_i is the i-th element in F in some 1-to-1 enumeration of F.

Definition 2.2.2 ($\mathrm{mat}(F)$)**.** *For finite, non-empty $F \subset \mathbb{K}[X]$ we define*

$$\begin{aligned} \mathrm{mat}(F) : \mathbb{N}_{|F|} \times A &\to \mathbb{K}, \\ (i,t) &\mapsto F_i(t), \end{aligned}$$

where $A = \bigcup_{f \in F} \mathrm{supp}(f)$.

Definition 2.2.3. *Let I and $J \subseteq [X]$ be non-empty, finite sets and $m \in \mathbb{K}^{I\times J}$. We define* $\mathrm{lt}(m) := \{\mathrm{lt}(m(i)) \mid i \in I \text{ and } m(i) \neq 0\}$.

In the next definition we give an exact specification of what we mean by row operations which are well known from linear algebra and are usually defined to be operations on one or two rows of a matrix producing a new row with the implicit understanding that the other rows in the matrix not affected by these operations are not changed. Since the exact understanding of the actions of these operations is crucial for our investigation, in the subsequent definition, we formulate the "row" operations in fact as matrix operations.

Definition 2.2.4 (Row operation)**.** *Let I and $J \subseteq [X]$ be non-empty, finite sets. A* row operation *on a matrix $m \in \mathbb{K}^{I\times J}$ is defined to be one of the following functions that generate from the given matrix a new matrix, where $c, c', c'' \in \mathbb{K} \setminus \{0\}$, and $i', i'' \in I$ with $i' \neq i''$:*

$$\begin{aligned} \mathrm{exchange}(m, i', i'') : I \times J &\to \mathbb{K}, \\ (i,j) &\mapsto \begin{cases} m(i'', j) & \text{if } i = i', \\ m(i', j) & \text{if } i = i'', \\ m(i, j) & \text{else} \end{cases}, \end{aligned} \tag{2.1}$$

$$\begin{aligned} \text{const-multiply}(m, i', c) : I \times J &\to \mathbb{K}, \\ (i,j) &\mapsto \begin{cases} c\, m(i, j) & \text{if } i = i', \\ m(i, j) & \text{else} \end{cases}, \end{aligned} \tag{2.2}$$

$$\begin{aligned} \mathrm{add}(m, i', c', i'', c'') : I \times J &\to \mathbb{K}, \\ (i,j) &\mapsto \begin{cases} c'\, m(i, j) + c''\, m(i'', j) & \text{if } i = i', \\ m(i, j) & \text{else} \end{cases}. \end{aligned} \tag{2.3}$$

Definition 2.2.5 (Triangular matrix, triangularization)**.** *Let I and $J \subseteq [X]$ be non-empty, finite sets. We call a matrix $m \in \mathbb{K}^{I\times J}$* triangular *iff no two rows of m have the same leading term. We say that matrix m'* results by triangularization from *matrix m if m' is triangular and it is obtained from m by a finite sequence of row operations.*

Definition 2.2.6 (Gaussian row operations)**.** *Let I and $J \subseteq [X]$ be non-empty, finite sets and $m \in \mathbb{K}^{I\times J}$. A* Gaussian row operation *on m is defined to be one of the operations (2.1), (2.2) or (2.3) from Defintion 2.2.4, where (2.3) may only be executed if either*

$$\mathrm{add}(m, i', c', i'', c'')(i') \text{ is constant zero}$$

or

$$\mathrm{lt}((\mathrm{add}(m, i', c', i'', c''))(i')) \prec \mathrm{lt}(m(i')).$$

We say that matrix m' results by Gaussian elimination from *matrix* m *if it is obtained from* m *by a finite sequence of Gaussian row operations.*

Remark 2.2.7. *One way to triangularize a matrix is by performing Gaussian elimination. If we consider a matrix* $\mathrm{mat}(F)$ *for some non-empty* $F \subseteq \mathbb{K}[X]$*, then the reduction of a non-zero row* r *by another non-zero row* r'*, where* $\mathrm{lt}(r) = \mathrm{lt}(r')$*, i.e. replacing row* r *by* $\mathrm{red}(r, r') := r - \frac{\mathrm{lc}(r)}{\mathrm{lc}(r')} r'$*, is an example of a row operation.*

Definition 2.2.8 (Reduced row echelon form)**.** *Let* I *and* $J \subseteq [X]$ *be non-empty, finite sets. A matrix* $m \in \mathbb{K}^{I \times J}$ *is in reduced row echelon form iff it is triangular and for all* $i \in I$ *with* $m(i) \neq 0$ *and all* $j \in \mathrm{lt}(m)$*,* $j \neq \mathrm{lt}(m(i))$*,*

$$m(i, \mathrm{lt}(m(i))) = 1 \text{ and } m(i, j) = 0.$$

Consider the following problem.

Problem 2.2.9 (Gcd computation of two univariate polynomials)**.**
Given: *Two polynomials* $f, f' \in \mathbb{K}[x]$ *of degrees* $\deg(f), \deg(f') \geq 1$*.*
Find: *A gcd of* f *and* f'*.*

Definition 2.2.10. *For a univariate polynomial* $h \in \mathbb{K}[x]$ *and a* $k \in \mathbb{N}$ *we define*

$$\mathrm{shifts}(h, k) := \{x^i \, h \mid 0 \leq i \leq k\}.$$

The following theorem was explicitly formulated by Laidacker in [46] but probably could have been deduced from a detailed analysis of Habicht [37]: Problem 2.2.9 can be solved by triangularizing the Sylvester matrix of the two input polynomials.

Theorem 2.2.11 (Laidacker)**.** *Let* $f, f' \in \mathbb{K}[x]$ *of degrees* $\deg(f), \deg(f') \geq 1$*,*

$$S = \mathrm{shifts}(f, \deg(f') - 1) \cup \mathrm{shifts}(f', \deg(f) - 1)$$

and m *be a matrix resulting by triangularization from* $\mathrm{mat}(S)$*.*
Let $A = \{x^i \mid 0 \leq i \leq \deg(f) + \deg(f') - 1\}$*, let* j *be the smallest leading term of* m *and let* $i \in \mathbb{N}_{\deg(f)+\deg(f')}$ *such that* $\mathrm{lt}(m(i)) = j$*. Then* $pol_A(m(i))$ *is a* gcd *of the polynomials* f *and* f'*.*

Corollary 2.2.12. *Let* f*,* f' *and* m *be as in Theorem 2.2.11 and let* g *be a gcd of* f *and* f'*. Then* $\deg(g) = \deg(f) + \deg(f') - \mathrm{rank}(m)$*.*

2.3 Gröbner Bases Computation by Matrix Triangularization

For the remainder of this subsection let $F \subseteq \mathbb{K}[X] \setminus \{0\}$ with $|F| = r$. We want to compute a Gröbner basis of F.

Definition 2.3.1. *(*contour(m)*) Let I and $J \subseteq [X]$ be non-empty, finite sets and $m \in \mathbb{K}^{I \times J}$ a triangular matrix. We define*

$$\begin{aligned}\text{contour}(m) := \{\text{pol}_J(m(i)) \mid i \in I \text{ and } m(i) \neq 0 \text{ and} \\ \text{lt}(m(i')) \text{ does not divide } \text{lt}(m(i)) \text{ for any } i' \in I \setminus \{i\}\}.\end{aligned}$$

Lemma 2.3.2. *Let I and $J \subseteq [X]$ be non-empty, finite sets and $m \in \mathbb{K}^{I \times J}$ a triangular matrix. Furthermore, let $M = \{\text{pol}_J(m(i)) \mid i \in I\}$ and $g \in \text{hull}(M)$. Then $\text{lt}(g) \in \text{lt}(m)$.*

Proof. Since $g \in \text{hull}(M)$, there exist $c_i \in \mathbb{K}$ $(i \in I)$ such that $g = \sum_{i \in I} c_i \, \text{pol}_J(m(i))$. First we observe that for all $i \in I$ such that $\text{lt}(g) \prec \text{lt}(m(i))$ we have $c_i = 0$, because m is triangular. Second we observe that, again because m is triangular, there must exist an $i \in I$ such that $\text{lt}(g) = \text{lt}(m(i))$, hence $\text{lt}(g) \in \text{lt}(m)$. □

Theorem 2.3.3. *Let G be a Gröbner basis of F and let $S \subseteq [X]F$ be finite such that for all $g \in G$ there exist $q_1, \ldots, q_r \in \mathbb{K}[X]$ such that $g = \sum_{i=1}^{r} q_i F_i$ and $\text{supp}(q_i)F_i \subseteq S$ for all $i \in \mathbb{N}_r$. Let m be a matrix resulting by triangularization from $\text{mat}(S)$. Then $\text{contour}(m)$ is a head-reduced Gröbner basis of F.*

Proof. Let $A = \bigcup_{s \in S} \text{supp}(s)$ and $M = \{\text{pol}_A(m(i)) \mid i \in \mathbb{N}_{|S|}\}$. We know $G \subseteq \text{hull}(S) = \text{hull}(M)$. By Lemma 2.3.2, $\text{lt}(G) \subseteq \text{lt}(m)$. Since $M \subseteq \text{ideal}(F)$ we know by Lemma 2.1.7 that $M \setminus \{0\}$ is a Gröbner basis of F and hence by Lemma 2.1.6, $\text{contour}(m)$ is a head-reduced Gröbner basis of F. □

The following theorem is due to Hermann [39] (also see [51] for a corrected proof).

Theorem 2.3.4. *Let $g \in \text{ideal}(F) \setminus \{0\}$ and $d = \text{maxdeg}(F)$. Then there exist $q_1, \ldots, q_r \in \mathbb{K}[X]$ such that*

$$g = \sum_{i=1}^{r} q_i F_i$$

and, if $q_i \neq 0$,

$$\deg(q_i) \leq \deg(g) + \sum_{j=0}^{n-1} (rd)^{2^j}$$

for all $i \in \mathbb{N}_r$.

This theorem can be used to find a candidate set for S as in Theorem 2.3.3 under the assumption that we have a degree bound for the elements in a Gröbner basis. Such a bound was given by Dubé in [28].

Theorem 2.3.5. *Let G be the reduced Gröbner basis of F and $d = \mathrm{maxdeg}(F)$. Then*

$$\deg(g) \leq 2(\frac{d^2}{2} + d)^{2^{n-1}}$$

for all $g \in G$.

Note that this bound holds for every ordering $\prec$. Now we can derive the following two theorems.

Theorem 2.3.6. *Let $d = \mathrm{maxdeg}(F)$ and $d' = 2(\frac{d^2}{2} + d)^{2^{n-1}} + \sum_{j=0}^{n-1}(rd)^{2^j}$. Let furthermore $U = \{t \in [X] : \deg(t) \leq d'\}$ and $S = \bigcup_{i=1}^{r} UF_i$. Let m be a matrix resulting by triangularization from $\mathrm{mat}(S)$. Then $\mathrm{contour}(m)$ is a head-reduced Gröbner basis of F. Moreover, if m is in reduced row echelon form, $\mathrm{contour}(m)$ is the reduced Gröbner basis of F.*

Proof. Let G be the reduced Gröbner basis of F and $g \in G$. By Theorem 2.3.5 we have

$$\deg(g) \leq 2(\frac{d^2}{2} + d)^{2^{n-1}}.$$

By Theorem 2.3.4 there exist $q_1, \ldots, q_r \in \mathbb{K}[X]$ such that $g = \sum_{i=1}^{r} q_i F_i$ and, if $q_i \neq 0$, $\deg(q_i) \leq \deg(g) + \sum_{j=0}^{n-1}(rd)^{2^j} \leq d'$ for all $i \in \mathbb{N}_r$. Therefore, $\mathrm{supp}(q_i) \subseteq U$ for all $i \in \mathbb{N}_r$, hence, $\mathrm{supp}(q_i)F_i \subseteq S$ for all $i \in \mathbb{N}_r$. By Theorem 2.3.3, $\mathrm{contour}(m)$ is a head-reduced Gröbner basis of F.

For the second part of the proof let m be in reduced row echelon form, $A = \bigcup_{s \in S} \mathrm{supp}(s)$ and $M = \{\mathrm{pol}_A(m(i)) \mid i \in \mathbb{N}_{|S|}\}$. We prove $G = \mathrm{contour}(m)$.
Let $g \in G$. We show $g \in \mathrm{contour}(m)$. Since g is head-reduced with respect to $G \setminus \{g\}$, there exists a $g' \in \mathrm{contour}(m)$ such that $\mathrm{lt}(g) = \mathrm{lt}(g')$. Suppose, $g \neq g'$. Note that $\mathrm{lc}(g) = \mathrm{lc}(g') = 1$. Then $g - g' \neq 0$. Let $t = \mathrm{lt}(g - g')$. Since $g, g' \in \mathrm{hull}(M)$, also $g - g' \in \mathrm{hull}(M)$. By Lemma 2.3.2, $t \in \mathrm{lt}(m)$, so there exists an $i \in \mathbb{N}_{|S|}$ such that $\mathrm{lt}(m(i)) = t$. Since g is irreducible with respect to $G \setminus \{g\}$, we know $g(t) = 0$ and since m is in reduced row echelon form, we know $m(i', t) = 0$ for all $i' \in \mathbb{N}_{|S|}$, $i' \neq i$, hence $g'(t) = 0$. This contradicts the assumption that $(g - g')(t) \neq 0$. Therefore, $g = g' \in \mathrm{contour}(m)$. From the definition of contour we easily derive $G = \mathrm{contour}(m)$. □

Theorem 2.3.7. *Let $d = \mathrm{maxdeg}(F)$ and $d'' = \sum_{j=0}^{n-1}(rd)^{2^j}$. Let furthermore $U = \{t \in [X] : \deg(t) \leq d''\}$ and $S = \bigcup_{i=1}^{r} UF_i$. Let m be a matrix resulting by triangularization from $\mathrm{mat}(S)$. Then the polynomial system $F = 0$ is unsolvable if and only if there exists a non-zero row in m with leading term 1.*

Proof. Let $A = \bigcup_{s \in S} \mathrm{supp}(s)$. If there is a row h in m with leading term 1, then $\mathrm{pol}_A(h) \in \mathrm{ideal}(F)$ is a non-zero constant polynomial and hence $F = 0$ is unsolvable.

If $F = 0$ is unsolvable then $\{1\}$ is a Gröbner basis of F. By Theorem 2.3.4, there exist $q_1, \ldots, q_r \in \mathbb{K}[X]$ such that

$$1 = \sum_{i=1}^{r} q_i F_i$$

and, if $q_i \neq 0$,

$$\deg(q_i) \leq \sum_{j=0}^{n-1} (rd)^{2^j}$$

for all $i \in \mathbb{N}_r$. By Theorem 2.3.3 it follows that $\mathrm{contour}(m)$ is a head-reduced Gröbner basis of F. Since $1 \in \mathrm{ideal}(F)$, there exists a $g \in \mathrm{contour}(m)$ such that $\mathrm{lt}(g)$ divides $\mathrm{lt}(1)$. Row $g|_A$ has leading term 1. □

In [45], Kühnle and Mayr use a similar technique for proving that Gröbner bases computations can be done in exponential space. They use systems of linear equations which have a similar structure as the matrix $\mathrm{mat}(S)$ used in Theorem 2.3.6 and by repeatedly solving these systems they get the reduced Gröbner basis of the input set F. For bounding the size as well as the number of these systems they also use the bounds given by Hermann and Dubé. More specifically, they enumerate all terms up to the degree bound given by Dubé and for every such term t and its direct divisors (a term u is a direct divisor of t iff it divides t but there is no term $v \notin \{u, t\}$ such that u divides v and v divides t) they construct a system of linear equations of the form $\mathcal{H} = \mathcal{F}\mathcal{C}$. For describing the structure of this system, let $\prec$ be given by n^2 integer weights bounded by A (for details on this see the paper; note that $A \geq 1$), let $d := \mathrm{maxdeg}(F)$, $N := ((2A(\frac{d^2}{2} + d)^{2^{n-1}} + 1)^n \deg(t))^{n+1}$ and $D := N + (rd)^{2^n}$. Now, the rows of the system are indexed by the terms in $\{u \in [X] : \deg(u) \leq d + D\}$ with increasing degree, $\mathcal{H}$ is the unit vector with 1 as the entry indexed by t, $\mathcal{C}$ is a vector of unknowns, and $\mathcal{F}$ is a matrix with the first $k := |\{u \in [X] : \deg(u) \leq N\}|$ columns being the unit vectors $\mathbf{e}_1, \ldots, \mathbf{e}_k$, i.e. transposed shifts of the polynomial 1 up to degree N, and the following $r|\{u \in [X] : \deg(u) \leq D\}|$ columns being transposed shifts of the input polynomials. The first k entries of the solution vector $\mathcal{C}$ give the coefficients of (not necessarily fully) reduced forms of t with respect to the reduced Gröbner basis of F. A certain minimal solution of the system w.r.t. $\prec$ gives the coefficients of the normal form $\mathrm{NF}(t)$ of t with respect to the reduced Gröbner basis of F. This solution is computed by finding a certain maximal regular minor $\mathcal{F}'$ of $\mathcal{F}$ and computing its inverse matrix. Now, the polynomial $t - \mathrm{NF}(t)$ is added to the intermediate Gröbner basis if it is not 0 and its direct divisors are irreducible, i.e. their normal forms are the same as the direct divisors themselves. In the end, this yields the reduced Gröbner basis of F.

The authors obtain the system $\mathcal{H} = \mathcal{FC}$ by setting up the equation $t - \mathrm{NF}(t) = \sum_{i=1}^{r} c_i F_i$, using a similar argument as we do for deriving the bounds N and D on $t - \mathrm{NF}(t)$ and the c_i, and then comparing coefficients. For deriving N, the authors use Dubé's bound $2(\frac{d^2}{2}+d)^{2^{n-1}}$, and D is the combination of N and Hermann's bound $\sum_{j=0}^{n-1}(rd)^{2^j} \leq (rd)^{2^n}$. Note that in the smallest case ($\deg(t) = 0$) the input polynomials are shifted up to degree $d + (rd)^{2^n}$, already in the case $\deg(t) = 1$ they are shifted up to degree $d + ((2A(\frac{d^2}{2}+d)^{2^{n-1}}+1)^n)^{n+1} + (rd)^{2^n} >> d + d'$ with d' as in Theorem 2.3.6 and in the biggest case ($\deg(t) = 2(\frac{d^2}{2}+d)^{2^{n-1}}$) they are shifted up to degree

$$d + ((2A(\frac{d^2}{2}+d)^{2^{n-1}}+1)^n\, 2(\frac{d^2}{2}+d)^{2^{n-1}})^{n+1} + (rd)^{2^n} >> d + d'.$$

Additionally to these shifts, the matrix $\mathcal{F}$ contains shifts of the polynomial 1 up to degree N. The number of systems to be solved in this way is at least $|\{u \in [X] : \deg(u) \leq 2(\frac{d^2}{2}+d)^{2^{n-1}}\}|$. In this thesis, in contrast, we build one matrix consisting of shifts of the input polynomials up to degree $d + d'$, triangularize this matrix and extract its contour as a head-reduced Gröbner basis of F. We do not make any claims about the size of the space needed for Gröbner bases computations but solve a different problem. Although the matrices in Kühnle and Mayr are similar to the matrix of shifts we are using, we do not see how the proof in Kühnle and Mayr could be used for showing that the matrices used in Kühnle and Mayr solve our problem and, also, our proof for the bounds for our problem is much shorter. Additionally, their matrix $\mathcal{F}$ is much bigger than ours in every case except the case $\deg(t) = 0$. However, for solving their systems of linear equations they avoid using the whole matrix $\mathcal{F}$ by computing a certain maximal regular minor $\mathcal{F}'$ and using this one instead.

For more recent results on the problem investigated by Kühnle and Mayr see Ritscher's PhD thesis [55].

2.4 GCD Computation of Several Univariate Polynomials

We consider the following problem.

Problem 2.4.1 (Gcd computation of several univariate polynomials)**.**
Given: *$F \in \mathbb{K}[x] \setminus \{0\}$ such that $|F| = r \geq 2$, with* $\mathrm{mindeg}(F) \geq 1$.
Find: *A gcd of F.*

Let $d := \mathrm{maxdeg}(F)$ and $d' := \mathrm{maxdeg}(F \setminus \{f\})$, where $f \in F$ is such that $\deg(f) = d$, and let $d'' := \mathrm{mindeg}(F)$. In [65] and [5] direct generalizations of the Sylvester matrix to the case of r univariate polynomials with $r \geq 2$ are given. In [65] the block size (i.e.

the number of shifts) for every polynomial is d, resulting in a $d\,r \times 2d$ matrix. In [5] the block size of one of the polynomials with degree d is d' and the block sizes of all of the other polynomials are d, resulting in a $(d' + (r-1)d) \times (d + d')$ matrix. As can been seen in Theorem 2.4.4, our block sizes are d for a polynomial with smallest degree d'' and d'' for the other polynomials, resulting in a $(d + (r-1)d'') \times (d + d'')$ matrix. Since

$$2d \geq d + d' \geq d + d''$$

and

$$\begin{aligned} d\,r &\geq d' + (r-1)d = d + d' + (r-2)d \\ &\geq d + d'' + (r-2)d'' = d + (r-1)d'', \end{aligned}$$

the matrix given in this thesis is smaller and it is equal to the other two if and only if all of the polynomials have the same degree. The difference is of course not big if the degrees are very close to each other. For example if $r = 10$, $d = 30$, $d' = 29$ and $d'' = 27$, we get a 300×60 matrix with [65], a 299×59 matrix with [5] and a 273×57 matrix using our block sizes. But if the degrees are not close to each other, the difference is significant. For example if $r = 10$, $d = 50$, $d' = 35$ and $d'' = 7$, we get a 500×100 matrix with [65], a 485×85 matrix with [5] and a 113×57 matrix using our block sizes.

Definition 2.4.2. *Let $P \subseteq \mathbb{K}[x] \setminus \{0\}$ be a non-empty set with $\operatorname{mindeg}(P) \geq 1$, and let $p \in P$. Then define*

$$\operatorname{Sylv}(P, p) := \left(\bigcup_{h \in P \setminus \{p\}} \operatorname{shifts}(h, \operatorname{mindeg}(P) - 1) \right) \cup \operatorname{shifts}(p, \operatorname{maxdeg}(P) - 1).$$

Lemma 2.4.3. *Let $f \in F$ such that $\deg(f) = \operatorname{mindeg}(F)$ and g be a gcd of F. Then $g \in \operatorname{hull}(\operatorname{Sylv}(F, f))$ and $x^i \in \operatorname{lt}(\operatorname{hull}(\operatorname{Sylv}(F, f)))$ for any i such that $\deg(g) \leq i \leq \operatorname{maxdeg}(F) + \operatorname{mindeg}(F)$*

Proof. We proceed by induction on $|F|$. For $|F| = 2$, the claim follows by Theorem 2.2.11 and Corollary 2.2.12.
Now fix $r > 1$. Take F with $|F| = r+1$, let $f \in F$ such that $\deg(f) = \operatorname{mindeg}(F)$, g be a gcd of F and assume (induction hypothesis) that for all $\tilde{F}$ with $|\tilde{F}| \leq r$ and for all $\tilde{f} \in \tilde{F}$ such that $\deg(\tilde{f}) = \operatorname{mindeg}(\tilde{F})$ and for any gcd $\tilde{g}$ of $\tilde{F}$ we have $\tilde{g} \in \operatorname{hull}(\operatorname{Sylv}(\tilde{F}, \tilde{f}))$ and $x^i \in \operatorname{lt}(\operatorname{hull}(\operatorname{Sylv}(\tilde{F}, \tilde{f})))$ for any i such that $\deg(\tilde{g}) \leq i \leq \operatorname{maxdeg}(\tilde{F}) + \operatorname{mindeg}(\tilde{F})$.
Let $f' \in F \setminus \{f\}$ such that $\deg(f') = \operatorname{mindeg}(F \setminus \{f\})$ and let g' be a gcd of $F \setminus \{f'\}$. Note that $\operatorname{maxdeg}(F \setminus \{f'\}) = \operatorname{maxdeg}(F)$ and $\operatorname{mindeg}(F \setminus \{f'\}) = \operatorname{mindeg}(F)$. By the induction hypothesis,

$$g' \in \operatorname{hull}(\operatorname{Sylv}(F \setminus \{f'\}, f)) \tag{2.4}$$

and

$$x^i \in \mathrm{lt}(\mathrm{hull}(\mathrm{Sylv}(F \setminus \{f'\}, f))) \text{ for any } i \text{ such that } \deg(g') \leq i \leq \mathrm{maxdeg}(F) + \mathrm{mindeg}(F). \tag{2.5}$$

The polynomial g is a gcd of g' and f'. Note that $\deg(g') \leq \deg(f) \leq \deg(f')$, so again by the induction hypothesis,

$$g \in \mathrm{hull}(\mathrm{Sylv}(\{f', g'\}, g')) \tag{2.6}$$

and

$$x^i \in \mathrm{lt}(\mathrm{hull}(\mathrm{Sylv}(\{f', g'\}, g'))) \text{ for any } i \text{ such that } \deg(g) \leq i \leq \deg(f') + \deg(g'). \tag{2.7}$$

In order to prove $g \in \mathrm{hull}(\mathrm{Sylv}(F, f))$, it suffices by (2.6) to show that $\mathrm{hull}(\mathrm{Sylv}(\{f', g'\}, g')) \subseteq \mathrm{hull}(\mathrm{Sylv}(F, f))$. For this we have to prove that

$$\mathrm{shifts}(f', \deg(g') - 1) \subseteq \mathrm{hull}(\mathrm{Sylv}(F, f))$$

and

$$\mathrm{shifts}(g', \deg(f') - 1) \subseteq \mathrm{hull}(\mathrm{Sylv}(F, f)).$$

Since $\deg(g') - 1 \leq \mathrm{mindeg}(F) - 1$, it immediately follows that

$$\mathrm{shifts}(f', \deg(g') - 1) \subseteq \mathrm{hull}(\mathrm{Sylv}(F, f)).$$

So we now show $\mathrm{shifts}(g', \deg(f') - 1) \subseteq \mathrm{hull}(\mathrm{Sylv}(F, f))$. We have

$$\mathrm{hull}(\mathrm{Sylv}(F \setminus \{f'\}, f)) \subseteq \mathrm{hull}(\mathrm{Sylv}(F, f)), \tag{2.8}$$

because the set $\mathrm{Sylv}(F \setminus \{f'\}, f)$ can be rewritten as

$$\begin{aligned}
&\mathrm{Sylv}(F \setminus \{f'\}, f) = \\
&\quad = \left(\bigcup_{h \in F \setminus \{f, f'\}} \mathrm{shifts}(h, \mathrm{mindeg}(F \setminus \{f'\}) - 1) \right) \cup \mathrm{shifts}(f, \mathrm{maxdeg}(F \setminus \{f'\}) - 1) \\
&\quad = \left(\bigcup_{h \in F \setminus \{f, f'\}} \mathrm{shifts}(h, \mathrm{mindeg}(F) - 1) \right) \cup \mathrm{shifts}(f, \mathrm{maxdeg}(F) - 1).
\end{aligned}$$

So it suffices to prove that

$$\mathrm{shifts}(g', \deg(f') - 1) \subseteq \mathrm{hull}(\mathrm{Sylv}(F \setminus \{f'\}, f)).$$

Let $k \in \mathbb{N}_{\deg(f')-1}$. We show $x^k g' \in \text{hull}(\text{Sylv}(F \setminus \{f'\}, f))$ in two steps. First, we show that there exists an $h \in \text{hull}(\text{Sylv}(F \setminus \{f'\}, f))$ which has the same coefficients as $x^k g'$ with respect to the terms of degree $\deg(g')$ and higher. Second, we show complete equality of h and $x^k g'$. Since $\deg(g') \leq \text{mindeg}(F)$, and $k \leq \text{maxdeg}(F) - 1$ it follows that

$$\deg(g') \leq \deg(x^k g') \leq \text{maxdeg}(F) + \text{mindeg}(F) - 1.$$

By (2.5) for any i such that $\deg(g') \leq i \leq \text{maxdeg}(F) + \text{mindeg}(F)$ there is a $p \in \text{hull}(\text{Sylv}(F \setminus \{f'\}, f))$ such that $\text{lt}(p) = x^i$. So there exists an $h \in \text{hull}(\text{Sylv}(F \setminus \{f'\}, f))$ such that

$$h(x^j) = (x^k g')(x^j)$$

for all j such that $\deg(g') \leq j \leq \text{maxdeg}(F) + \text{mindeg}(F) - 1$. If $h \neq x^k g'$, then there exists a $j \in \mathbb{N}_{\deg(g')-1}$ such that $h(x^j) \neq (x^k g')(x^j)$. But then we have that

$$h - x^k g' \in \text{ideal}(F \setminus \{f'\}) \setminus \{0\}$$

and

$$\deg(h - x^k g') < \deg(g'),$$

which contradicts the fact that g' is a gcd of $F \setminus \{f'\}$. So in fact,

$$x^k g' = h \in \text{hull}(\text{Sylv}(F \setminus \{f'\}, f))$$

and we get

$$\text{shifts}(g', \deg(f') - 1) \subseteq \text{hull}(\text{Sylv}(F \setminus \{f'\}, f)) \subseteq \text{hull}(\text{Sylv}(F, f)).$$

Altogether we obtain

$$g \in \text{hull}(\text{Sylv}(\{f', g'\}, g')) \subseteq \text{hull}(\text{Sylv}(F, f)). \tag{2.9}$$

Now we show $x^i \in \text{lt}(\text{hull}(\text{Sylv}(F, f)))$ for any i such that $\deg(g) \leq i \leq \text{maxdeg}(F) + \text{mindeg}(F)$. By (2.7) and (2.9) we obtain $x^i \in \text{lt}(\text{hull}(\text{Sylv}(F, f)))$ for any i such that $\deg(g) \leq i \leq \deg(f') + \deg(g')$. By (2.5) and (2.8) we obtain $x^i \in \text{lt}(\text{hull}(\text{Sylv}(F, f)))$ for any i such that $\deg(g') \leq i \leq \text{maxdeg}(F) + \text{mindeg}(F)$. Since $\deg(f') + \deg(g') \geq \deg(g')$, this proves the claim. □

Theorem 2.4.4. *Let $f \in F$ such that $\deg(f) = \text{mindeg}(F)$ and let m be a matrix resulting by triangularization from $\text{mat}(\text{Sylv}(F, f))$.*
Then $\text{contour}(m)$ contains only one element, which is a gcd of F.

Proof. Let g be a gcd of F. By Lemma 2.4.3, $g \in \text{hull}(\text{Sylv}(F, f))$. We derive that $\text{Sylv}(F, f) \subseteq [X]F$ is such that there exist $q_1, \ldots, q_r \in \mathbb{K}[x]$ such that $g = \sum_{j=1}^{r} q_j F_j$

and $\mathrm{supp}(q_j)F_j \subseteq \mathrm{Sylv}(F, f)$ for all $j \in \mathbb{N}_r$. Hence, by Theorem 2.3.3, $\mathrm{contour}(m)$ is a head-reduced Gröbner basis of F, i.e. it consists of a gcd of F. □

As in the case $r = 2$, we can infer the following two corollaries.

Corollary 2.4.5. *Let $f \in F$ such that $\deg(f) = \mathrm{mindeg}(F)$ and let g be a gcd of F. Then $\deg(g) = \mathrm{maxdeg}(F) + \mathrm{mindeg}(F) - \mathrm{rank}(\mathrm{mat}(\mathrm{Sylv}(F, f)))$.*

Proof. The claim follows immediately from Theorem 2.4.4, Lemma 2.4.3 and Lemma 2.3.2. □

Corollary 2.4.6. *Let $f \in F$ such that $\deg(f) = \mathrm{mindeg}(F)$ and let g be a gcd of F. The polynomials in F are co-prime, i.e. the degree of their gcd is 0, if and only if $\mathrm{rank}(\mathrm{mat}(\mathrm{Sylv}(F, f))) = \mathrm{maxdeg}(F) + \mathrm{mindeg}(F)$.*

Proof. The claim follows immediately from Corollary 2.4.5. □

Chapter 3

New Bounds for the Membership Problem for Binomial Ideals

3.1 Introduction and Summary of the Main Results

In this and the following chapter we investigate the case of binomial ideals, where the input basis consists of two binomials. Binomial ideals arise in many interesting problems in different fields, for example integer programming (e.g. [21, 1, 63, 64, 40, 58, 25]; for a general introduction to linear and integer programming, see [56]), computational statistics ([27]) and dynamical systems (e.g. [41]). Toric ideals are the pure difference prime binomial ideals, where a pure difference binomial is a binomial of the form $X^\alpha - X^\beta$. There is a large amount of literature studying toric ideals (e.g. [57, 58, 6]). For more literature on binomial ideals see e.g. [30, 42, 43, 44, 59].

We want to find an upper degree bound for the shifts of the input polynomials needed to compute a Gröbner basis the way described in the last chapter for the case, where the input polynomials are two binomials. For this, we solve in this chapter the subproblem of finding an upper bound on the shifts of the two input binomials needed to compute a particular given element of a Gröbner basis.

In this subsection we give a summary of the main results in this chapter. The proofs follow in Subsections 3.2 and 3.3.

Definition 3.1.1 (Binomial)**.** *A polynomial $f \in \mathbb{K}[X] \setminus \{0\}$ is a* binomial *iff $|\operatorname{supp}(f)| \leq 2$. If $|\operatorname{supp}(f)| = 2$, we call f a* proper binomial*.*

Definition 3.1.2 (Binomial ideal)**.** *An ideal is a binomial ideal if it is generated by a set of binomials.*

Note the following basic fact (see for example [30]).

Theorem 3.1.3. *For a set H of binomials, the reduced Gröbner basis of H is a set of binomials.*

For the rest of the thesis we denote by F the set of input polynomials and assume that it consists of two binomials.

Remark 3.1.4. *Since we want to generate a Gröbner basis, we have to have the necessary shifts to generate, by linear combinations, enough polynomials such that their leading terms include all the terms in* $\mathrm{lt}(G)$*. If there is a* $g \in G$ *such that* $\mathrm{lt}(g) \in \mathrm{lt}(F)$*, then* $\mathrm{lt}(g)$ *is already taken care of since the polynomials in* F *will be contained in the shifts. Hence, such a* g *needs not to be considered for our investigation of how big the shifts should get. The ones that are interesting are the* $g \in G$ *with* $\mathrm{lt}(g) \notin \mathrm{lt}(F)$*. The reduced Gröbner basis* G *of* F *has the property that it contains only binomials (c.f. Theorem 3.1.3) and that for every* g *in* G*,* g *is irreducible with respect to* $G \setminus \{g\}$*. From this follow the weaker properties that for every* $g \in G$ *with* $\mathrm{lt}(g) \notin \mathrm{lt}(F)$*,* g *is irreducible with respect to* F *and, if* g *is a proper binomial,* $\mathrm{supp}(g) \not\subseteq \mathrm{ideal}(F)$*. Therefore, it suffices if for our investigation we only consider those* $g \in \mathrm{ideal}(F)$ *which are binomials, are irreducible with respect to* F *and, if* g *is a proper binomial,* $\mathrm{supp}(g) \not\subseteq \mathrm{ideal}(F)$*.*

If F contains only monomials, then F already is a Gröbner basis. For the other cases we analyze the following problem.

Problem 3.1.5.
Find an explicit expression d' *in six terms such that for all* $F, g, r, r', s, s', t, t'$

if $\mathrm{supp}(F_1) \subseteq \{r, r'\}$, $\mathrm{supp}(F_2) \subseteq \{s, s'\}$, $\mathrm{supp}(g) \subseteq \{t, t'\}$, $g \in \mathrm{ideal}(F)$*,* g *is irreducible with respect to* F *and, if* g *is a proper binomial,* $\mathrm{supp}(g) \not\subseteq \mathrm{ideal}(F)$*,*

then *there exist* $q_1, q_2 \in \mathbb{K}[X]$ *such that* $g = q_1F_1 + q_2F_2$ *and, if* $q_i \neq 0$*,* $\deg(q_iF_i) \leq d'(r, r', s, s', t, t')$ *for all* $i = 1, 2$*.*

Note that with this we want to improve the Hermann part of the bound in Theorem 2.3.6.

Let for the rest of this chapter g be a binomial such that $g \in \mathrm{ideal}(F)$, g is irreducible with respect to F and, if g is a proper binomial, $\mathrm{supp}(g) \not\subseteq \mathrm{ideal}(F)$.

Definition 3.1.6 (Trailing term, trailing coefficient, trailing monomial)**.** *For any binomial* $f \in \mathbb{K}[X]$*, we define the* trailing term*,* trailing coefficient *and* trailing monomial *of* f *by* $\mathrm{tt}(f) := \min_{\prec}(\mathrm{supp}(f))$*,* $\mathrm{tc}(f) := f(\mathrm{tt}(f))$ *and* $\mathrm{lm}(f) := \mathrm{tc}(f)\,\mathrm{tt}(f)$*, respectively. For any set* H *of binomials we define* $\mathrm{tt}(H) := \{\mathrm{tt}(h) \mid h \in H\}$*.*

If f is a monomial, then $\mathrm{lm}(f) = \mathrm{tm}(f)$.

Remark 3.1.7. *Since g is irreducible with respect to F, it follows for any $t \in \mathrm{supp}(g)$ that $\mathrm{lt}(f)$ does not divide t for any $f \in F$, but $\mathrm{tt}(f)$ divides t for some $f \in F$.*

Before we summarize our main results we need a few definitions.

Definition 3.1.8 ($\mathrm{e}(t)$)**.** *For any term $t \in [X]$, we define $\mathrm{e}(t)$ to be the exponent vector of t. The function $\mathrm{e} : [X] \to \mathbb{N}^n$ is bijective. For any set $T \subseteq [X]$, we define $\mathrm{e}(T) := \{\mathrm{e}(t) \mid t \in T\}$.*

Definition 3.1.9 (Degree of a point)**.** *The degree of an $A \in \mathbb{Z}^n$ is the sum of its components. For a finite $U \subseteq \mathbb{Z}^n$ we define $\mathrm{maxdeg}(U) := \max(\{\deg(A) \mid A \in U\})$ and $\mathrm{mindeg}(U) := \min(\{\deg(A) \mid A \in U\})$.*

Definition 3.1.10 (gcd, lcm, $\leq$)**.** *For $A, B \in \mathbb{N}^n$ we define*

$$\gcd(A, B) := \mathrm{e}(\gcd(\mathrm{e}^{-1}(A), \mathrm{e}^{-1}(B))),$$

$$\mathrm{lcm}(A, B) := \mathrm{e}(\mathrm{lcm}(\mathrm{e}^{-1}(A), \mathrm{e}^{-1}(B)))$$

and

$$A \leq B \text{ (or } B \geq A \text{ respectively) iff } A_i \leq B_i \text{ for all } i \in \mathbb{N}_n.$$

Definition 3.1.11 ($\mathrm{overlap}(H)$)**.** *Let H be a set of two binomials in $\mathbb{K}[X]$. We define $\mathrm{overlap}(H) := \mathrm{lcm}(\xi^{(1)}, \xi^{(2)})$, where $\xi^{(i)} = \gcd(\mathrm{e}(\mathrm{lt}(H_i)), \mathrm{e}(\mathrm{tt}(H_i)))$ for $i = 1, 2$.*

Definition 3.1.12 ($\mathrm{vect}(h)$)**.** *For a proper binomial $h \in \mathbb{K}[X]$, we define*

$$\mathrm{vect}(h) := \mathrm{e}(\mathrm{lt}(h)) - \mathrm{e}(\mathrm{tt}(h)).$$

Lemma 3.1.13. *Let $P \in \mathbb{N}^n$ such that $\mathrm{e}(\mathrm{tt}(F_1)) \leq P$ and $\mathrm{e}(\mathrm{tt}(F_2)) \leq P$. Then $P \geq \mathrm{overlap}(F)$.*

Proof. We have $\gcd(\mathrm{e}(\mathrm{lt}(F_i)), \mathrm{e}(\mathrm{tt}(F_i))) \leq P$ for all $i = 1, 2$, and hence $P \geq \mathrm{overlap}(F)$. □

Definition 3.1.14 ($\mathrm{step}(P)$, $\mathrm{overlapshift}(P)$)**.** *For a $P \in \mathbb{N}^n$ with $\mathrm{e}(\mathrm{tt}(f)) \leq P$ for a proper binomial $f \in F$, we define $\mathrm{step}(P)$ and $\mathrm{overlapshift}(P)$ the following way.*

Take a proper binomial $f \in F$ such that $\mathrm{e}(\mathrm{tt}(f)) \leq P$. Which one does not matter (see below). Then

$$\mathrm{step}(P) := \max\left(\left\{\left\lceil \frac{\mathrm{overlap}(F)_j - P_j}{\mathrm{vect}(f)_j} \right\rceil \mid j \in \mathbb{N}_n, \mathrm{vect}(f)_j \neq 0, \mathrm{overlap}(F)_j > P_j\right\} \cup \{0\}\right)$$

and

$$\text{overlapshift}(P) := P + \text{step}(P)\,\text{vect}(f).$$

The choice of f does not matter, because if both F_1 and F_2 are suitable choices for f, then by Lemma 3.1.13 we have $P \geq \text{overlap}(F)$ and hence $\text{step}(P) = 0$ and $\text{overlapshift}(P) = P$, no matter the choice.

We now summarize our main results by distinguishing three cases and give some examples.

Case 1: F consists of a proper binomial and a monomial (c.f. Theorem 3.2.1).
Then g is a monomial and $d' = \text{maxdeg}(\text{e}(\text{lt}(g)), \text{overlapshift}(\text{e}(\text{lt}(g))))$ solves Problem 3.1.5 and is optimal among all the solutions.

Example 3.1.15. *Suppose $F = \{X_1^5X_2 + 2X_1^3, 4X_2^5\}$ and $g = X_1^4$ and assume the terms are ordered with respect to the lexicographic ordering with $X_2 \prec X_1$. We have that $g \in \text{ideal}(F)$ and g is irreducible with respect to F. We obtain $\text{e}(\text{lt}(g)) = (4,0)$, $\text{vect}(F_1) = (2,1)$, $\text{overlap}(F) = (3,5)$, $\text{step}(\text{e}(\text{lt}(g))) = 5$, $\text{overlapshift}(\text{e}(\text{lt}(g))) = (14,5)$ and hence the optimal $d' = \text{maxdeg}((4,0),(14,5)) = 19$. Using the Hermann bound in Theorem 2.3.4 we get 166 as an upper degree bound on the shifts necessary to generate g.*

Example 3.1.16. *Suppose $F = \{X_1X_2X_3^5 + 3X_1^3X_2^2, 2X_3^7\}$ and $g = X_1^5X_2^3$ and assume the terms are ordered with respect to the degree lexicographic ordering with $X_3 \prec X_2 \prec X_1$. We have that $g \in \text{ideal}(F)$ and g is irreducible with respect to F. We obtain $\text{e}(\text{lt}(g)) = (5,3,0)$, $\text{vect}(F_1) = (-2,-1,5)$, $\text{overlap}(F) = (1,1,7)$, $\text{step}(\text{e}(\text{lt}(g))) = 2$, $\text{overlapshift}(\text{e}(\text{lt}(g))) = (1,1,10)$ and hence the optimal $d' = \text{maxdeg}((5,3,0),(1,1,10)) = 12$. Using the Hermann bound in Theorem 2.3.4 we get 38641 as an upper degree bound on the shifts necessary to generate g.*

Case 2: F consists of two proper binomials f, f' such that $r\,\text{vect}(f) = \text{vect}(f')$ for some $r \in \mathbb{Q} \setminus \{0\}$ and g is a monomial (c.f. Theorem 3.2.2).
Then $d' = \text{maxdeg}(\text{e}(\text{lt}(g)), \text{overlapshift}(\text{e}(\text{lt}(g))) + \text{vect}(f) + \text{vect}(f'))$ solves Problem 3.1.5.

Example 3.1.17. *Suppose $F = \{X_1^6X_2^8 + 5X_1^2X_2^{10}, 3X_1^{11} - 2X_1^5X_2^3\}$ and $g = X_1^2X_2^{15}$ and assume the terms are ordered with respect to the lexicographic ordering with $X_2 \prec X_1$. We have that $g \in \text{ideal}(F)$ and g is irreducible with respect to F. We obtain $\text{e}(\text{lt}(g)) = (2,15)$, $\text{vect}(F_1) = (4,-2)$, $\text{vect}(F_2) = (6,-3)$, $\text{overlap}(F) = (5,8)$, $\text{step}(\text{e}(\text{lt}(g))) = 1$, $\text{overlapshift}(\text{e}(\text{lt}(g))) = (6,13)$ and hence*

$$\begin{aligned} d' &= \text{maxdeg}((2,15),\,(6,13) + (4,-2) + (6,-3)) \\ &= \text{maxdeg}((2,15),\,(16,8)) = 24. \end{aligned}$$

Using the Hermann bound in Theorem 2.3.4 we get 843 *as an upper degree bound on the shifts necessary to generate* g *and the optimal bound is* 23*.*

Case 3: F consists of two proper binomials f, f' and g is a proper binomial (c.f. Theorem 3.3.35).
Let $A = \mathrm{e}(\mathrm{lt}(g))$, $B = \mathrm{e}(\mathrm{tt}(g))$ and $m = |\deg(\mathrm{vect}(f))| + |\deg(\mathrm{vect}(f'))|$. Then $d' = \max(\mathrm{maxdeg}(A, B), \mathrm{maxdeg}(\mathrm{overlapshift}(A), \mathrm{overlapshift}(B)) + m)$ solves Problem 3.1.5.

Example 3.1.18. *Consider* $F = \{X_1^2X_2^3 - X_2^4, X_1^6 - X_1^3X_2^2\}$ *and* $g = X_2^7 - X_2^6$ *and assume the terms are ordered with respect to the lexicographic ordering with* $X_2 \prec X_1$*. We have that* $g \in \mathrm{ideal}(F)$*,* g *is irreducible with respect to* F *and* $\mathrm{supp}(g) \not\subseteq \mathrm{ideal}(F)$*. Let* $A = (0, 7)$ *and* $B = (0, 6)$*. We calculate* $\mathrm{overlap}(F) = (3, 3)$*,* $\mathrm{vect}(F_1) = (2, -1)$*,* $\mathrm{vect}(F_2) = (3, -2)$*,* $\mathrm{overlapshift}(A) = A + 2\,\mathrm{vect}(F_1) = (4, 5)$ *and* $\mathrm{overlapshift}(B) = B + 2\,\mathrm{vect}(F_1) = (4, 4)$*. We obtain* $d' = \max(7, 9 + 1 + 1) = 11$ *as a solution for Problem 3.1.5. Using the Hermann bound in Theorem 2.3.4 we get* 169 *as an upper degree bound on the shifts necessary to generate* g *and the optimal bound is* 10*.*

Section 3.2 treats the case where g is a monomial, Section 3.3 the case where g is a proper binomial.

3.2 Degree Bounds on the Shifts for Generating a Monomial in a Gröbner Basis

Theorems 3.2.1 and 3.2.2 treat all the possible structures for F where it is possible for g to be a monomial and give expressions for d' of Problem 3.1.5.

Note that k as described in Theorems 3.2.1 and 3.2.2 is the value we receive if we apply the step function defined in Definition 3.1.14 to the exponent vector of $\mathrm{lt}(g)$. There the function is given in a closed form, whereas in this section k is given in implicit form. Also note that in Theorems 3.2.1 and 3.2.2 and in their proofs there occur expressions of the form $t\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^i$ or $t\left(\frac{\mathrm{lm}(f)}{\mathrm{tm}(f)}\right)^i$ for some monomial t and $i \in \mathbb{Q}$. In these cases, $\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^i$ resp. $\left(\frac{\mathrm{lm}(f)}{\mathrm{tm}(f)}\right)^i$ need not be monomials but can rather have negative integer exponents. However, the whole expression $t\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^i$ resp. $t\left(\frac{\mathrm{lm}(f)}{\mathrm{tm}(f)}\right)^i$ is a monomial.

Theorem 3.2.1. *Let F contain a proper binomial f and a monomial f'. Then g is a monomial and there exists a $k \in \mathbb{N} \setminus \{0\}$ such that f' divides $g\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^k$. Let k be minimal with this property. Then*

$$d' = \mathrm{maxdeg}\left(g,\, g\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^k\right)$$

solves Problem 3.1.5 and is optimal among all the solutions.

Proof. It is easy to see that g is a monomial that is divided by $\mathrm{tt}(f)$. The existence of k is a necessary condition for g to be generated by both f and f'. So if k did not exist, then g would be generated by f alone, which contradicts the fact that g is a monomial. We can write g as

$$g = qf + q'f',$$

where

$$q = \frac{g}{\mathrm{tm}(f)}\left(\sum_{i=0}^{k-1}\left(-\frac{\mathrm{lm}(f)}{\mathrm{tm}(f)}\right)^i\right) \in \mathbb{K}[X] \setminus \{0\},$$

$$q' = \frac{g\left(-\frac{\mathrm{lm}(f)}{\mathrm{tm}(f)}\right)^k}{f'} \in \mathbb{K}[X] \setminus \{0\}$$

and k is as in the theorem. We obtain

$$\begin{aligned} \deg(q'f') &\leq \deg(qf) \\ &= \mathrm{maxdeg}\left(g,\, g\left(\frac{\mathrm{lm}(f)}{\mathrm{tm}(f)}\right)^k\right) \\ &= d' \end{aligned} \tag{3.1}$$

Note that by choosing k minimally, q and q' are such that their degree is minimal among all the possible cofactors of g with respect to F. With this and (3.1) we obtain that d' is optimal among the solutions of Problem 3.1.5. □

Theorem 3.2.2. *Let F consist of two proper binomials f, f' such that*

$$\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^m = \left(\frac{\mathrm{lt}(f')}{\mathrm{tt}(f')}\right)^{m'}$$

for some $m, m' \in \mathbb{N} \setminus \{0\}$. Assume, g is a monomial and $\mathrm{tt}(f)$ divides g. There exists a $k \in \mathbb{N}$ such that $\gcd(\mathrm{lt}(f'), \mathrm{tt}(f'))$ divides $g\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^k$. Let k be minimal with this property. Then

$$d' = \mathrm{maxdeg}\left(g,\, g\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^{k+1}\left(\frac{\mathrm{lt}(f')}{\mathrm{tt}(f')}\right)\right),$$

solves Problem 3.1.5.

Proof. Let k be as in the theorem. If k did not exist, then g would be generated by f alone, which contradicts the assumption that g is a monomial. Let $q, q' \in \mathbb{K}[X]$ such that $g = qf + q'f'$. Note that $q, q' \neq 0$, since otherwise g cannot be a monomial. For all $\xi \in \operatorname{supp}(qf) \cup \operatorname{supp}(q'f')$ we obtain $\xi = \operatorname{lt}(g)\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^l$ for a nonnegative $l \in \mathbb{Q}$. If $\deg(\operatorname{lt}(f)) \leq \deg(\operatorname{tt}(f))$, we get $\deg(qf) \leq \deg(g) = d'$ and $\deg(q'f') \leq \deg(g) = d'$.

Now let us assume that $\deg(\operatorname{lt}(f)) > \deg(\operatorname{tt}(f))$. Since $\operatorname{lt}(qf) = \operatorname{lt}(q'f')$ it follows that

$$\deg(qf) = \deg(\operatorname{lt}(qf)) = \deg(\operatorname{lt}(q'f')) = \deg(q'f').$$

We can assume q, q' to be chosen in such a way that $\deg(qf) = \deg(q'f')$ is minimal. We show

$$\deg(qf) \leq \deg\left(g\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{k+1}\left(\frac{\operatorname{lt}(f')}{\operatorname{tt}(f')}\right)\right) = d'.$$

Assume for a contradiction, $\deg(qf) > \deg\left(g\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{k+1}\left(\frac{\operatorname{lt}(f')}{\operatorname{tt}(f')}\right)\right)$. Then there exists an $l' \in \mathbb{Q}$ such that $\operatorname{lt}(qf) = \operatorname{lt}(g)\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{l'}$ and $l' > k + 1 + \frac{m}{m'}$. We obtain

$$\operatorname{lt}(q')\operatorname{tt}(f') = \operatorname{lt}(g)\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{l' - \frac{m}{m'}}$$

and $k + 1 < l' - \frac{m}{m'} < l'$. Since $\operatorname{lt}(f)$ divides both $\operatorname{lt}(g)\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{k+1}$ and $\operatorname{lt}(g)\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{l'}$, it also divides $\operatorname{lt}(q')\operatorname{tt}(f')$.
Also,

$$\operatorname{lt}(q)\operatorname{tt}(f) = \operatorname{lt}(g)\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{l'-1}$$

and $k + \frac{m}{m'} < l' - 1 < l'$. Since $\operatorname{lt}(f')$ divides both $\operatorname{lt}(g)\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{k+\frac{m}{m'}}$ and $\operatorname{lt}(g)\left(\frac{\operatorname{lt}(f)}{\operatorname{tt}(f)}\right)^{l'}$, it also divides $\operatorname{lt}(q)\operatorname{tt}(f)$. Hence, $g = q''f + q'''f'$ for

$$q'' = q - \operatorname{lm}(q) + \frac{\operatorname{lm}(q')\operatorname{tm}(f')}{\operatorname{lm}(f)} \in \mathbb{K}[X] \setminus \{0\}$$

and

$$q''' = q' - \operatorname{lm}(q') + \frac{\operatorname{lm}(q)\operatorname{tm}(f)}{\operatorname{lm}(f')} \in \mathbb{K}[X] \setminus \{0\},$$

and $\deg(q''f) < \deg(qf)$ and $\deg(q'''f') < \deg(q'f')$, which contradicts the choice of q and q'. □

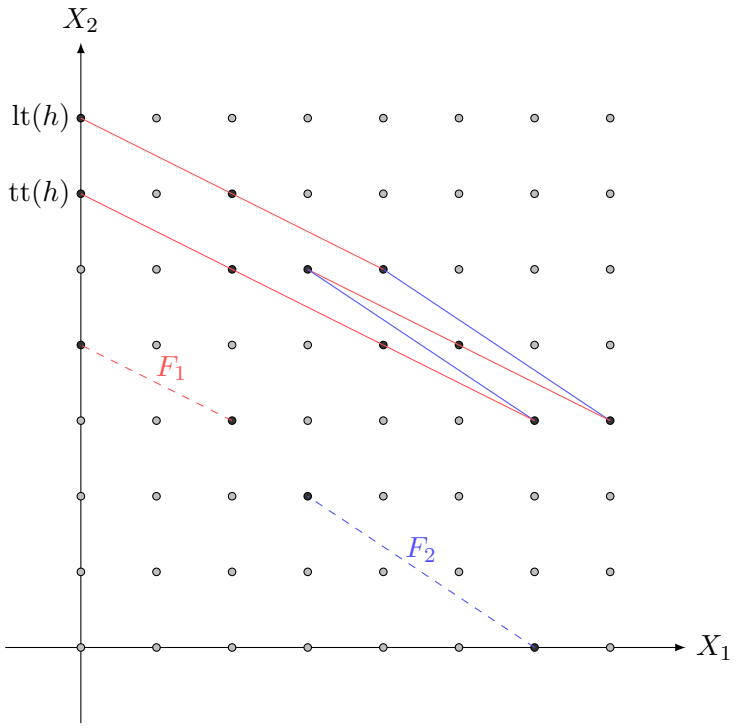


Figure 3.1: Graphical representation of a proper binomial in the ideal.

3.3 Degree Bounds on the Shifts for Generating a Proper Binomial in a Gröbner Basis

In this section, assume that F consists only of proper binomials and assume that g is a proper binomial such that g is irreducible with respect to F and $\text{supp}(g) \not\subseteq \text{ideal}(F)$.

3.3.1 Graphical Interpretation

We show how the representation of a proper binomial in the ideal in terms of the input polynomials can be viewed graphically.

Example 3.3.1. *Given* $F = \{X_1^2x_2^3 + X_2^4, X_1^6 + X_1^3X_2^2\}$, *the binomial* $h = X_2^7 + X_2^6$ *lies in* ideal(F), *since*

$$h = (-X_1^5 + X_1^4 + X_1^3X_2 - X_1^2X_2^2 - X_1^2X_2 + X_2^3 + X_2^2)F_1 + (X_1X_2^3 - X_2^3)F_2, \quad (3.2)$$

and it can be expressed as shifts of F_1 *and* F_2 *graphically as in Figure 3.1.*
The two dashed lines represent the two input polynomials, which have support $\text{supp}(F_1) = \{X_1^2X_2^3, X_2^4\}$ *and* $\text{supp}(F_2) = \{X_1^6, X_1^3X_2^2\}$, *and the polygon line consists*

of the shifts of F_1 and F_2 as described in (3.2). Starting point and ending point of the polygon chain form the support $\operatorname{supp}(h) = \{X_2^7, X_2^6\}$ *of h.*

Question: Is there always such a connection between a proper binomial in the ideal and a polygon chain connecting the elements in the support of the binomial?

This question will be answered in Theorems 3.3.14 and 3.3.17.

Definition 3.3.2 (posshift(f), negshift(f), shifts(H))**.** *For any proper binomial $f \in \mathbb{K}[X]$, we define*

$$\operatorname{posshift}(f) := (\operatorname{e}(\operatorname{tt}(f)), \operatorname{e}(\operatorname{lt}(f)))$$

and

$$\operatorname{negshift}(f) := (\operatorname{e}(\operatorname{lt}(f)), \operatorname{e}(\operatorname{tt}(f)))$$

and for any $\tau \in \mathbb{N}^n$ and any $\xi, \xi' \in \mathbb{N}^n$, we define

$$\tau + (\xi, \xi') := (\tau + \xi, \tau + \xi').$$

For any set H of proper binomials we define

$$\operatorname{shifts}(H) := \{\operatorname{posshift}(f) \mid f \in H\} \cup \{\operatorname{negshift}(f) \mid f \in H\}$$

and

$$\mathbb{N}^n + \operatorname{shifts}(H) := \{\tau + h \mid \tau \in \mathbb{N}^n \text{ and } h \in \operatorname{shifts}(H)\}.$$

For any proper binomial $f \in \mathbb{K}[X]$ we call $h \in \mathbb{N}^n + \operatorname{shifts}(\{f\})$ a positive shift of f if $h = \tau + \operatorname{posshift}(f)$ and a negative shift of f if $h = \tau + \operatorname{negshift}(f)$ for some $\tau \in \mathbb{N}^n$, or simply a shift of f, and for any $f' \in \operatorname{shifts}(\{f\})$ we call h a shift of f' if $h = \tau + f'$ for some $\tau \in \mathbb{N}^n$.

We extend Definition 3.1.12.

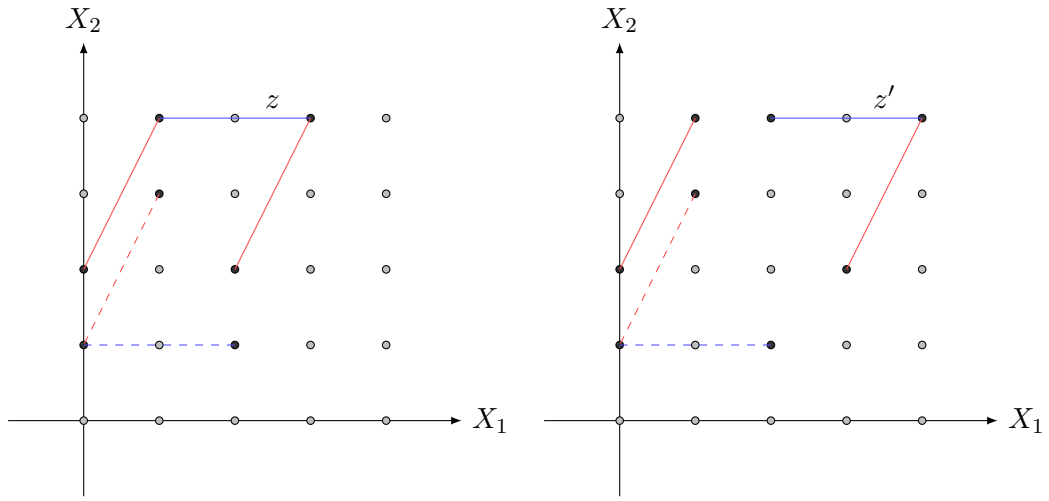
Definition 3.3.3 (vect of a shift)**.** *For any $h \in \mathbb{N}^n \times \mathbb{N}^n$ we define*

$$\operatorname{vect}(h) := h_2 - h_1.$$

Definition 3.3.4 (Valid polygon chain (vpc))**.** *Let $A, B \in \mathbb{N}^n$, $A \neq B$. We call a finite sequence z of elements in $\mathbb{N}^n + \operatorname{shifts}(F)$ a* valid polygon chain (vpc) *(from A to B) if $z_{k,2} = z_{k+1,1}$ for all $k \in \mathbb{N}_{\operatorname{len}(z)-1}$ (and $z_{1,1} = A$ and $z_{\operatorname{len}(z),2} = B$).*

Example 3.3.5. *Let $F = \{X_1^2 X_2 + 3X_2, 2X_1 X_2^3 - 2X_2\}$. The sequence*

$$z = (((0,2),(1,4)),\ ((1,4),(3,4)),\ ((3,4),(2,2)))$$



(a) Vpc z from $(0,2)$ to $(2,2)$. (b) Not a vpc.

Figure 3.2: Figure for Example 3.3.5.

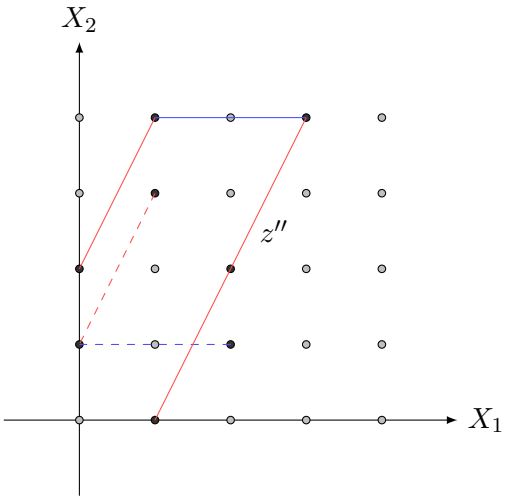


Figure 3.3: Figure for Example 3.3.5. Not a vpc.

is a vpc from $(0,2)$ *to* $(2,2)$ *(see Figure 3.2a), the sequence*

$$z' = (((0,2),(1,4)),\ ((2,4),(4,4)),\ ((4,4),(3,2)))$$

is not a vpc since $z'_{1,2} = (1,4) \neq (2,4) = z'_{2,1}$ *(see Figure 3.2b). Also the sequence*

$$z'' = (((0,2),(1,4)),\ ((1,4),(3,4)),\ ((3,4),(2,2)),\ ((2,2),(1,0)))$$

is not a vpc since $z''_4 = ((2,2),(1,0)) \notin \mathbb{N}^n + \text{shifts}(F)$*, which means that* z''_4 *isn't a valid shift of an input binomial (see Figure 3.3).*

Definition 3.3.6 (Degree of a vpc)**.** *The degree of a* $\xi = (\xi_1, \xi_2) \in \mathbb{Z}^n \times \mathbb{Z}^n$ *is defined as*

$$\deg(\xi) := \max(\deg(\xi_1), \deg(\xi_2)).$$

For a vpc z,

$$\deg(z) := \max(\{\deg(z_k) \mid k \in \mathbb{N}_{\text{len}(z)}\}).$$

Example 3.3.7. *Let F and z be as in Example 3.3.5. Then* $\deg(z) = 7$.

Definition 3.3.8 (Minimal vpc)**.** *Let $A, B \in \mathbb{N}^n$. A vpc z from A to B is* minimal *iff for all vpc's z' from A to B*

$$\text{len}(z) \leq \text{len}(z') \text{ and if } \text{len}(z) = \text{len}(z') \text{ then } \deg(z) \leq \deg(z').$$

Minimal vpcs are not unique.

Example 3.3.9. *Let $F = \{X_1X_2^3 + 2X_2, 2X_1^2X_2 - 2X_2\}$. The sequences*

$$z = (((1,7),(0,5)),\ ((0,5),(2,5)),\ ((2,5),(1,3)),\ ((1,3),(0,1))\,((0,1),(2,1)))$$

and

$$z' = (((1,7),(0,5)),\ ((0,5),(2,5)),\ ((2,5),(1,3)),\ ((1,3),(3,3))\,((3,3),(2,1)))$$

are both minimal vpcs from $(1,7)$ to $(2,1)$ with

$$\text{len}(z) = \text{len}(z') = 5$$

and

$$\deg(z) = \deg(z') = 8.$$

See Figure 3.4.

Minimal vpcs may even have a different number of respective shifts.

Example 3.3.10. *Let $F = \{X_1 + 2X_2, 2X_1^3 - X_2^3\}$. The sequences*

$$z = (((0,3),(1,2)),\ ((1,2),(2,1)))$$

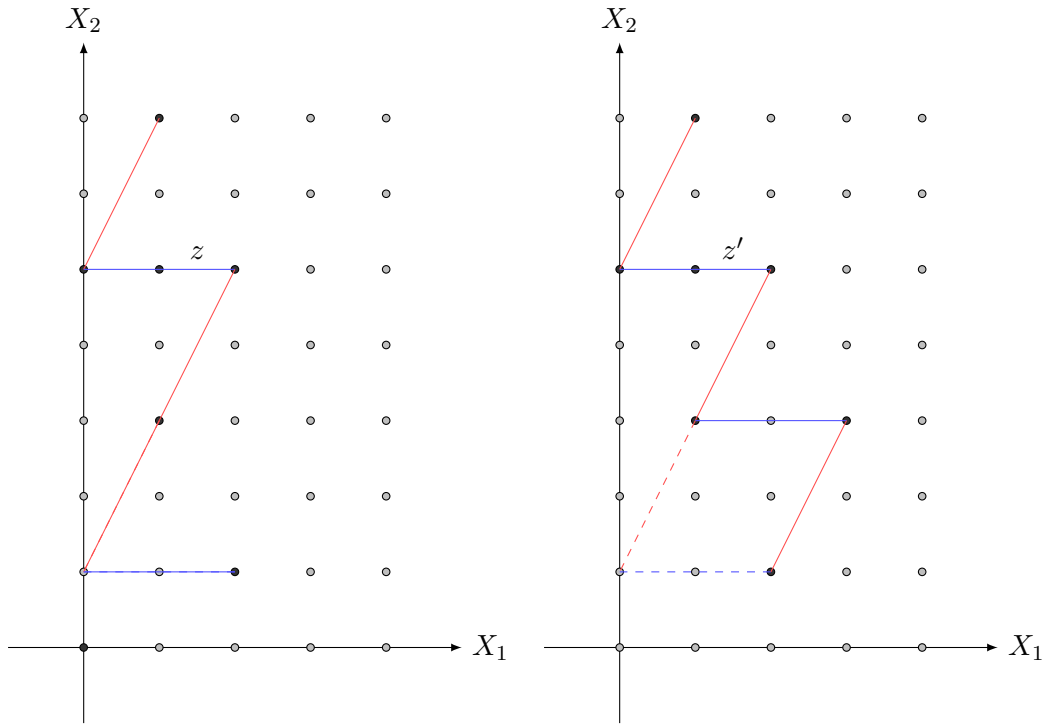
and

$$z' = (((0,3),(3,0)),\ ((3,0),(2,1)))$$

are both minimal vpcs from $(0,3)$ to $(2,1)$, where z consists of two shifts of F_1 and no shifts of F_2, and z consists of one shift of F_1 and one shift of F_2.

The following two lemmas are needed for the proof of Theorem 3.3.14.

Lemma 3.3.11. *Let $f \in \text{ideal}(F)$ such that $|\text{supp}(f)| = 3$ and $t, t' \in \text{supp}(f)$ such that $t \neq t'$ and $t, t' \notin \text{ideal}(F)$. Let $q_1, q_2 \in \mathbb{K}[X]$ such that $f = q_1F_1 + q_2F_2$. Then*



(a) Minimal vpc from $(1,7)$ to $(2,1)$. (b) Minimal vpc from $(1,7)$ to $(2,1)$.

Figure 3.4: Minimal vpcs are not unique.

there exist $q_1', q_2' \in \mathbb{K}[X]$ *and a* $c \in \mathbb{K} \setminus \{0\}$ *such that* $\operatorname{supp}(q_i') \subseteq \operatorname{supp}(q_i)$ *for all* $i = 1, 2$ *and* $q_1'F_1 + q_2'F_2 = f(t)t + ct'$.

Proof. We proceed by induction on $|\operatorname{supp}(q_1)| + |\operatorname{supp}(q_2)|$.
We assume $|\operatorname{supp}(q_1)| + |\operatorname{supp}(q_2)| = 2$. We distinguish three cases: $|\operatorname{supp}(q_1)| = 2$, $|\operatorname{supp}(q_2)| = 2$ and $|\operatorname{supp}(q_1)| = |\operatorname{supp}(q_2)| = 1$. Consider the case where $|\operatorname{supp}(q_1)| = 2$. Let $\operatorname{supp}(q_1) = \{\xi, \xi'\}$. We have

$$f = q_1(\xi)\xi F_1 + q_1(\xi')\xi' F_1.$$

Let $t'' \in \operatorname{supp}(f) \setminus \{t, t'\}$. Exactly one of the terms t, t', t'' lies in $\operatorname{supp}(\xi F_1) \cap \operatorname{supp}(\xi' F_1)$. If $t \in \operatorname{supp}(\xi F_1) \cap \operatorname{supp}(\xi' F_1)$, assume w.l.o.g. $t' \in \operatorname{supp}(\xi F_1)$. We then have

$$\begin{aligned}\frac{f(t)}{F_1(t/\xi)}\xi F_1 &= \frac{f(t)}{F_1(t/\xi)}(F_1(t/\xi)t + F_1(t'/\xi)t') \\ &= f(t)t + \frac{f(t)F_1(t'/\xi)}{F_1(t/\xi)}t' \\ &= q_1'F_1 + q_2'F_2,\end{aligned}$$

where $\frac{f(t)F_1(t'/\xi)}{F_1(t/\xi)} \neq 0$, $q_1' = \frac{f(t)}{F_1(t/\xi)}\xi$, $q_2' = 0$, $\operatorname{supp}(q_1') = \{\xi\} \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') = \emptyset \subseteq \operatorname{supp}(q_2)$.
If $t' \in \operatorname{supp}(\xi F_1) \cap \operatorname{supp}(\xi' F_1)$, assume w.l.o.g. $t \in \operatorname{supp}(\xi F_1)$. It follows

$$q_1(\xi)\xi F_1 = f(t)t + q_1(\xi)F_1(t'/\xi)t' = q_1'F_1 + q_2'F_2,$$

where $q_1(\xi)F_1(t'/\xi) \neq 0$, $q_1' = q_1(\xi)\xi$, $q_2' = 0$, $\operatorname{supp}(q_1') = \{\xi\} \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') = \emptyset \subseteq \operatorname{supp}(q_2)$.
If $t'' \in \operatorname{supp}(\xi F_1) \cap \operatorname{supp}(\xi' F_1)$, assume w.l.o.g. $t \in \operatorname{supp}(\xi F_1)$ and $t' \in \operatorname{supp}(\xi' F_1)$. We then have

$$\begin{aligned} q_1(\xi)\xi F_1 - \frac{q_1(\xi)F_1(t''/\xi)}{F_1(t''/\xi')}\xi' F_1 &= f(t)t + \frac{q_1(\xi)F_1(t''/\xi)F_1(t'/\xi')}{F_1(t''/\xi')}t' \\ &= q_1'F_1 + q_2'F_2, \end{aligned}$$

where $\frac{q_1(\xi)F_1(t''/\xi)F_1(t'/\xi')}{F_1(t''/\xi')} \neq 0$, $q_1' = q_1(\xi)\xi - \frac{q_1(\xi)F_1(t''/\xi)}{F_1(t''/\xi')}\xi'$, $q_2' = 0$, $\operatorname{supp}(q_1') = \{\xi, \xi'\} \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') = \emptyset \subseteq \operatorname{supp}(q_2)$.
The cases $|\operatorname{supp}(q_2)| = 2$ and $|\operatorname{supp}(q_1)| = |\operatorname{supp}(q_2)| = 1$ work analogously.

Let now $k \in \mathbb{N}$, $k \geq 2$. Let f, t, t', q_1 and q_2 be as in the lemma and assume, $|\operatorname{supp}(q_1)| + |\operatorname{supp}(q_2)| = k + 1$.
Let $t'' \in \operatorname{supp}(f) \setminus \{t, t'\}$ and let $Y_1 \subseteq \operatorname{supp}(q_1)$, $Y_2 \subseteq \operatorname{supp}(q_2)$ such that for

$$h := \left(\sum_{\mu \in Y_1} q_1(\mu)\mu\right) F_1 + \left(\sum_{\nu \in Y_2} q_2(\nu)\nu\right) F_2$$

we have $|\operatorname{supp}(h)| = 2$, $t \in \operatorname{supp}(h)$ and that $|Y_1| + |Y_2|$ is maximal. Such Y_1, Y_2 exist, since there are $i \in \{1, 2\}$ and $s \in \operatorname{supp}(q_i)$ such that $t \in \operatorname{supp}(q_i(s)sF_i)$, where $q_i(s)sF_i$ is a proper binomial. If $h(t') \neq 0$, it follows that

$$\begin{aligned} \frac{f(t)}{h(t)}h &= f(t)t + \frac{f(t)h(t')}{h(t)}t' \\ &= q_1'F_1 + q_2'F_2, \end{aligned}$$

where $\frac{f(t)h(t')}{h(t)} \neq 0$, $q_1' = \frac{f(t)}{h(t)}\left(\sum_{\mu \in Y_1} q_1(\mu)\mu\right)$, $q_2' = \frac{f(t)}{h(t)}\left(\sum_{\nu \in Y_2} q_2(\nu)\nu\right)$, $\operatorname{supp}(q_1') = Y_1 \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') = Y_2 \subseteq \operatorname{supp}(q_2)$.
We now assume $h(t') = 0$. Similar to before, let $Y_1' \subseteq \operatorname{supp}(q_1) \setminus Y_1$ and $Y_2' \subseteq \operatorname{supp}(q_2) \setminus Y_2$ such that for

$$h' := \left(\sum_{\mu \in Y_1'} q_1(\mu)\mu\right) F_1 + \left(\sum_{\nu \in Y_2'} q_2(\nu)\nu\right) F_2$$

we have $|\operatorname{supp}(h')| = 2$, $t' \in \operatorname{supp}(h')$ and that $|Y_1'| + |Y_2'|$ is maximal. By the same argument as above, such Y_1', Y_2' exist, since $t' \in \operatorname{supp}(f-h)$. Let

$$h'' := f - h - h'$$

and $l, l' \in [X]$ such that $\operatorname{supp}(h) = \{t, l\}$ and $\operatorname{supp}(h') = \{t', l'\}$.
If $l = t''$, then

$$\frac{f(t'')}{h(t'')}h = \frac{f(t'')h(t)}{h(t'')}t + f(t'')t'',$$

hence,

$$f - \frac{f(t'')}{h(t'')}h = f(t')t' + (f(t) - \frac{f(t'')h(t)}{h(t'')})t,$$

where $f(t) - \frac{f(t'')h(t)}{h(t'')} \neq 0$ since otherwise t' would be an element of ideal(F). We obtain

$$\begin{aligned}\frac{f(t)}{f(t) - \frac{f(t'')h(t)}{h(t'')}}(f - \frac{f(t'')}{h(t'')}h) &= f(t)t + \frac{f(t)f(t')}{f(t) - \frac{f(t'')h(t)}{h(t'')}}t' \\ &= q_1'F_1 + q_2'F_2,\end{aligned}$$

where

$$c = \frac{f(t)f(t')}{f(t) - \frac{f(t'')h(t)}{h(t'')}} \neq 0,$$

$$q_1' = \frac{c}{f(t')}\left(q_1 - \frac{f(t'')}{h(t'')}\left(\sum_{\mu \in Y_1} q_1(\mu)\mu\right)\right),$$

$$q_2' = \frac{c}{f(t')}\left(q_2 - \frac{f(t'')}{h(t'')}\left(\sum_{\nu \in Y_2} q_2(\nu)\nu\right)\right),$$

$\operatorname{supp}(q_1') \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') \subseteq \operatorname{supp}(q_2)$.
If $l' = t''$, then

$$\frac{f(t'')}{h'(t'')}h' = \frac{f(t'')h'(t')}{h'(t'')}t' + f(t'')t'',$$

hence,

$$\begin{aligned}f - \frac{f(t'')}{h'(t'')}h' &= f(t)t + (f(t') - \frac{f(t'')h'(t')}{h'(t'')})t' \\ &= q_1'F_1 + q_2'F_2,\end{aligned}$$

where $f(t') - \frac{f(t'')h'(t')}{h'(t'')} \neq 0$ since otherwise t would be an element of ideal(F),

$$q_1' = q_1 - \frac{f(t'')}{h'(t'')}\left(\sum_{\mu \in Y_1'} q_1(\mu)\mu\right),$$

$$q_2' = q_2 - \frac{f(t'')}{h'(t'')} \left(\sum_{\nu \in Y_2'} q_2(\nu)\nu \right),$$

$\operatorname{supp}(q_1') \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') \subseteq \operatorname{supp}(q_2)$.
If $l' = t$, then

$$\begin{aligned} \frac{f(t)}{h'(t)} h' &= f(t)t + \frac{f(t)h'(t')}{h'(t)} t' \\ &= q_1' F_1 + q_2' F_2, \end{aligned}$$

where $\frac{f(t)h'(t')}{h'(t)} \neq 0$, $q_1' = \frac{f(t)}{h'(t)} \left(\sum_{\mu \in Y_1'} q_1(\mu)\mu \right)$, $q_2' = \frac{f(t)}{h'(t)} \left(\sum_{\nu \in Y_2'} q_2(\nu)\nu \right)$, $\operatorname{supp}(q_1') = Y_1' \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') = Y_2' \subseteq \operatorname{supp}(q_2)$.
If $l = l'$, then

$$\begin{aligned} \frac{f(t)}{h(t)}(h - \frac{h(l)}{h'(l)} h') &= \frac{f(t)}{h(t)}(h(t)t + h(l)l - h(l)l - \frac{h(l)h'(t')}{h'(l)} t') \\ &= f(t)t - \frac{f(t)h(l)h'(t')}{h(t)h'(l)} t' \\ &= q_1' F_1 + q_2' F_2, \end{aligned}$$

where $-\frac{f(t)h(l)h'(t')}{h(t)h'(l)} \neq 0$,

$$q_1' = \frac{f(t)}{h(t)} \left(\left(\sum_{\mu \in Y_1} q_1(\mu)\mu \right) - \frac{h(l)}{h'(l)} \left(\sum_{\mu \in Y_1'} q_1(\mu)\mu \right) \right),$$

$$q_2' = \frac{f(t)}{h(t)} \left(\left(\sum_{\nu \in Y_2} q_2(\nu)\nu \right) - \frac{h(l)}{h'(l)} \left(\sum_{\nu \in Y_2'} q_2(\nu)\nu \right) \right),$$

$\operatorname{supp}(q_1') \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') \subseteq \operatorname{supp}(q_2)$.

Additionally to $h(t') = 0$ (see earlier in the proof), hence $l \neq t'$, we now assume $l \neq t''$, $l' \neq t''$, $l' \neq t$ and $l \neq l'$.
From $l \neq t'$ and $l \neq l'$ it follows that $h(l) = h''(l)$. From $l' \neq t$ and $l' \neq l$ it follows that $h'(l') = h''(l')$. We have $\operatorname{supp}(h'') = \{t'', l, l'\}$ and $l, l' \notin \operatorname{ideal}(F)$ since otherwise $\frac{1}{h(t)}(h - h(l)l) = t \in \operatorname{ideal}(F)$ and $\frac{1}{h'(t')}(h' - h'(l')l') = t' \in \operatorname{ideal}(F)$, respectively, which is a contradiction to the assumptions in the lemma. With

$$q_1'' := \sum_{\mu \in \operatorname{supp}(q_1) \setminus (Y_1 \cup Y_1')} q_1(\mu)\mu$$

and

$$q_2'' := \sum_{\nu \in \operatorname{supp}(q_2) \setminus (Y_2 \cup Y_2')} q_2(\nu)\nu$$

we have

$$h'' = q_1'' F_1 + q_2'' F_2,$$

and, since $|Y_1 \cup Y_1'| + |Y_2 \cup Y_2'| \geq 2$, $|\operatorname{supp}(q_1'')| + |\operatorname{supp}(q_2'')| < k$. By the induction assumption there exist $q_1''', q_2''' \in \mathbb{K}[X]$ and $c' \in \mathbb{K} \setminus \{0\}$ such that $\operatorname{supp}(q_i''') \subseteq \operatorname{supp}(q_i'')$ for all $i = 1, 2$ and

$$q_1''' F_1 + q_2''' F_2 = h''(l)l + c'l' =: h'''.$$

From this follows

$$\begin{aligned}\frac{f(t)}{h(t)}(h - h''') &= \frac{f(t)}{h(t)}(h(t)t + h(l)l - h''(l)l - c'l') \\ &= \frac{f(t)}{h(t)}(h(t)t + h(l)l - h(l)l - c'l') \\ &= f(t)t - \frac{f(t)c'}{h(t)}l'\end{aligned}$$

and hence

$$\begin{aligned}\frac{f(t)}{h(t)}(h - h''') + \frac{f(t)c'}{h(t)h'(l')}h' &= f(t)t + \frac{f(t)c'h'(t')}{h(t)h'(l')}t' \\ &= q_1' F_1 + q_2' F_2,\end{aligned}$$

where $\frac{f(t)c'h'(t')}{h(t)h'(l')} \neq 0$,

$$q_1' = \frac{f(t)}{h(t)}\left(\sum_{\mu \in Y_1} q_1(\mu)\mu - q_1'''\right) + \frac{f(t)c'}{h(t)h'(l')}\left(\sum_{\mu \in Y_1'} q_1(\mu)\mu\right),$$

$$q_2' = \frac{f(t)}{h(t)}\left(\sum_{\nu \in Y_2} q_2(\nu)\nu - q_2'''\right) + \frac{f(t)c'}{h(t)h'(l')}\left(\sum_{\nu \in Y_2'} q_2(\nu)\nu\right),$$

$\operatorname{supp}(q_1') \subseteq \operatorname{supp}(q_1)$ and $\operatorname{supp}(q_2') \subseteq \operatorname{supp}(q_2)$.

□

Lemma 3.3.12. *Let $f \in \operatorname{ideal}(F)$ be a proper binomial such that $\operatorname{tt}(f) \notin \operatorname{ideal}(F)$. Then for every $f' \in \operatorname{ideal}(F)$ with $\operatorname{supp}(f') = \operatorname{supp}(f)$, there exists a $c \in \mathbb{K} \setminus \{0\}$ such that $f = cf'$.*

Proof. Let $f' \in \operatorname{ideal}(F)$ with $\operatorname{supp}(f') = \operatorname{supp}(f)$ and $c = \frac{\operatorname{lc}(f)}{\operatorname{lc}(f')} \in \mathbb{K} \setminus \{0\}$. We have

$$\begin{aligned}cf' &= c\operatorname{lc}(f')\operatorname{lt}(f') + c\operatorname{tc}(f')\operatorname{tt}(f') \\ &= \operatorname{lc}(f)\operatorname{lt}(f) + c\operatorname{tc}(f')\operatorname{tt}(f).\end{aligned}$$

If $c\,\mathrm{tc}(f') \neq \mathrm{tc}(f)$, we get

$$f - cf' = (\mathrm{tc}(f) - c\,\mathrm{tc}(f'))\,\mathrm{tt}(f) \in \mathrm{ideal}(F),$$

which contradicts $\mathrm{tt}(f) \notin \mathrm{ideal}(F)$. Hence $f = cf'$. □

Definition 3.3.13. *For $f \in \mathrm{ideal}(F)$ let*

$$\mathrm{mincofsupp}(f) := \min(\{|\,\mathrm{supp}(q_1)| + |\,\mathrm{supp}(q_2)| \mid q_1, q_2 \in \mathbb{K}[X] \text{ and } f = q_1F_1 + q_2F_2\}).$$

Theorem 3.3.14. *Let $f \in \mathrm{ideal}(F)$ be a proper binomial such that $\mathrm{lt}(f) \notin \mathrm{ideal}(F)$. Then there exists a vpc from $\mathrm{e}(\mathrm{lt}(f))$ to $\mathrm{e}(\mathrm{tt}(f))$.*

Proof. First note that $\mathrm{tt}(f) \notin \mathrm{ideal}(F)$, since otherwise

$$\mathrm{lt}(f) = \frac{1}{\mathrm{lc}(f)} f - \frac{\mathrm{tc}(f)}{\mathrm{lc}(f)}\,\mathrm{tt}(f) \in \mathrm{ideal}(F),$$

which contradicts $\mathrm{lt}(f) \notin \mathrm{ideal}(F)$. We proceed by induction on $\mathrm{mincofsupp}(f)$. Suppose $\mathrm{mincofsupp}(f) = 1$. Then there exist $t \in [X]$, $i \in \{1, 2\}$ and $c \in \mathbb{K} \setminus \{0\}$ such that $f = ctF_i$. A vpc z from $\mathrm{e}(\mathrm{lt}(f))$ to $\mathrm{e}(\mathrm{tt}(f))$ is given by

$$z = (\mathrm{e}(t) + \mathrm{e}(\mathrm{lt}(F_i)), \mathrm{e}(t) + \mathrm{e}(\mathrm{tt}(F_i))) = (\mathrm{e}(t) + \mathrm{negshift}(F_i))\,.$$

Let now $k \in \mathbb{N}\setminus\{0\}$. Let f be as in the theorem and assume $\mathrm{mincofsupp}(f) = k+1$. Let $q_1, q_2 \in \mathbb{K}[X]$ such that $f = q_1F_1 + q_2F_2$ and $|\,\mathrm{supp}(q_1)| + |\,\mathrm{supp}(q_2)| = \mathrm{mincofsupp}(f)$. There are $i \in \{1, 2\}$ and $t \in \mathrm{supp}(q_i)$ such that $t\,\mathrm{lt}(F_i) = \mathrm{lt}(f)$ or $t\,\mathrm{tt}(F_i) = \mathrm{lt}(f)$. Let w.l.o.g. $i = 1$ and let $q_1' := q_1 - q_1(t)t$ and $f' := f - q_1(t)tF_1$.
We first consider the case where $t\,\mathrm{lt}(F_1) = \mathrm{lt}(f)$. We obtain

$$\begin{aligned} f' &= \mathrm{lm}(f) + \mathrm{tm}(f) - (q_1(t)t\,\mathrm{lm}(F_1) + q_1(t)t\,\mathrm{tm}(F_1)) \\ &= (\mathrm{lc}(f) - q_1(t)\,\mathrm{lc}(F_1))t\,\mathrm{lt}(F_1) + \mathrm{tm}(f) - q_1(t)t\,\mathrm{tm}(F_1). \end{aligned}$$

Note that $\mathrm{tt}(f) \neq t\,\mathrm{tt}(F_1)$, since otherwise either $f = ctF_1$ for some $c \in \mathbb{K} \setminus \{0\}$, which contradicts the assumption that $\mathrm{mincofsupp}(f) = k + 1 > 1$, or $\mathrm{lt}(f) \in \mathrm{ideal}(F)$, which contradicts the assumption $\mathrm{lt}(f) \notin \mathrm{ideal}(F)$. If $\mathrm{lc}(f) - q_1(t)\,\mathrm{lc}(F_1) \neq 0$, then by Lemma 3.3.11 there exist $q_1'', q_2'' \in \mathbb{K}[X]$ and $c \in \mathbb{K} \setminus \{0\}$ such that $\mathrm{supp}(q_1'') \subseteq \mathrm{supp}(q_1') \subset \mathrm{supp}(q_1)$, $\mathrm{supp}(q_2'') \subseteq \mathrm{supp}(q_2)$ and

$$\begin{aligned} q_1''F_1 + q_2''F_2 &= (\mathrm{lc}(f) - q_1(t)\,\mathrm{lc}(F_1))t\,\mathrm{lt}(F_1) + c\,\mathrm{tt}(f) \\ &= (\mathrm{lc}(f) - q_1(t)\,\mathrm{lc}(F_1))\,\mathrm{lt}(f) + c\,\mathrm{tt}(f). \end{aligned}$$

By Lemma 3.3.12 there exists a $c' \in \mathbb{K} \setminus \{0\}$ such that

$$c'(\operatorname{lc}(f) - q_1(t)\operatorname{lc}(F_1))\operatorname{lt}(f) + c'c\operatorname{tt}(f) = f,$$

hence $f = c'q_1''F_1 + c'q_2''F_2$. But since

$$|\operatorname{supp}(c'q_1'')| + |\operatorname{supp}(c'q_2'')| < |\operatorname{supp}(q_1)| + |\operatorname{supp}(q_2)|,$$

this contradicts $|\operatorname{supp}(q_1)| + |\operatorname{supp}(q_2)| = \operatorname{mincofsupp}(f)$. Therefore,

$$\operatorname{lc}(f) - q_1(t)\operatorname{lc}(F_1) = 0.$$

We have $t\operatorname{tt}(F_1) \notin \operatorname{ideal}(F)$ because otherwise

$$\operatorname{lt}(f) = t\operatorname{lt}(F_1) = \frac{1}{\operatorname{lc}(F_1)}tF_1 - \frac{\operatorname{tc}(F_1)}{\operatorname{lc}(F_1)}t\operatorname{tt}(F_1) \in \operatorname{ideal}(F),$$

which contradicts the assumption in the lemma.
Let w.l.o.g. $\operatorname{tt}(f) \prec t\operatorname{tm}(F_1)$. According to the induction assumption there exists a vpc z' from $\operatorname{e}(t\operatorname{tm}(F_1))$ to $\operatorname{e}(\operatorname{tt}(f))$. A vpc z from $\operatorname{e}(\operatorname{lt}(f)$ to $\operatorname{e}(\operatorname{tt}(f))$ then is given by

$$z_j := \begin{cases} \operatorname{e}(t) + \operatorname{negshift}(F_1) & \text{if } j = 1 \\ z'_{j-1} & \text{if } 2 \leq j \leq \operatorname{len}(z') + 1. \end{cases}$$

The case $t\operatorname{tt}(F_1) = \operatorname{lt}(f)$ proceeds analogously, the definition of the vpc z reads as

$$z_j := \begin{cases} \operatorname{e}(t) + \operatorname{posshift}(F_1) & \text{if } j = 1 \\ z'_{j-1} & \text{if } 2 \leq j \leq \operatorname{len}(z') + 1. \end{cases}$$

□

If for a proper binomial $f \in \operatorname{ideal}(F)$ we have $\operatorname{lt}(f) \in \operatorname{ideal}(F)$. Then there need not exist a vpc from $\operatorname{e}(\operatorname{lt}(f))$ to $\operatorname{e}(\operatorname{tt}(f))$.

Example 3.3.15. *Let* $F_1 = X_1^2X_2^6 - 2X_2^4$ *and* $F_2 = X_1^7X_2^3 - 3X_1^4$. *We have* $f = X_1^4 + X_2^4 \in \operatorname{ideal}(F)$ *with* $\operatorname{supp}(f) \subseteq \operatorname{ideal}(F)$, *hence also* $\operatorname{lt}(f) \in \operatorname{ideal}(F)$ *w.r.t. any ordering, but the equation*

$$\operatorname{e}(\operatorname{lt}(f)) - \operatorname{e}(\operatorname{tt}(f)) = k\operatorname{vect}(F_1) + k'\operatorname{vect}(F_2)$$

in k *and* k', *which reads*

$$(4, -4) = k(2, 2) + k'(3, 3),$$

has no solution in $\mathbb{Z}^2$. *Such a solution is a necessary (although not sufficient) condition for the existence of a vpc from* $\operatorname{e}(\operatorname{lt}(f))$ *to* $\operatorname{e}(\operatorname{tt}(f))$.

Proposition 3.3.16. *Let $A, B \in \mathbb{N}^n$. If there is a vpc from A to B, then there is a vpc from B to A.*

Proof. Let z be a vpc from A to B. Then a vpc z' from B to A is given by

$$z'_j := (z_{\mathrm{len}(z)+1-j,\,2},\ z_{\mathrm{len}(z)+1-j,\,1})$$

for $j \in \mathbb{N}_{\mathrm{len}(z)}$. □

Theorem 3.3.17. *Let $A, B \in \mathbb{N}^n$, $A \neq B$, and z be a vpc from A to B. Then there exist $f \in \mathrm{ideal}(F)$ and $q_1, q_2 \in \mathbb{K}[X]$ such that $\mathrm{e}(\mathrm{supp}(f)) = \{A, B\}$, $f = q_1F_1 + q_2F_2$ and, if $q_i \neq 0$, $\deg(q_iF_i) \leq \deg(z)$ for all $i = 1, 2$.*

Proof. Every sequence element in z is of the form $\tau + \mathrm{posshift}(F_k)$ or $\tau + \mathrm{negshift}(F_k)$ for some $\tau \in \mathbb{N}^n$ and some $k \in \{1, 2\}$. Let $k_1 \in \{1, 2\}$ and $\tau^{(1)} \in \mathbb{N}^n$ such that $z_1 = \tau^{(1)} + \mathrm{posshift}(F_{k_1})$ or $z_1 = \tau^{(1)} + \mathrm{negshift}(F_{k_1})$. Then we define

$$f^{(1)} := \mathrm{e}^{-1}(\tau^{(1)})F_{k_1}$$

and for $i \in \{1, 2\}$

$$q_i^{(1)} := \begin{cases} \mathrm{e}^{-1}(\tau^{(1)}) & \text{if } i = k_1 \\ 0 & \text{else.} \end{cases}$$

For j with $2 \leq j \leq \mathrm{len}(z)$ let now $k_j \in \{1, 2\}$ and $\tau^{(j)} \in \mathbb{N}^n$ such that $z_j = \tau^{(j)} + \mathrm{posshift}(F_{k_j})$ or $z_j = \tau^{(j)} + \mathrm{negshift}(F_{k_j})$. Then we define

$$f^{(j)} := f^{(j-1)} + \xi^{(j)}F_{k_j}$$

and for $i \in \{1, 2\}$

$$q_i^{(j)} := \begin{cases} q_i^{(j-1)} + \xi^{(j)} & \text{if } i = k_j \\ q_i^{(j-1)} & \text{else,} \end{cases}$$

where

$$\xi^{(j)} := \begin{cases} -\frac{f^{(j-1)}(\mathrm{e}^{-1}(z_{j,1}))}{\mathrm{tc}(F_{k_j})}\,\mathrm{e}^{-1}(\tau^{(j)}) & \text{if } z_j = \tau^{(j)} + \mathrm{posshift}(F_{k_j}) \\ -\frac{f^{(j-1)}(\mathrm{e}^{-1}(z_{j,1}))}{\mathrm{lc}(F_{k_j})}\,\mathrm{e}^{-1}(\tau^{(j)}) & \text{if } z_j = \tau^{(j)} + \mathrm{negshift}(F_{k_j}). \end{cases}$$

We have $f^{(\mathrm{len}(z))} \in \mathrm{ideal}(F)$, $\mathrm{e}(\mathrm{supp}(f^{(\mathrm{len}(z))})) = \{A, B\}$, $f = q_1^{(\mathrm{len}(z))}F_1 + q_2^{(\mathrm{len}(z))}F_2$ and, if $q_i^{(\mathrm{len}(z))} \neq 0$, $\deg(q_i^{(\mathrm{len}(z))}F_i) \leq \deg(z)$ for all $i = 1, 2$. □

Together with Lemma 3.3.12, Theorems 3.3.14 and 3.3.17 show that in order to find a d' that solves Problem 3.1.5 for the proper binomial g, it suffices to find a degree bound on a vpc from $\mathrm{e}(\mathrm{lt}(g))$ to $\mathrm{e}(\mathrm{tt}(g))$. The latter is a combinatorial problem.

3.3.2 Upper Degree Bound on a Valid Polygon Chain

Recall that in the beginning of Section 3.3 we required $\mathrm{lt}(g), \mathrm{tt}(g) \notin \mathrm{ideal}(F)$. Let in this whole section $U, V \in \mathbb{N}^n$ be such that $\mathrm{e}(\mathrm{supp}(g)) = \{U, V\}$. We know from Theorem 3.3.14 and Proposition 3.3.16 that there exists a vpc from U to V.

Recall Definition 3.1.11.

Theorem 3.3.18. *Let z be a vpc and let $k \in \mathbb{N}_{\mathrm{len}(z)-1}$. Assume, z_k is a shift of f and z_{k+1} is a shift of f' with $f, f' \in F$ and $f \neq f'$, then $z_{k,2} = z_{k+1,1} \geq \mathrm{overlap}(F)$.*

Proof. We show

$$z_{k,2} \geq \gcd(\mathrm{e}(\mathrm{lt}(F_i)), \mathrm{e}(\mathrm{tt}(F_i))) \text{ for all } i = 1, 2.$$

Depending on whether the shifts are positive or negative, we distinguish four cases. We show one of them, the others work analogously. If z_k is a positive shift of f and z_{k+1} is a positive shift of f', then $z_{k,2} \geq \mathrm{e}(\mathrm{lt}(f))$ and $z_{k,2} \geq \mathrm{e}(\mathrm{tt}(f'))$. It follows that

$$z_{k,2} \geq \gcd(\mathrm{e}(\mathrm{lt}(F_i)), \mathrm{e}(\mathrm{tt}(F_i))) \text{ for all } i = 1, 2.$$

So we obtain

$$\begin{aligned} z_{k,2} &\geq \mathrm{lcm}(\gcd(\mathrm{e}(\mathrm{lt}(F_1)), \mathrm{e}(\mathrm{tt}(F_1))), \gcd(\mathrm{e}(\mathrm{lt}(F_2)), \mathrm{e}(\mathrm{tt}(F_2)))) \\ &= \mathrm{overlap}(F). \end{aligned}$$

□

We conclude that interactions between shifts of F_1 and F_2 in a vpc occur only in the area $\mathrm{Aoverlap}(F) := \{P \in \mathbb{N}^n \mid P \geq \mathrm{overlap}(F)\}$. Outside of this area there can only be a sequence of shifts of F_1 or a sequence of shifts of F_2. The length of these sequences is given by the step function of Definition 3.1.14. Note that for any $P \in \mathbb{N}^n$ with $\mathrm{e}(\mathrm{tt}(f)) \leq P$ for some $f \in F$, if there exists a vpc from P to some $P' \geq \mathrm{overlap}(F)$, we have $\mathrm{overlapshift}(P) \in \mathrm{Aoverlap}(F)$. Details follow in the next subsection.

3.3.2.1 Structure of a Minimal Valid Polygon Chain

We investigate the structure of a minimal vpc $\mathfrak{z}$ from U to V. As an illustration, see Figure 3.5. Recall, that we assumed $U \neq V$ and, since g is irreducible with respect to F, $U, V \not\geq \mathrm{e}(\mathrm{lt}(f))$ for all $f \in F$. So $\mathfrak{z}_1$ has to be a positive shift of f' and $\mathfrak{z}_{\mathrm{len}(z)}$ has to be a negative shift f'', where $f', f'' \in F$. Recall that shifts of F_1 and F_2 can only interact

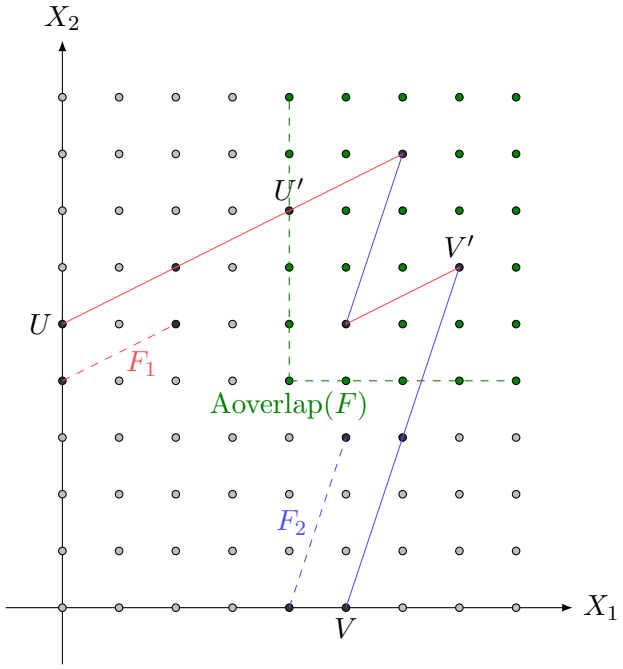


Figure 3.5: Minimal vpc from U to V. Here we denote overlapshift(U) as U' and overlapshift(V) as V'.

in the area Aoverlap(F). So the first step(U) elements in $\mathfrak{z}$ will be positive shifts of f' going from U to overlapshift(U) and the last step(V) elements in $\mathfrak{z}$ will be negative shifts of f'' going from overlapshift(V) to V. If overlapshift(U) = overlapshift(V), then $\mathfrak{z}$ is given by

$$\mathfrak{z}_j = \begin{cases} (U - \mathrm{e}(\mathrm{tt}(f'))) + \mathrm{posshift}(f') & \text{if } j = 1, \\ \mathrm{vect}(f') + \mathfrak{z}_{j-1} & \text{if } 2 \leq j \leq \mathrm{step}(U), \\ -\mathrm{vect}(f'') + \mathfrak{z}_{j-1} & \text{if } \mathrm{step}(U) + 1 \leq j \leq \mathrm{step}(U) + \mathrm{step}(V). \end{cases}$$

If overlapshift(U) $\neq$ overlapshift(V), we need to investigate the structure of that part of $\mathfrak{z}$ going from overlapshift(U) to overlapshift(V). This part is again a minimal vpc.

Lemma 3.3.19. *Let $A, B \in \mathbb{N}^n$ with $A \neq B$ and let z be a vpc from A to B of minimal length. Let $j \in \mathbb{N}_{\mathrm{len}(z)-1}$ such that z_j and z_{j+1} are shifts of the same binomial $f \in F$. Then z_j and z_{j+1} are either both positive shifts of f or both negative shifts of f.*

Proof. For a contradiction, assume w.l.o.g. that z_j is a positive shift of f and z_{j+1} is a negative shift of f. Then z' with

$$z'_{j'} = \begin{cases} z_{j'} & \text{if } 1 \leq j' \leq j-1 \\ z_{j'+2} & \text{if } j \leq j' \leq \mathrm{len}(z) - 2 \end{cases}$$

is a vpc from A to B with $\operatorname{len}(z') = \operatorname{len}(z) - 2 < \operatorname{len}(z)$, hence z cannot have minimal length. □

In the following theorem we show that a vpc of minimal length (hence also a minimal vpc) starting and ending in $\operatorname{Aoverlap}(F)$ lies in $\operatorname{Aoverlap}(F)$ in its entirety.

Theorem 3.3.20. *Let $A, B \in \operatorname{Aoverlap}(F)$ such that $A \neq B$, let z be a vpc from A to B of minimal length and let $k \in \mathbb{N}_{\operatorname{len}(z)}$. Then $z_{k,1} \in \operatorname{Aoverlap}(F)$.*

Proof. We proceed by induction on k. If $k = 1$, then $z_{k,1} = z_{1,1} = A \in \operatorname{Aoverlap}(F)$. Let now $k \in \mathbb{N}_{\operatorname{len}(z)-1}$ and assume that $z_{k,1} \geq \operatorname{overlap}(F)$. We show that $z_{k+1,1} \geq \operatorname{overlap}(F)$. Let z_{k+1} be a shift of f, where $f \in \operatorname{shifts}(F)$. Assume $z_{k+1,1} = z_{k,1} + \operatorname{vect}(f) \not\geq \operatorname{overlap}(F)$. If z_j is a shift of the same input binomial as f for all j with $k+1 \leq j \leq \operatorname{len}(z)$, then by Lemma 3.3.19 z_j is a shift of f for all these j and

$$B = z_{k,1} + (\operatorname{len}(z) - k + 1)\operatorname{vect}(f).$$

Since $z_{k,1} + \operatorname{vect}(f) \not\geq \operatorname{overlap}(F)$, there must be an $i \in \mathbb{N}_n$ such that

$$z_{k,1,i} + \operatorname{vect}(f)_i < \operatorname{overlap}(F)_i,$$

and since $z_{k,1,i} \geq \operatorname{overlap}(F)_i$ it follows that $\operatorname{vect}(f)_i < 0$. Hence,

$$B_i = z_{k,1,i} + (\operatorname{len}(z) - k + 1)\operatorname{vect}(f)_i < \operatorname{overlap}(F)_i,$$

since $\operatorname{len}(z) - k + 1 > 1$. This contradicts $B \geq \operatorname{overlap}(F)$.

If z, after the $(k+1)$-th shift, also contains shifts of f', where $f' \in \operatorname{shifts}(F)$ such that f and f' are shifts of two different input binomials, then let $k' \in \mathbb{N}_{\operatorname{len}(z)}$ with $k' > k+1$ be minimal such that $z_{k'}$ is a shift of f'. We first show that $z_{k',1} \in \operatorname{Aoverlap}(F)$. Since $z_{k',1}$ is a shift of f', we have $z_{k',1} \geq \gcd(f'_1, f'_2)$. Since $z_{k'-1,1}$ is a shift of f we have $z_{k',1} = z_{k'-1,2} \geq \gcd(f_1, f_2)$. Therfore, we obtain $z_{k',1} \geq \operatorname{overlap}(F)$. Now the same argument as before with $z_{k',1}$ instead of B and $k'-1$ instead of $\operatorname{len}(z)$ leads to a contradiction. Therefore, $z_{k,1} \in \operatorname{Aoverlap}(F)$. □

In Theorem 3.3.22 we show that for $A, B \in \operatorname{Aoverlap}(F)$ with $A \neq B$ and $f \in F$, a vpc from A to B of minimal length (hence also a minimal vpc) cannot contain both a positive shift of f and a negative shift of f. But first we need the following lemma.

Lemma 3.3.21. *Let $A \in \operatorname{Aoverlap}(F)$ and $f \in F$. If $A + \operatorname{vect}(f) \geq \operatorname{overlap}(F)$, then $(A - \operatorname{e}(\operatorname{tt}(f)) + \operatorname{posshift}(f))$ is a vpc from A to $A + \operatorname{vect}(f)$. If $A - \operatorname{vect}(f) \geq \operatorname{overlap}(F)$, then $(A - \operatorname{e}(\operatorname{lt}(f)) + \operatorname{negshift}(f))$ is a vpc from A to $A - \operatorname{vect}(f)$.*

Proof. Assume, $A + \mathrm{vect}(f) \geq \mathrm{overlap}(F)$ and $(A - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f))$ is not a vpc from A to $A + \mathrm{vect}(f)$. This can only be the case if $A - \mathrm{e}(\mathrm{tt}(f)) \notin \mathbb{N}^n$. Let therefore $i \in \mathbb{N}_n$ such that

$$A_i < \mathrm{e}(\mathrm{tt}(f))_i. \tag{3.3}$$

From this we derive

$$\begin{aligned} A_i + \mathrm{vect}(f)_i &= A_i + \mathrm{e}(\mathrm{lt}(f))_i - \mathrm{e}(\mathrm{tt}(f))_i \\ &< \mathrm{e}(\mathrm{lt}(f))_i. \end{aligned} \tag{3.4}$$

From $A \geq \mathrm{overlap}(F)$ and (3.3) we get

$$\begin{aligned} A_i &\geq \mathrm{gcd}(\mathrm{e}(\mathrm{lt}(f)), \mathrm{e}(\mathrm{tt}(f)))_i \\ &= \min(\mathrm{e}(\mathrm{lt}(f))_i, \mathrm{e}(\mathrm{tt}(f))_i) \\ &= \mathrm{e}(\mathrm{lt}(f))_i, \end{aligned}$$

hence, $\mathrm{e}(\mathrm{lt}(f))_i < \mathrm{e}(\mathrm{tt}(f))_i$. From $A + \mathrm{vect}(f) \geq \mathrm{overlap}(F)$ and (3.4) we get

$$\begin{aligned} A_i + \mathrm{vect}(f)_i &\geq \mathrm{gcd}(\mathrm{e}(\mathrm{lt}(f)), \mathrm{e}(\mathrm{tt}(f)))_i \\ &= \min(\mathrm{e}(\mathrm{lt}(f))_i, \mathrm{e}(\mathrm{tt}(f))_i) \\ &= \mathrm{e}(\mathrm{tt}(f))_i, \end{aligned}$$

hence, $\mathrm{e}(\mathrm{tt}(f))_i < \mathrm{e}(\mathrm{lt}(f))_i$. This is a contradiction.
The proof for the second claim in the lemma proceeds analogously. □

Theorem 3.3.22. *Let $A, B \in \mathrm{Aoverlap}(F)$, $A \neq B$. Then for any $f \in F$, a vpc from A to B of minimal length cannot contain both a positive shift of f and a negative shift of f.*

Proof. Let z be a vpc from A to B of minimal length. Now assume there is an $f \in F$ such that z contains a nonzero number of positive shifts of f and of negative shifts of f, respectively. Then by Lemma 3.3.19 there must be $m, m' \in \mathbb{N}_{\mathrm{len}(z)}$ with $m + 1 < m'$ such that z_m, w.l.o.g., is a positive shift of f, $z_{m'}$ is a negative shift of f and z_j is either a negative shift of f' for all j with $m + 1 \leq j \leq m' - 1$ or z_j is a positive shift of f' for all j with $m + 1 \leq j \leq m' - 1$, where $f' \in F \setminus \{f\}$. Let w.l.o.g. the latter be the case. From Theorem 3.3.20 we know that

$$z_{m,1} \geq \mathrm{overlap}(F) \tag{3.5}$$

and (note that either $z_{m',2} = B$ or else $z_{m',2} = z_{m'+1,1}$)

$$z_{m',2} \geq \mathrm{overlap}(F). \tag{3.6}$$

We also know that

$$\begin{aligned} z_{m',2} &= z_{m,1} + \operatorname{vect}(f) + (m' - 1 - m)\operatorname{vect}(f') - \operatorname{vect}(f) \\ &= z_{m,1} + (m' - 1 - m)\operatorname{vect}(f'). \end{aligned}$$

We show that for all $\xi \in \mathbb{N}_{m'-1-m}$

$$z_{m,1} + \xi \operatorname{vect}(f') \geq \operatorname{overlap}(F).$$

Assume, there is a $\xi' \in \mathbb{N}_{m'-1-m}$ such that $z_{m,1} + \xi' \operatorname{vect}(f') \not\geq \operatorname{overlap}(F)$. Because of (3.5), this means that $\operatorname{vect}(f')_i < 0$ for some $i \in \mathbb{N}_n$. But then it follows directly that $z_{m',2} = z_{m,1} + (m' - 1 - m)\operatorname{vect}(f') \not\geq \operatorname{overlap}(F)$, which contradicts (3.6). By inductive use of Lemma 3.3.21, it follows that z' given by

$$z'_j = \begin{cases} (z_{m,1} - \mathrm{e}(\mathrm{tt}(f'))) + \operatorname{posshift}(f') & \text{if } j = 1 \\ (z'_{j-1,2} - \mathrm{e}(\mathrm{tt}(f'))) + \operatorname{posshift}(f') & \text{if } 2 \leq j \leq m' - 1 - m \end{cases}$$

is a vpc from $z_{m,1}$ to $z_{m',2}$ with $\operatorname{len}(z') = m' - 1 - m$. Therefore, z'' given by

$$z''_j = \begin{cases} z_j & \text{if } 1 \leq j \leq m - 1 \\ z'_{j-(m-1)} & \text{if } m \leq j \leq m' - 2 \\ z_{j+2} & \text{if } m' - 1 \leq j \leq \operatorname{len}(z) - 2 \end{cases}$$

is a vpc from A to B, since

$$\begin{aligned} z''_{m,1} &= ((z''_{m-1,2} - \mathrm{e}(\mathrm{tt}(f'))) + \operatorname{posshift}(f'))_1 \\ &= (z''_{m-1,2} - \mathrm{e}(\mathrm{tt}(f'))) + (\operatorname{posshift}(f'))_1 \\ &= (z''_{m-1,2} - \mathrm{e}(\mathrm{tt}(f'))) + \mathrm{e}(\mathrm{tt}(f')) \\ &= z''_{m-1,2} \end{aligned}$$

and

$$\begin{aligned} z''_{m'-2,2} &= ((z''_{m'-3,2} - \mathrm{e}(\mathrm{tt}(f'))) + \operatorname{posshift}(f'))_2 \\ &= (z''_{m'-3,2} - \mathrm{e}(\mathrm{tt}(f'))) + (\operatorname{posshift}(f'))_2 \\ &= (z''_{m'-3,2} - \mathrm{e}(\mathrm{tt}(f'))) + \mathrm{e}(\mathrm{lt}(f')) \\ &= z''_{m'-3,2} + \operatorname{vect}(f') \\ &= z''_{m-1,2} + (m' - 1 - m)\operatorname{vect}(f') \\ &= z_{m-1,2} + (m' - 1 - m)\operatorname{vect}(f') \\ &= z_{m,1} + (m' - 1 - m)\operatorname{vect}(f') \\ &= z_{m',2} = z_{m'+1,1} = z''_{m'-1,1}. \end{aligned}$$

We obtain $\text{len}(z'') = (m-1) + \text{len}(z') + (\text{len}(z) - m') = \text{len}(z) - 2$, hence z cannot have minimal length.
Therefore, z cannot contain both a positive shift of f and a negative shift of f. □

3.3.2.2 Degree Bound on a Minimal Valid Polygon Chain

In the next part we derive an upper bound on the degree of a minimal vpc from U to V. In Subsection 3.3.2.1, we described the structure of $\mathfrak{z}$ in the case where $\text{overlapshift}(U) = \text{overlapshift}(V)$. There,

$$\deg(\mathfrak{z}) = \text{maxdeg}(U, V, \text{overlapshift}(U)).$$

So from now on assume $\text{overlapshift}(U) \neq \text{overlapshift}(V)$. We investigate the subproblem of finding a degree bound on a minimal vpc from $\text{overlapshift}(U)$ to $\text{overlapshift}(V)$.

Definition 3.3.23 (Peak/Valley of a vpc)**.** *Let $A, B \in \mathbb{N}^n$, $A \neq B$, and z be a vpc from A to B of minimal length. Assume z consists of a nonzero number of shifts of f and f', respectively, where $f, f' \in \text{shifts}(F)$, $\deg(\text{vect}(f)) \geq 0$ and $\deg(\text{vect}(f')) < 0$.*

An $S \in \mathbb{Z}^n$ is a peak *of z iff there is an $m \in \mathbb{N}_{\text{len}(z)-1}$ such that $S = z_{m,2}$ and z_m is a shift of f and z_{m+1} is a shift of f'.*

An element $T \in \mathbb{Z}^n$ is a valley *of z iff there is an $m \in \mathbb{N}_{\text{len}(z)-1}$ such that $T = z_{m,2}$ and z_m is a shift of f' and z_{m+1} is a shift of f.*

Example 3.3.24. *Let $F = \{X_1^3X_2^4 + X_2^2, 2X_1^2X_2^2 - 1\}$ (c.f. Figure 3.6). The sequence*

$$z = (((0,2),(3,4)),\ ((3,4),(1,2)),\ ((1,2),(4,4)),\ ((4,4),(2,2)),\ ((2,2),(0,0)))$$

is a vpc from $(0,2)$ to $(0,0)$ of minimal length. We have $\text{posshift}(F_1) = ((0,2),(3,4))$ and $\text{negshift}(F_2) = ((2,2),(0,0))$. It therefore consists of two positive shifts of F_1 and three negative shifts of F_2, where

$$\deg(\text{vect}(\text{posshift}(F_1))) = \deg((3,2)) = 5 \geq 0$$

and

$$\deg(\text{vect}(\text{negshift}(F_2))) = \deg((-2,-2)) = -4 < 0.$$

$S = ((3,4))$ and $S' = (4,4)$ are peaks of z since z_1 and z_3 are positive shifts of F_1 and z_2 and z_4 are negative shifts of F_2. $T = (1,2)$ is a valley of z since z_2 is a negative shift of F_2 and z_3 is a positive shift of F_1.

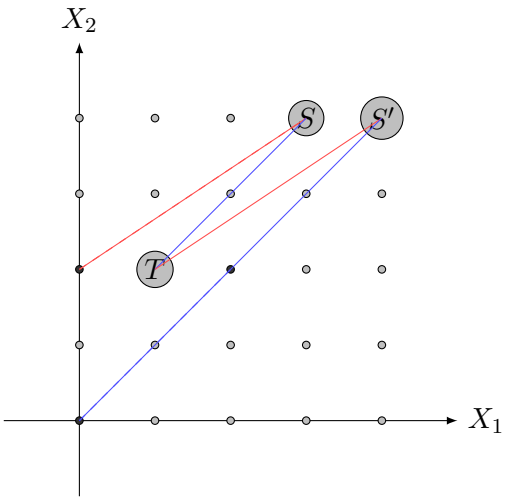


Figure 3.6: Peak and valley of a vpc.

Given a vpc from A to B of minimal length, where $A, B \in \mathbb{N}^n$ with $A \neq B$, we show in the following theorem under which circumstances we can turn a peak into a valley and again obtain a vpc from A to B of minimal length.

Theorem 3.3.25. *Let $A, B \in \mathbb{N}^n$, $A \neq B$, and z be a vpc from A to B of minimal length. Let $m \in \mathbb{N}_{\text{len}(z)-1}$ and $f, f' \in \text{shifts}(F)$ such that $z_{m,2}$ is a peak of z, z_m is a shift of f and z_{m+1} is a shift of f'. Let z' be defined as*

$$z'_j = \begin{cases} z_j & \text{if } 1 \leq j \leq m-1 \\ -\operatorname{vect}(f) + z_{j+1} & \text{if } j = m \\ \operatorname{vect}(f') + z_{j-1} & \text{if } j = m+1 \\ z_j & \text{if } m+2 \leq j \leq \operatorname{len}(z) \end{cases}.$$

If $z'_{m,2} \geq \operatorname{lcm}(f_1, f'_2)$, then z' is also a vpc from A to B of minimal length. Furthermore, $z'_{m,2}$ is a valley of z'.

Proof. We first show that

$$z'_{m-1,2} = z'_{m,1}, \tag{3.7}$$
$$z'_{m,2} = z'_{m+1,1}, \tag{3.8}$$
$$z'_{m+1,2} = z'_{m+2,1}. \tag{3.9}$$

Ad (3.7):

$$\begin{aligned} z'_{m,1} &= z_{m+1,1} - \operatorname{vect}(f) \\ &= (z_{m-1,2} + \operatorname{vect}(f)) - \operatorname{vect}(f) \\ &= z_{m-1,2} \end{aligned}$$

$$= z'_{m-1,2}.$$

Ad (3.8):

$$\begin{aligned} z'_{m+1,1} &= z_{m,1} + \mathrm{vect}(f') \\ &= (z_{m+1,2} - \mathrm{vect}(f') - \mathrm{vect}(f)) + \mathrm{vect}(f') \\ &= z_{m+1,2} - \mathrm{vect}(f) \\ &= z'_{m,2}. \end{aligned}$$

Ad (3.9):

$$\begin{aligned} z'_{m+1,2} &= z_{m,2} + \mathrm{vect}(f') \\ &= (z_{m+2,1} - \mathrm{vect}(f')) + \mathrm{vect}(f') \\ &= z_{m+2,1} \\ &= z'_{m+2,1}. \end{aligned}$$

Since z is a vpc and $z'_{m,2} \geq \mathrm{lcm}(f_1, f'_2)$, it remains to show that $z'_m, z'_{m+1} \in \mathbb{N}^n + \mathrm{shifts}(F)$. We know that z'_m is a shift of f' and z'_{m+1} is a shift of f. From $z'_{m,2} \geq \mathrm{lcm}(f_1, f'_2) \geq f'_2$ it follows that $z'_m \geq f'$, hence $z'_m \in \mathbb{N}^n + \mathrm{shifts}(F)$. From $z'_{m+1,1} = z'_{m,2} \geq \mathrm{lcm}(f_1, f'_2) \geq f_1$ it follows that $z'_{m+1} \geq f$, hence $z'_{m+1} \in \mathbb{N}^n + \mathrm{shifts}(F)$.
Furthermore, since z'_m is a shift of f' and z'_{m+1} is a shift of f, $z'_{m,2}$ is a valley of z'. □

If changing a peak of a vpc into a valley does lead to a new vpc, we can use this to reduce the degree of a vpc.

We now state one of our main theorems in this section. It gives a degree bound on a minimal vpc from overlapshift(U) to overlapshift(V).

Theorem 3.3.26. *Let $A, B \in \mathrm{Aoverlap}(F)$, $A \neq B$, and z be a minimal vpc from A to B. Then* $\deg(z) \leq \mathrm{maxdeg}(A, B) + |\deg(\mathrm{vect}(F_1))| + |\deg(\mathrm{vect}(F_2))|$.

The proof requires four more lemmas and three definitions. First, let us extend the definitions of $\gcd(A, B)$, $\mathrm{lcm}(A, B)$ and $A \leq B$ to $A, B \in \mathbb{R}^n$.

Definition 3.3.27 (gcd, lcm, $\leq$ in $\mathbb{R}^n$)**.** *For $A, B \in \mathbb{R}^n$ we define* $\gcd(A, B)$ *and* $\mathrm{lcm}(A, B)$ *by*

$$\gcd(A, B)_i = \min(A_i, B_i) \text{ for } i \in \mathbb{N}_n$$

and

$$\mathrm{lcm}(A, B)_i = \max(A_i, B_i) \text{ for } i \in \mathbb{N}_n,$$

and

$$A \leq B \text{ (or } B \geq A \text{ respectively) iff } A_i \leq B_i \text{ for all } i \in \mathbb{N}_n.$$

Lemma 3.3.28. *Let $A, B, R \in \mathbb{Z}^n$ such that $A \geq R$ and $B \geq R$. Then* $\gcd(A, B) \geq R$.

Proof. Let $i \in \mathbb{N}_n$. From $A_i \geq R_i$ and $B_i \geq R_i$ it follows that $\min(A_i, B_i) \geq R_i$. Hence, $\gcd(A, B) \geq R$. □

Lemma 3.3.29. *Let $A, B, R \in \mathbb{Z}^n$. Then* $R + \gcd(A, B) = \gcd(R + A, R + B)$.

Proof. Let $i \in \mathbb{N}_n$. We get

$$\begin{aligned}(R + \gcd(A, B))_i &= R_i + \min(A_i, B_i) \\ &= \min(R_i + A_i, R_i + B_i) \\ &= \gcd(R + A, R + B)_i.\end{aligned}$$

□

Lemma 3.3.30. *Let $f, f' \in \text{shifts}(F)$ such that they are not shifts of the same input binomial and such that* $\deg(\text{vect}(f)) \geq 0$ *and* $\deg(\text{vect}(f')) < 0$. *Let $R \in \mathbb{Z}^n$ such that*

$$\begin{aligned}R &\ngeq \text{lcm}(f_1, f_2'), \\ R + \text{vect}(f) &\geq \text{overlap}(F), \\ R - \text{vect}(f') &\geq \text{overlap}(F).\end{aligned}$$

Then $R \ngeq \text{overlap}(F)$.

Proof. Assume, $R \geq \text{overlap}(F)$. Since $R \ngeq \text{lcm}(f_1, f_2')$, it follows that $R \ngeq f_1$ or $R \ngeq f_2'$. Assume w.l.o.g. $R \ngeq f_1$. We know

$$R \geq \text{overlap}(F) \geq \gcd(f_1, f_2)$$

and

$$R + \text{vect}(f) \geq \text{overlap}(F) \geq \gcd(f_1, f_2).$$

By, first, Lemma 3.3.28 and, then, Lemma 3.3.29 we get

$$\begin{aligned}\gcd(f_1, f_2) &\leq \gcd(R, R + \text{vect}(f)) \\ &= R + \gcd(0, \text{vect}(f)) \\ &= R + \gcd(0, f_2 - f_1),\end{aligned}$$

which by Lemma 3.3.29 leads to

$$\gcd(f_1, f_2) + f_1 \leq R + \gcd(f_1, f_2),$$

hence $f_1 \leq R$, which contradicts our assumption that $R \not\geq f_1$.
Therefore, $R \not\geq \text{overlap}(F)$. □

Let us extend our view from $\mathbb{Z}^n$ to $\mathbb{R}^n$.

Definition 3.3.31 ($\text{cone}_{\mathbb{N}}(H,A,B)$,$\text{cone}_{\mathbb{R}}(H,A,B)$)**.** *For $H, A, B \in \mathbb{Z}^n$, we define*

$$\text{cone}_{\mathbb{N}}(H,A,B) := \{H + \lambda A + \mu B \mid \lambda, \mu \in \mathbb{N} \setminus \{0\}\},$$

and

$$\text{cone}_{\mathbb{R}}(H,A,B) := \{H + \lambda A + \mu B \mid \lambda, \mu \in \mathbb{R}^+\}.$$

Note that $\text{cone}_{\mathbb{N}}(H,A,B) \subset \text{cone}_{\mathbb{R}}(H,A,B)$.

Definition 3.3.32. *For $A, B \in \mathbb{R}^n$ we define* $\text{conn}(A,B) := \{(1-\lambda)A + \lambda B \mid \lambda \in [0,1]\}$ *to be the connecting line between A and B.*

Lemma 3.3.33. *Let $H, A, B \in \mathbb{Z}^n$, $R \in \text{cone}_{\mathbb{R}}(H,A,B)$ and $C, D \in \mathbb{Z}^n$ such that there exist $k, k' \in \mathbb{R}^+$ such that $C = H + kA$ and $D = H + k'B$. Then there exist $L \in \text{conn}(C,D)$ and $\lambda \in \mathbb{R}^+$ such that $R = H + \lambda(L - H)$.*

Proof. Let $l, l' \in \mathbb{R}^+$ such that $R = H + lA + l'B$. We obtain that the following should hold for some $\lambda \in \mathbb{R}^+$ and some $\mu \in [0,1]$:

$$\begin{aligned} lA + l'B &= R - H \\ &= \lambda(L - H) \\ &= \lambda((1-\mu)C + \mu D - H) \\ &= (1-\mu)\lambda kA + \mu\lambda k'B + (1-\mu)H + \mu H - H \\ &= (1-\mu)\lambda kA + \mu\lambda k'B. \end{aligned}$$

This leads to the following system of equations

$$\begin{cases} l &= (1-\mu)\lambda k \\ l' &= \mu\lambda k', \end{cases}$$

which we solve for λ and μ and obtain $\lambda = \frac{k'l + kl'}{kk'} \in \mathbb{R}^+$ and $\mu = \frac{kl'}{k'l + kl'} \in [0,1]$. □

Proof of Theorem 3.3.26. By Theorem 3.3.22, z consists either of a nonzero number of shifts of f for an $f \in \text{shifts}(F)$ or of a nonzero number of shifts of f and f', respectively, where $f, f' \in \text{shifts}(F)$ are shifts of two different input binomials.

If z only consists of a nonzero number of shifts of f, where $f \in \text{shifts}(F)$, we obtain

$$\begin{aligned}\deg(z) &= \text{maxdeg}(A, B)\\ &\leq \text{maxdeg}(A, B) + |\deg(\text{vect}(F_1))| + |\deg(\text{vect}(F_2))|.\end{aligned}$$

Let now $f, f' \in \text{shifts}(F)$ be shifts of two different input binomials such that z consists of a nonzero number of shifts of f and f'. We distinguish two cases.

In the case that ($\deg(\text{vect}(f)) \geq 0$ and $\deg(\text{vect}(f')) \geq 0$) or ($\deg(\text{vect}(f)) \leq 0$ and $\deg(\text{vect}(f')) \leq 0$) we again obtain

$$\begin{aligned}\deg(z) &= \text{maxdeg}(A, B)\\ &\leq \text{maxdeg}(A, B) + |\deg(\text{vect}(F_1))| + |\deg(\text{vect}(F_2))|.\end{aligned}$$

For the second case assume $\deg(\text{vect}(f)) \geq 0$ and $\deg(\text{vect}(f')) < 0$. Let z' be a vpc from A to B of minimal length $\text{len}(z)$ consisting of k shifts of f and k' shifts of f', where $k, k' \in \mathbb{N} \setminus \{0\}$. Starting from z', we successively generate new vpcs by turning peaks into valleys if the resulting valleys R fulfill $R \geq \text{lcm}(f_1, f_2')$ (c.f. Theorem 3.3.25). Their degrees do not increase and their number of respective shifts remains unchanged in each iteration step. The procedure stops if either there are no more peaks in the current vpc or no remaining peak may be changed anymore, because the resulting valley R would not fulfill $R \geq \text{lcm}(f_1, f_2')$. The number of operations is bounded by $(k+1)(k'+1) - (k+k'-1) - 2$, since the number of peaks in a vpc from A to B of minimal length $k + k'$ is bounded by $(k+1)(k'+1) - (k+k'-1) - 2$ (note that A and B cannot be peaks). In the case that the procedure stops with a vpc that does not contain any peaks, this vpc is a minimal vpc and has degree

$$\deg(z) = \text{maxdeg}(A, B) \leq \text{maxdeg}(A, B) + |\deg(\text{vect}(F_1))| + |\deg(\text{vect}(F_2))|.$$

So now assume that it stops with a vpc z'' that does contain peaks. We know $\text{len}(z) = \text{len}(z'')$ and $\deg(z) \leq \deg(z'')$, so it suffices to find an upper bound on

$$\deg(z'') = \max(\{\deg(A), \deg(B)\} \cup \{\deg(P) \in \mathbb{Z}^n \mid P \text{ is a peak in } z''\}). \tag{3.10}$$

Let $H := A + k\,\text{vect}(f) = B - k'\,\text{vect}(f')$. H is not necessarily an element of $\mathbb{N}^n$. Every vpc z''' from A to B consisting of k shifts of f and k' shifts of f' fulfills

$$z'''_{j,2} \in \text{cone}_{\mathbb{N}}(H, -\text{vect}(f), \text{vect}(f'))$$

for all $j \in \mathbb{N}_{\text{len}(z)-1}$. Let P be a peak in z''. Then there exists an $R \in \mathbb{Z}^n$ such that $R \not\geq \text{lcm}(f_1, f_2')$ and $R + \text{vect}(f) - \text{vect}(f') = P$. Note that R is the valley we couldn't change P into. This point R fulfills the following:

$$R \in \text{cone}_{\mathbb{N}}(H, -\text{vect}(f), \text{vect}(f')), \tag{3.11}$$

$$P = R + \text{vect}(f) - \text{vect}(f'), \tag{3.12}$$

$$R \not\geq \text{lcm}(f_1, f_2'), \tag{3.13}$$

$$R + \text{vect}(f) \geq \text{overlap}(F), \tag{3.14}$$

$$R - \text{vect}(f') \geq \text{overlap}(F). \tag{3.15}$$

By Lemma 3.3.30, from (3.13)–(3.15) additionally follows

$$R \not\geq \text{overlap}(F). \tag{3.16}$$

We show $\deg(R) \leq \text{maxdeg}(A, B)$. Let $a, b \in \mathbb{N}$ be maximal such that

$$A' := A - a\,\text{vect}(f) \geq \text{overlap}(F)$$

and

$$B' := B + b\,\text{vect}(f') \geq \text{overlap}(F).$$

Since $\deg(A') \leq \deg(A) \leq \text{maxdeg}(A, B)$ and $\deg(B') \leq \deg(B) \leq \text{maxdeg}(A, B)$, it suffices to show $\deg(R) \leq \text{maxdeg}(A', B')$.
Since $A' \geq \text{overlap}(F)$ and $B' \geq \text{overlap}(F)$, we have

$$L'' \geq \text{overlap}(F) \text{ for all } L'' \in \text{conn}(A', B'). \tag{3.17}$$

Additionally, we know

$$\deg(L'') \leq \text{maxdeg}(A', B') \text{ for all } L'' \in \text{conn}(A', B'). \tag{3.18}$$

Note that $A' = H + (k + a)(-\text{vect}(f))$ and $B' = H + (k' + b)(\text{vect}(f'))$ with $k + a > 0$ and $k' + b > 0$. By Lemma 3.3.33 and (3.11), there are $L \in \text{conn}(A', B')$ and $\lambda \in \mathbb{R}^+$ such that $R = H + \lambda(L - H)$. We show that $\lambda \in (1, \infty)$.

Assume $\lambda \in (0, 1]$. Then there are two cases: $H \geq \text{overlap}(F)$ and $H \not\geq \text{overlap}(F)$.
First assume $H \geq \text{overlap}(F)$. Since by (3.17) $L \geq \text{overlap}(F)$, we also know that $R' \geq \text{overlap}(F)$ for all $R' \in \text{conn}(H, L)$. But since by case assumption $R \in \text{conn}(H, L)$, this implies $R \geq \text{overlap}(F)$, which contradicts (3.16).
Now assume $H \not\geq \text{overlap}(F)$. From (3.14) and (3.15) we obtain

$$R' \geq \text{overlap}(F) \text{ for all } R' \in \mathcal{L} := \text{conn}(R + \text{vect}(f), R - \text{vect}(f')). \tag{3.19}$$

Furthermore, we have

$$R \in \text{cone}_{\mathbb{R}}(H, R + \text{vect}(f) - H, R - \text{vect}(f') - H), \tag{3.20}$$

since

$$R = H + \frac{r}{r+r'-1}(R + \operatorname{vect}(f) - H) + \frac{r'}{r+r'-1}(R - \operatorname{vect}(f') - H),$$

where $r, r' \in \mathbb{N} \setminus \{0\}$ such that $R = H - r\operatorname{vect}(f) + r'\operatorname{vect}(f')$, which exist because of (3.11). We also have

$$R + \operatorname{vect}(f) = H + 1(R + \operatorname{vect}(f) - H), \tag{3.21}$$

and

$$R - \operatorname{vect}(f') = H + 1(R - \operatorname{vect}(f') - H). \tag{3.22}$$

By (3.20)–(3.22) and Lemma 3.3.33, there exist $L' \in \mathcal{L}$ and $\lambda' \in \mathbb{R}^+$ such that $R = H + \lambda'(L' - H)$. Since $H \not\geq \operatorname{overlap}(F)$ by case assumption and $L' \geq \operatorname{overlap}(F)$ by (3.19), there exists a minimal $\xi \in [0,1]$ such that $H + \mu(L' - H) \not\geq \operatorname{overlap}(F)$ for all $\mu \in [0, \xi)$ and $H + \mu(L' - H) \geq \operatorname{overlap}(F)$ for all $\mu \in [\xi, 1]$. We obtain $\lambda' \in (0, \xi)$ and hence $\lambda' \in (0,1)$.
Let now $\zeta \in [0,1]$ such that $L' = (1-\zeta)(R + \operatorname{vect}(f)) + \zeta(R - \operatorname{vect}(f'))$. We obtain

$$\begin{aligned} R &= H + \lambda'(L' - H) \\ &= H + \lambda'((1-\zeta)(R + \operatorname{vect}(f)) + \zeta(R - \operatorname{vect}(f'))) - \lambda' H, \\ &= H + \lambda' R + \lambda' \operatorname{vect}(f) + \lambda'\zeta(-\operatorname{vect}(f) - \operatorname{vect}(f')) - \lambda' H, \end{aligned}$$

hence,

$$(1-\lambda')R = (1-\lambda')H + \lambda'(1-\zeta)\operatorname{vect}(f) - \lambda'\zeta\operatorname{vect}(f')$$

and therefore,

$$R = H - \frac{\lambda'(1-\zeta)}{1-\lambda'}(-\operatorname{vect}(f)) - \frac{\lambda'\zeta}{1-\lambda'}\operatorname{vect}(f').$$

We have $\lambda' \in (0,1)$, $1-\lambda' \in (0,1)$, $\zeta \in [0,1]$, $1-\zeta \in [0,1]$, $\lambda'\zeta \in [0,1)$ and $\lambda'(1-\zeta) \in [0,1)$. Therefore, $-\frac{\lambda'(1-\zeta)}{1-\lambda'} \in \mathbb{R}_0^-$ and $-\frac{\lambda'\zeta}{1-\lambda'} \in \mathbb{R}_0^-$. This implies $R \notin \operatorname{cone}_{\mathbb{N}}(H, -\operatorname{vect}(f), \operatorname{vect}(f'))$, which contradicts (3.11). We conclude that $\lambda \in (1, \infty)$.

For all $L'' \in \operatorname{cone}_{\mathbb{R}}(H, -\operatorname{vect}(f), \operatorname{vect}(f'))$ we know that $\deg(L'') \leq \deg(H)$, hence $\deg(H + \zeta'(L'' - H)) \leq \deg(H + \zeta''(L'' - H))$ for any $\zeta', \zeta'' \in \mathbb{R}_0^+$, $\zeta' \geq \zeta''$. Since $L \in \operatorname{cone}_{\mathbb{R}}(H, -\operatorname{vect}(f), \operatorname{vect}(f'))$, this leads to

$$\begin{aligned} \deg(R) &= \deg(H + \lambda(L - H)) \\ &\leq \deg(H + 1(L - H)) \\ &= \deg(L). \end{aligned}$$

Since $\deg(L) \leq \operatorname{maxdeg}(A', B')$ by (3.18), it follows that

$$\begin{aligned}\deg(R) &\leq \operatorname{maxdeg}(A', B') \\ &\leq \operatorname{maxdeg}(A, B).\end{aligned}$$

Therefore, by (3.10) and (3.12),

$$\begin{aligned}\deg(z) &\leq \deg(z'') \\ &\leq \operatorname{maxdeg}(A, B) + \deg(\operatorname{vect}(f)) - \deg(\operatorname{vect}(f')) \\ &\leq \operatorname{maxdeg}(A, B) + |\deg(\operatorname{vect}(f))| + |\deg(\operatorname{vect}(f'))| \\ &\leq \operatorname{maxdeg}(A, B) + |\deg(\operatorname{vect}(F_1))| + |\deg(\operatorname{vect}(F_2))|.\end{aligned}$$

□

Together with the remarks at the beginning of subsections 3.3.2.1 and 3.3.2.2, this theorem leads to the following bound for $\deg(\mathfrak{z})$.

Theorem 3.3.34. *Let $A, B \in \mathbb{N}^n$ such that $A \neq B$, $\operatorname{e}(\operatorname{lt}(f)) \not\leq A$ and $\operatorname{e}(\operatorname{lt}(f)) \not\leq B$ for any $f \in F$, and let z be a minimal vpc from A to B. Then*

$$\deg(z) \leq \max(\operatorname{maxdeg}(A, B),\ \operatorname{maxdeg}(\operatorname{overlapshift}(A), \operatorname{overlapshift}(B)) + m),$$

where $m = |\deg(\operatorname{vect}(F_1))| + |\deg(\operatorname{vect}(F_2))|$.

From this we derive the following theorem.

Theorem 3.3.35. *Let F consist of two proper binomials and let $g \in \operatorname{ideal}(F)$ be a proper binomial irreducible with respect to F such that $\operatorname{supp}(g) \not\subseteq \operatorname{ideal}(F)$. Furthermore, let $A = \operatorname{e}(\operatorname{lt}(g))$, $B = \operatorname{e}(\operatorname{tt}(g))$ and $m = |\deg(\operatorname{vect}(F_1))| + |\deg(\operatorname{vect}(F_2))|$. Then*

$$d' = \max(\operatorname{maxdeg}(A, B),\ \operatorname{maxdeg}(\operatorname{overlapshift}(A), \operatorname{overlapshift}(B)) + m)$$

solves Problem 3.1.5.

Note that in Theorems 3.2.1 and 3.2.2, $k = \operatorname{step}(\operatorname{e}(\operatorname{lt}(g)))$, so the formulas for the degree bounds of the cofactors are similar.

Chapter 4

New Bounds for Gröbner Bases Computation for Binomial Ideals

4.1 Introduction and Summary of the Main Results

In this chapter we give degree bounds for the shifts of the input polynomials needed to compute a Gröbner basis the way described in Chapter 2 for the case, where the input polynomials are two binomials.

In this subsection we give a summary of the main results in this chapter. The proofs follow in Subsections 4.2, 4.3, 4.4 and 4.5.

We consider the following two problems.

Problem 4.1.1.
Find an explicit expression d in two natural numbers and four terms such that for all F, m, n, r, r', s, s'

if $m = \mathrm{maxdeg}(F)$, $n = |[X]|$, $\mathrm{supp}(F_1) \subseteq \{r, r'\}$ *and* $\mathrm{supp}(F_2) \subseteq \{s, s'\}$

then *there exists a Gröbner basis G such that for all $g \in G$ there exist $q_1, q_2 \in \mathbb{K}[X]$ such that $g = q_1F_1 + q_2F_2$ and, if $q_i \neq 0$, $\deg(q_iF_i) \leq d(m, n, r, r', s, s')$ for all $i = 1, 2$.*

Problem 4.1.2.
Find an explicit expression d in four terms such that for all F, r, r', s, s'

if $\mathrm{supp}(F_1) \subseteq \{r, r'\}$ *and* $\mathrm{supp}(F_2) \subseteq \{s, s'\}$

then *there exists a Gröbner basis G such that for all $g \in G$ there exist $q_1, q_2 \in \mathbb{K}[X]$ such that $g = q_1F_1 + q_2F_2$ and, if $q_i \neq 0$, $\deg(q_iF_i) \leq d(r, r', s, s')$ for all $i = 1, 2$.*

If we have a d as specified in Problem 4.1.1 or 4.1.2, respectively, then by Theorem 2.3.3 this is a degree bound for the shifts in the generalized Sylvester matrix.

As mentioned in the last chapter, if F contains only monomials, then F already is a Gröbner basis, so we will not consider this case.

Before we summarize our main results we give the following definitions and algorithm. Recall also the definitions at the beginning of Chapter 3.

Definition 4.1.3 (A^+, A^-)**.** *Let $A \in \mathbb{Z}^n$. We define A^+ and A^- by*

$$(A^+)_i := \begin{cases} A_i & \text{if } A_i > 0 \\ 0 & \text{otherwise} \end{cases}$$

and

$$(A^-)_i := \begin{cases} -A_i & \text{if } A_i < 0 \\ 0 & \text{otherwise} \end{cases}$$

for $i \in \mathbb{N}_n$. Note that $A = A^+ - A^-$.

Definition 4.1.4. *We define $\Omega_\prec := \{v \in \mathbb{Z}^n \mid v^- \prec v^+\}$. For a $v \in \mathbb{Z}^n$ and an $H \subseteq \mathbb{Z}^n$ we define* $\operatorname{negind}(v) := \{i \in \mathbb{N}_n \mid v_i \leq 0\}$ *and* $\operatorname{negind}(H) := \bigcup_{v \in H} \operatorname{negind}(v)$.

Algorithm 4.1.5.

Input: *F, a set of two proper binomials*

Output: *$V(F)$, a finite sequence of tuples of the form $((k,k'),w) \in \mathbb{Z}^2 \times \mathbb{N}^n$, where $k\operatorname{vect}(F_1) + k'\operatorname{vect}(F_2) = w$, $w \in \Omega_\prec$ and $\bigcup_{j \in \operatorname{len}(V)} \operatorname{negind}(V_{j,2}) = \mathbb{N}_n$, such that $V_i \in \{v, -v\}$ for all $i \in \mathbb{N}_{\operatorname{len}(V)}$, where $v = V(F)_{\max(\{j \in \mathbb{N}_{i-1} \mid V(F)_{j,1,1} > 0\})} - V(F)_{\max(\{j \in \mathbb{N}_{i-1} \mid V(F)_{j,1,2} > 0\})}$*

$V \leftarrow (((1,0), \operatorname{vect}(F_1)), ((0,1), \operatorname{vect}(F_2)))$;
$E \leftarrow \operatorname{negind}(\operatorname{vect}(F_1)) \cup \operatorname{negind}(\operatorname{vect}(F_2))$;
$c \leftarrow 1$;
$c' \leftarrow 2$;
while $E \neq \mathbb{N}_n$
  $v \leftarrow V_c - V_{c'}$;
  if $v_2 \in \Omega_\prec$ ***then*** $V \leftarrow \operatorname{append}(V, v)$; $c \leftarrow \operatorname{len}(V)$; $E \leftarrow E \cup \operatorname{negind}(v_2)$;
    else $V \leftarrow \operatorname{append}(V, -v)$; $c' \leftarrow \operatorname{len}(V)$; $E \leftarrow E \cup \operatorname{negind}(-v_2)$;
  end if;
end while;
Return V;

In the algorithm above, $\operatorname{append}(V, v)$ appends the tuple v to the sequence V.

Example 4.1.6. *For input* $F = \{X_1^6X_2^3X_3^2X_4^2 - X_1^2X_2^6X_4,\ X_1^9X_2^2X_4^3 - X_3^4\}$ *with respect to the degree lexicographic ordering with* $X_4 \prec X_3 \prec X_2 \prec X_1$*, Algorithm 4.1.5 yields*

$$\begin{aligned} V(F) = (&((1,0),(4,-3,2,1)),\ ((0,1),(9,2,-4,3)),\ ((-1,1),(5,5,-6,2)),\\ &((-2,1),(1,8,-8,1)),\ ((3,-1),(3,-11,10,0)),\ ((5,-2),(2,-19,18,-1)),\\ &((-7,3),(-1,27,-26,2))) \end{aligned}$$

A correctness and termination proof of Algorithm 4.1.5 is given in Theorem 4.5.6. The termination proof also proves an upper bound on the iterations of the while loop. Let

$$m := \max(\{\max(\operatorname{vect}(F_1)_j, \operatorname{vect}(F_2)_j) \mid j \in \mathbb{N}_n, \operatorname{vect}(F_1)_j > 0, \operatorname{vect}(F_2))_j > 0\}).$$

Then there are at most m iterations of the while loop in Algorithm 4.1.5. This number itself is bounded by

$$m' := \max(\{\operatorname{vect}(F_i)_j \mid i \in \{1,2\}, j \in \mathbb{N}_n\}).$$

Example 4.1.7. *Assume* F *is such that* $\operatorname{vect}(F_1) = (2,3,-4,6)$ *and* $\operatorname{vect}(F_2) = (1,4,-4,0)$*. Then there are at most* $m = 4$ *iterations of the while loop.*

We now summarize our main results and give some examples.

General Bound using the results from Chapter 3 and Dubé:
(c.f. Corollary 4.2.3). Let

$$\begin{aligned} d'' := \max(\{&\operatorname{step}(\mathrm{e}(\mathrm{tt}(f)))\deg(\operatorname{vect}(f)) \mid\\ &f \in F, |\operatorname{supp}(f)| = 2, \deg(\operatorname{vect}(f)) \geq 0\} \cup \{0\}). \end{aligned}$$

Then

$$d := \left\lfloor 2\left(\frac{\operatorname{maxdeg}(F)^2}{2} + \operatorname{maxdeg}(F)\right)^{2^{n-1}} \right\rfloor + d'' + |\deg(\operatorname{vect}(F_1))| + |\deg(\operatorname{vect}(F_2))|$$

solves Problem 4.1.1.

Example 4.1.8. *Consider* $F = \{4X_1^8X_2^3X_3^2 - 3X_2^5X_3,\ X_1X_2^7 + 2X_1^2X_3\}$*. As the term ordering we choose the degree lexicographic ordering with* $X_3 \prec X_2 \prec X_1$*. We have* $\operatorname{maxdeg}(F) = 13$*,* $n = 3$*,* $\operatorname{overlap}(F) = (1,3,1)$*,* $\operatorname{vect}(F_1) = (7,-2,1)$*,* $\operatorname{vect}(F_2) = (-1,7,-1)$*,* $\operatorname{step}(\mathrm{e}(\mathrm{tt}(F_1))) = 1$ *and* $\operatorname{step}(\mathrm{e}(\mathrm{tt}(F_2))) = 1$*. We compute* $d'' = \max(6,5) = 6$ *and get* $d = 180\,737\,595$ *as a degree bound on the shifts in the Sylvester matrix. The bound in Theorem 2.3.6 yields* $181\,195\,269$ *for the degree of the shifts. The optimal number is* 20*.*

Even though here, the Hermann part of the bound in Theorem 2.3.6 has been significantly improved, the Dubé part still yields a very high bound. In the following we give improved bounds for certain cases of input binomials. **Case 1:** F consists of a proper binomial f and a monomial f' (c.f. Theorem 4.3.2).
Let $P = \mathrm{lcm}(\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f))), \mathrm{overlap}(F))$. Then

$$d = \mathrm{maxdeg}(P, P - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f))$$

solves Problem 4.1.2 and is optimal among all the solutions.

Example 4.1.9. *Suppose* $F = \{X_1X_2X_3^5 + 3X_1^3X_2^2, 2X_3^7\}$ *and assume the terms are ordered with respect to the degree lexicographic ordering with* $X_3 \prec X_2 \prec X_1$. *With the notation above we have* $f = X_1X_2X_3^5 + 3X_1^3X_2^2$ *and* $f' = 2X_3^7$. *We compute* $\mathrm{overlap}(F) = (1,1,7)$, $\mathrm{vect}(f) = (-2,-1,5)$, $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f))) = 2$ *and* $\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f))) = (-1,0,10)$. *We get* $P = (1,1,10)$ *and hence the optimal*

$$d = \mathrm{maxdeg}((1,1,10),(5,3,0)) = \max(12,8) = 12.$$

Using Theorem 2.3.6 we get 2 007 753 *as an upper degree bound on the necessary shifts in the Sylvester matrix, using the general bound above we get* 1 969 126.

Case 2: F consists of two proper binomials f, f' such that $r\,\mathrm{vect}(f) = \mathrm{vect}(f')$ for some $r \in \mathbb{Q} \setminus \{0\}$ (c.f. Theorem 4.4.1).
Let $V := \mathrm{vect}(f) + \mathrm{vect}(f')$, $P := \mathrm{lcm}(\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f))) + V, \mathrm{overlap}(F))$ and $P' := \mathrm{lcm}(\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f'))) + V, \mathrm{overlap}(F))$. Then

$$d = \mathrm{maxdeg}(P, P - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f) - V, P', P' - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f')))\,\mathrm{vect}(f') - V)$$

solves Problem 4.1.2.

Example 4.1.10. *Suppose* $F = \{X_1^6X_2^8 + 5X_1^2X_2^{10}, 3X_1^{11} - 2X_1^5X_2^3\}$ *and assume the terms are ordered with respect to the degree lexicographic ordering with* $X_2 \prec X_1$. *With the notation above we have* $f = X_1^6X_2^8 + 5X_1^2X_2^{10}$, $f' = 3X_1^{11} - 2X_1^5X_2^3$, $\mathrm{vect}(f) = (4,-2)$, $\mathrm{vect}(f') = (6,-3)$ *and* $r = \frac{3}{2}$. *We compute* $V = (10,-5)$, $\mathrm{overlap}(F) = (5,8)$, $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f))) = 1$, $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f'))) = 0$, $\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f))) = (6,8)$ *and* $\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f'))) = (5,3)$. *We get* $P = (16,8)$, $P' = (15,8)$ *and hence*

$$d = \mathrm{maxdeg}((16,8),(2,15),(15,8),(5,13)) = 24.$$

Using Theorem 2.3.6 we get 25 914 *as an upper degree bound on the necessary shifts in the Sylvester matrix, using the general bound above we get* 25 095. *The optimal bound is* 22.

Case 3: F consists of two proper binomials f, f' such that $r\,\mathrm{vect}(f) \neq \mathrm{vect}(f')$ for any $r \in \mathbb{Q} \setminus \{0\}$ and $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f'))) = 0$ (c.f. Theorem 4.5.30).
Let $V(F)$ be the output of Algorithm 4.1.5 and

$$T = \gcd(\mathrm{e}(\mathrm{tt}(f)) + \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f),\, \mathrm{overlap}(F))$$

and

$$T' = \gcd(T + \mathrm{vect}(f) + \mathrm{vect}(f'),\, \mathrm{overlap}(F)) - (\mathrm{vect}(f) + \mathrm{vect}(f')).$$

Then

$$\begin{aligned} d =& \,\mathrm{maxdeg}(T',\, T' + \mathrm{vect}(f) + \mathrm{vect}(f')) \\ &+ \max(\{\mathrm{maxdeg}((V(F)_{i,2})^-, (V(F)_{i,2})^+) \mid i \in \mathbb{N}_{\mathrm{len}(V(F))}\}) \\ &+ \max(0,\, \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\deg(-\,\mathrm{vect}(f))) \end{aligned}$$

solves Problem 4.1.2.

Example 4.1.11. *Consider* $F = \{X_1^8X_2^4 - X_1^4X_2^3,\, X_1^{11}X_2 - X_1^4X_2^2\}$. *As the term ordering we choose the lexicographic ordering with* $X_2 \prec X_1$. *With the notation above we have* $f = X_1^8X_2^4 - X_1^4X_2^3$, $f' = X_1^{11}X_2 - X_1^4X_2^2$, $\mathrm{vect}(f) = (4,1)$, $\mathrm{vect}(f') = (7,-1)$, $\mathrm{overlap}(F) = (4,3)$ *and* $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f))) = \mathrm{step}(\mathrm{e}(\mathrm{tt}(f'))) = 0$. *Algorithm 4.1.5 returns*

$$\begin{aligned} V(F) =& (((1,0),(4,1)),\, ((0,1),(7,-1)),\, ((-1,1),(3,-2)),\, ((2,-1),(1,3)), \\ & ((-3,2),(2,-5)),\, ((-5,3),(1,-8)),\, ((7,-4),(0,11))). \end{aligned}$$

We compute $T = \mathrm{e}(\mathrm{tt}(f)) = (4,3)$ *and* $T' = T$, *and obtain*

$$d = \max(7, 7+11) + \max(5,7,3,4,5,8,11) + 0 = 29.$$

Using the bound in Theorem 2.3.6 we obtain 14 724 *as an upper degree bound on the necessary shifts in the Sylvester matrix and using the general bound above we get* 14 123. *The optimal number is* 22.

Example 4.1.12. *Consider* $F = \{X_1^8X_2^4X_3^2 - X_1^4X_2^3X_3,\, X_1^{10}X_2X_3^3 - X_1^4X_2^2X_3^4\}$. *As the term ordering we choose the degree lexicographic ordering with* $X_3 \prec X_2 \prec X_1$. *With the notation above we have* $f = X_1^8X_2^4X_3^2 - X_1^4X_2^3X_3$, $f' = X_1^{10}X_2X_3^3 - X_1^4X_2^2X_3^4$, $\mathrm{vect}(f) = (4,1,1)$, $\mathrm{vect}(f') = (6,-1,-1)$, $\mathrm{overlap}(F) = (4,3,3)$, $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f))) = 2$ *and* $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f'))) = 0$. *Algorithm 4.1.5 returns*

$$V(F) = (((1,0),(4,1,1)),\, ((0,1),(6,-1,-1)),\, ((1,-1),(-2,2,2))).$$

We compute $T = (12,5,3)$ *and* $T' = T$, *and obtain*

$$d = \max(20, 20+10) + \max(6,6,4) + \max(0,-12) = 36.$$

Using the bound in Theorem 2.3.6 we obtain 315 319 354 *as an upper degree bound on the necessary shifts in the Sylvester matrix and using the general bound above we get* 314 703 894. *The optimal number is* 26.

Example 4.1.13. *Consider* $F = \{X_1^8X_2^4X_3^2 - X_1^4X_2^3X_3,\ X_1^{10}X_2X_3^3 - X_1^4X_2^2X_3^6\}$. *As the term ordering we choose the degree lexicographic ordering with* $X_3 \prec X_2 \prec X_1$. *With the notation above we have* $f = X_1^8X_2^4X_3^2 - X_1^4X_2^3X_3$, $f' = X_1^{10}X_2X_3^3 - X_1^4X_2^2X_3^6$, $\mathrm{vect}(f) = (4,1,1)$, $\mathrm{vect}(f') = (6,-1,-3)$, $\mathrm{overlap}(F) = (4,3,3)$, $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f))) = 2$ *and* $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f'))) = 0$. *Algorithm 4.1.5 returns*

$$V(F) = (((1,0),(4,1,1)),\ ((0,1),(6,-1,-3)),\ ((1,-1),(-2,2,4))).$$

We compute $T = (12,5,3)$ *and* $T' = (12,5,5)$, *and obtain*

$$d = \max(22, 22+8) + \max(6,6,6) + \max(0,-12) = 36.$$

Using the bound in Theorem 2.3.6 we obtain 315 319 354 *as an upper degree bound on the necessary shifts in the Sylvester matrix and using the general bound above we get* 314 703 892. *The optimal number is* 26.

This case includes the case where F is **saturated**, i.e. where $\gcd(\mathrm{lt}(F_i), \mathrm{tt}(F_i)) = 1$ for every $i = 1, 2$. In this case, we can simplify the bound the following way (c.f. Corollary 4.5.31). Let $V(F)$ be the output of Algorithm 4.1.5 and $T := (\mathrm{vect}(F_1) + \mathrm{vect}(F_2))^-$. Then

$$\begin{aligned} d =& \mathrm{maxdeg}(T,\ T + \mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \\ &+ \max(\{\mathrm{maxdeg}(((V(F)_i)_2)^-, ((V(F)_i)_2)^+) \mid i \in \mathbb{N}_{\mathrm{len}(V(F))}\}) \end{aligned}$$

solves Problem 4.1.2.

Example 4.1.14. *Consider* $F_1 = X_1X_3^3X_4^2 - 2X_2^6$ *and* $F_2 = 9X_1X_2^4 + 3X_3^4$. *As the term ordering we choose the degree lexicographic ordering with* $X_4 \prec X_3 \prec X_2 \prec X_1$. *We have* $\mathrm{vect}(F_1) = (1,-6,3,2)$ *and* $\mathrm{vect}(F_2) = (1,4,-4,0)$. *Algorithm 4.1.5 returns*

$$V(F) = (((1,0),(1,-6,3,2)),\ ((0,1),(1,4,-4,0)),\ ((-1,1),(0,10,-7,-2))).$$

We compute $T = (0,2,1,0)$ *and obtain*

$$d = \max(3, 3+1) + \max(6,5,10) = 14.$$

Using the bound in Theorem 2.3.6 we obtain 220 580 630 946 *as an upper degree bound on the necessary shifts in the Sylvester matrix and using the general bound above we get* 220 150 628 353. *The optimal number is* 10.

Case 4: F consists of two proper binomials f, f' such that $r\,\mathrm{vect}(f) \neq \mathrm{vect}(f')$ for any $r \in \mathbb{Q} \setminus \{0\}$ and $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f))) > 0$ and $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f'))) > 0$ (c.f. Subsection 4.5.3). Unfortunately we cannot give a better bound for the Sylvester matrix for this case as of yet.

4.2 Degree Bound on the Shifts using the Results from Chapter 3 and Dubé

In Theorem 4.2.2 we use the results of the last chapter to give a bound on the necessary shifts for the case where a bound on the reduced Gröbner basis is already known. For its proof we need the following lemma.

Lemma 4.2.1. *Let $f \in F$ be a proper binomial and $P \in \mathbb{N}^n$ such that $P \geq \mathrm{e}(\mathrm{tt}(f))$. Then $\mathrm{step}(P) \leq \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))$.*

Proof. Assume $\mathrm{step}(P) > \mathrm{step}(\mathrm{e}(\mathrm{tt}(f))$. It follows that $\mathrm{step}(P) > 0$. Let $j \in \mathbb{N}_n$ such that $\mathrm{vect}(f)_j \neq 0$, $\mathrm{overlap}(F)_j > P_j$ and $\mathrm{step}(P) = \left\lceil \frac{\mathrm{overlap}(F)_j - P_j}{\mathrm{vect}(f)_j} \right\rceil$. We obtain

$$\left\lceil \frac{\mathrm{overlap}(F)_j - P_j}{\mathrm{vect}(f)_j} \right\rceil > \left\lceil \frac{\mathrm{overlap}(F)_j - \mathrm{e}(\mathrm{tt}(f))_j}{\mathrm{vect}(f)_j} \right\rceil. \tag{4.1}$$

Now we distinguish two cases: $\mathrm{vect}(f)_j < 0$ and $\mathrm{vect}(f)_j > 0$.
If $\mathrm{vect}(f)_j < 0$, then by (4.1) and the fact that $\mathrm{step}(P) > 0$, we get $P_j > \mathrm{overlap}(F)_j$, which contradicts $\mathrm{overlap}(F)_j > P_j$. If $\mathrm{vect}(f)_j > 0$, then by (4.1) we get $P_j < \mathrm{e}(\mathrm{tt}(f))_j$, which contradicts $P \geq \mathrm{e}(\mathrm{tt}(f))$. □

Theorem 4.2.2. *Let $d' \in \mathbb{N}$ be a degree bound on the reduced Gröbner basis of F and let*

$$\begin{aligned} d'' := \max(\{\, &\mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\deg(\mathrm{vect}(f)) \mid \\ &f \in F, |\,\mathrm{supp}(f)| = 2, \deg(\mathrm{vect}(f)) \geq 0\} \cup \{0\}). \end{aligned}$$

Then

$$d := d' + d'' + |\,\deg(\mathrm{vect}(F_1))| + |\,\deg(\mathrm{vect}(F_2))|$$

gives an upper degree bound on the necessary shifts in the Sylvester matrix.

Proof. Let G be the reduced Gröbner basis of F. For $g \in G \cap F$, we have $g = 1F_1 + 0F_2$ or $g = 0F_1 + 1F_2$.
Now let $g \in G \setminus F$. If g is a term, let $f \in F$ be such that $\mathrm{tt}(f)$ divides g and let

$f' \in F \setminus \{f\}$. By Lemma 4.2.1 we have $\mathrm{step}(\mathrm{e}(\mathrm{tt}(f))) \geq \mathrm{step}(\mathrm{e}(g))$. By Theorems 3.2.1 and 3.2.2 there exist $q, q' \in \mathbb{K}[X] \setminus \{0\}$ such that $g = qf + q'f'$ and

$$\begin{aligned}\mathrm{maxdeg}(qf, q'f') &\leq \mathrm{maxdeg}(\mathrm{e}(g), \mathrm{e}(g) + \mathrm{step}(\mathrm{e}(g))\,\mathrm{vect}(f)) \\ &\leq d' + d'' \\ &\leq d\end{aligned}$$

and

$$\begin{aligned}\mathrm{maxdeg}(qf, q'f') &\leq \mathrm{maxdeg}(\mathrm{e}(g), \mathrm{e}(g) + (\mathrm{step}(\mathrm{e}(g)) + 1)\,\mathrm{vect}(f) + \mathrm{vect}(f')) \\ &\leq d,\end{aligned}$$

respectively.
If g is a proper binomial, let $A = \mathrm{e}(\mathrm{lt}(g))$, $B = \mathrm{e}(\mathrm{tt}(g))$ and $m = |\deg(\mathrm{vect}(F_1))| + |\deg(\mathrm{vect}(F_2))|$. Then by Theorem 3.3.35 there exist $q, q' \in \mathbb{K}[X] \setminus \{0\}$ such that $g = qf + q'f'$ and

$$\begin{aligned}\mathrm{maxdeg}(qf, q'f') &\leq \max(\mathrm{maxdeg}(A, B),\, \mathrm{maxdeg}(\mathrm{overlapshift}(A), \mathrm{overlapshift}(B)) + m) \\ &\leq d' + d'' + m \\ &= d,\end{aligned}$$

where we again used Lemma 4.2.1. □

Corollary 4.2.3. *Let d'' be as in Theorem 4.2.2. Then*

$$d := \left\lfloor 2\left(\frac{\mathrm{maxdeg}(F)^2}{2} + \mathrm{maxdeg}(F)\right)^{2^{n-1}} \right\rfloor + d'' + |\deg(\mathrm{vect}(F_1))| + |\deg(\mathrm{vect}(F_2))|$$

solves Problem 4.1.1.
Proof. The claim follows immediately from Theorems 4.2.2 and 2.3.5. □

Even though the Hermann part of the bound in Theorem 2.3.6 has been significantly improved, the Dubé part still yields a very high bound in Corollary 4.2.3. In the rest of this chapter we improve the whole bound for certain cases of input binomials.

4.3 Degree Bound on the Shifts for a Monomial and a Proper Binomial as Input

Theorem 4.3.2 gives a degree bound on the shifts for the case where F consists of a proper binomial and a monomial. But first we need the following lemma.

Lemma 4.3.1. *Let $f \in F$ be a proper binomial and $k \in \mathbb{N}_{\mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))}$. Then*

$$\mathrm{lcm}(\mathrm{e}(\mathrm{tt}(f)) + k\,\mathrm{vect}(f), \mathrm{overlap}(F)) \leq \mathrm{lcm}(\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f))), \mathrm{overlap}(F)).$$

Proof. Let $i \in \mathbb{N}_n$. We show

$$\begin{aligned} &\max(\,\mathrm{e}(\mathrm{tt}(f))_i + k\,\mathrm{vect}(f)_i, \mathrm{overlap}(F)_i) \\ &\quad \leq \max(\mathrm{e}(\mathrm{tt}(f))_i + \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f)_i, \mathrm{overlap}(F)_i). \end{aligned} \tag{4.2}$$

If $\mathrm{vect}(f)_i \geq 0$, then

$$\mathrm{e}(\mathrm{tt}(f))_i + k\,\mathrm{vect}(f)_i \leq \mathrm{e}(\mathrm{tt}(f))_i + \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f)_i,$$

hence (4.2) holds. Now assume $\mathrm{vect}(f)_i < 0$. Then

$$\mathrm{e}(\mathrm{tt}(f))_i + k\,\mathrm{vect}(f)_i > \mathrm{e}(\mathrm{tt}(f))_i + \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f)_i.$$

But in this case,

$$\begin{aligned} \mathrm{overlap}(F)_i &\geq \min(\mathrm{e}(\mathrm{lt}(f))_i, \mathrm{e}(\mathrm{tt}(f))_i) \\ &= \mathrm{e}(\mathrm{lt}(f))_i \\ &\geq \mathrm{e}(\mathrm{tt}(f))_i + k\,\mathrm{vect}(f)_i, \end{aligned}$$

therefore (4.2) holds. □

Theorem 4.3.2. *Let $f \in F$ be a proper binomial and $f' \in F$ a monomial. Let*

$$P = \mathrm{lcm}(\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f))), \mathrm{overlap}(F)).$$

Then

$$d = \mathrm{maxdeg}(P, P - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f))$$

solves Problem 4.1.2 and is optimal among all the solutions.

Proof. Let G be the reduced Gröbner basis of F. For $g \in G \cap F$, we either have $g = 0f + 1f'$ and $\deg(f') \leq d$ or $g = 1f + 0f'$. The latter can only happen if $P \neq \mathrm{e}(\mathrm{tt}(g))$ because otherwise $\mathrm{e}(\mathrm{tt}(g)) \geq \mathrm{overlap}(F)$ and hence f' would divide $\mathrm{tt}(g)$. Therefore, $\deg(f) \leq d$.
Now let $g \in G \setminus F$. Then g is a term that is divided by $\mathrm{tt}(f)$ and not by f' and hence does not lie in $\mathrm{Aoverlap}(F)$. By Lemma 4.2.1, $\mathrm{step}(\mathrm{e}(g)) \in \mathbb{N}_{\mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))}$. Let

$$Q := \mathrm{lcm}(\mathrm{e}(\mathrm{tt}(f)) + \mathrm{step}(\mathrm{e}(g))\,\mathrm{vect}(f), \mathrm{overlap}(F)).$$

We first show that

$$Q - \mathrm{step}(\mathrm{e}(g))\,\mathrm{vect}(f) = \mathrm{e}(g).$$

Note that by construction,

$$Q - \mathrm{step}(\mathrm{e}(g))\,\mathrm{vect}(f) \leq Q'$$

for all $Q' \in \mathbb{N}^n$ such that $\mathrm{step}(Q') = \mathrm{step}(Q) = \mathrm{step}(\mathrm{e}(g))$ and $\mathrm{e}^{-1}(Q') \in \mathrm{ideal}(F)$, hence also

$$Q - \mathrm{step}(\mathrm{e}(g))\,\mathrm{vect}(f) \leq \mathrm{e}(g).$$

Since g is irreducible with respect to $G \setminus \{g\}$, equality follows.
From Theorem 3.2.1 we get (note that there, $k = \mathrm{step}(\mathrm{e}(g)) = \mathrm{step}(Q)$)

$$\deg(q'f') \leq \deg(qf) = \mathrm{maxdeg}(Q, Q - \mathrm{step}(Q)\,\mathrm{vect}(f)) \tag{4.3}$$

for some $q, q' \in \mathbb{K}[X] \setminus \{0\}$ such that $g = qf + q'f'$. From Lemma 4.3.1 we know $Q \leq P$, hence $\deg(Q) \leq \deg(P)$. So if $\deg(\mathrm{vect}(f)) \geq 0$, then

$$d = \deg(P) \geq \deg(Q) = \mathrm{maxdeg}(Q, Q - \mathrm{step}(Q)\,\mathrm{vect}(f)).$$

If $\deg(\mathrm{vect}(f)) < 0$, then

$$\begin{aligned} d &= \deg(P - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f)) \\ &= \deg(P) - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\deg(\mathrm{vect}(f)) \\ &\geq \deg(Q) - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\deg(\mathrm{vect}(f)) \\ &\geq \deg(Q) - \mathrm{step}(Q)\deg(\mathrm{vect}(f)) \\ &= \deg(Q - \mathrm{step}(Q)\,\mathrm{vect}(f)) \\ &= \mathrm{maxdeg}(Q, Q - \mathrm{step}(Q)\,\mathrm{vect}(f)). \end{aligned}$$

Note that there is a $g' \in G \cap F$ such that $\mathrm{step}(\mathrm{e}(g)) = \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))$, so because of (4.3), d is optimal. □

4.4 Degree Bound on the Shifts for Proper Binomials with Linearly Dependent Vectors as Input

Theorem 4.4.1 gives a bound on the shifts for the case where F consists of two proper binomials f and f' whose exponent vectors $\mathrm{vect}(f)$ and $\mathrm{vect}(f')$ are linearly dependent.

Theorem 4.4.1. *Let F consist of two proper binomials f, f' such that $r\,\mathrm{vect}(f) = \mathrm{vect}(f')$ for some $r \in \mathbb{Q} \setminus \{0\}$ and let*

$$P := \mathrm{lcm}(\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f))) + V, \mathrm{overlap}(F))$$

and

$$P' := \mathrm{lcm}(\mathrm{overlapshift}(\mathrm{e}(\mathrm{tt}(f'))) + V, \mathrm{overlap}(F)),$$

where $V := \mathrm{vect}(f) + \mathrm{vect}(f')$. Then

$$d = \mathrm{maxdeg}(P, P - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f) - V, P', P' - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f')))\,\mathrm{vect}(f') - V)$$

solves Problem 4.1.2.

Proof. Let G be the reduced Gröbner basis of F. For $g \in G \cap F$, we have either $g = 0f + 1f'$ or $g = 1f + 0f'$. It can be easily checked that $\deg(f), \deg(f') \leq d$.
Now let $g \in G \setminus F$. First note that either $\mathrm{tt}(f)$ divides both $\mathrm{lt}(g)$ and $\mathrm{tt}(g)$ or $\mathrm{tt}(f')$ divides both $\mathrm{lt}(g)$ and $\mathrm{tt}(g)$. Assume the first case. Let $q, q' \in \mathbb{K}[X]$ such that $g = qf + q'f'$. Then for all $\xi \in \mathrm{supp}(qf) \cup \mathrm{supp}(q'f')$ we get $\xi = \mathrm{tt}(g)\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^l$ for some nonnegative $l \in \mathbb{Q}$. Let

$$l' := \max(\{l \in \mathbb{Q} \mid l \geq 0,\ \mathrm{tt}(g)\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^l \in \mathrm{supp}(qf) \cup \mathrm{supp}(q'f')\}).$$

It follows that $\mathrm{lt}(qf) = \mathrm{lt}(q'f') = \mathrm{tt}(g)\left(\frac{\mathrm{lt}(f)}{\mathrm{tt}(f)}\right)^{l'}$. With the same argument as in the proof of Theorem 3.2.2 we can assume that q and q' were chosen in such a way that

$$l' \leq \mathrm{step}(\mathrm{e}(\mathrm{tt}(g))) + 1 + r.$$

Let

$$Q := \mathrm{lcm}(\mathrm{e}(\mathrm{tt}(f)) + \mathrm{step}(\mathrm{e}(\mathrm{tt}(g)))\,\mathrm{vect}(f) + V, \mathrm{overlap}(F)).$$

Since g is irreducible with respect to $G \setminus \{g\}$, we have

$$\begin{aligned}\mathrm{e}(\mathrm{tt}(g)) + (\mathrm{step}(\mathrm{e}(\mathrm{tt}(g))) + 1 + r - l')(\mathrm{vect}(f))^- = \\ = Q - \mathrm{step}(\mathrm{e}(\mathrm{tt}(g)))\,\mathrm{vect}(f) - V \qquad (4.4)\end{aligned}$$

and

$$\mathrm{e}(\mathrm{lt}(qf)) + (\mathrm{step}(\mathrm{e}(\mathrm{tt}(g))) + 1 + r - l')(\mathrm{vect}(f))^+ = Q. \qquad (4.5)$$

By Lemma 4.3.1, $Q \leq P$ (it is easily checked that because of the addition of V, here this also holds if $\mathrm{step}(\mathrm{e}(\mathrm{tt}(g))) = 0$), hence we obtain from (4.4)

$$\begin{aligned}\mathrm{e}(\mathrm{tt}(g)) &\leq Q - \mathrm{step}(\mathrm{e}(\mathrm{tt}(g)))\,\mathrm{vect}(f) - V \\ &\leq P - \mathrm{step}(\mathrm{e}(\mathrm{tt}(g)))\,\mathrm{vect}(f) - V\end{aligned}$$

and from (4.5)

$$\begin{aligned} \mathrm{e}(\mathrm{lt}(qf)) &\leq Q \\ &\leq P. \end{aligned}$$

Now if $\deg(\mathrm{vect}(f)) \leq 0$, then using Lemma 4.2.1,

$$\begin{aligned} \deg(q'f') &\leq \deg(qf) \\ &= \deg(\mathrm{tt}(g)) \\ &\leq \deg(P - \mathrm{step}(\mathrm{e}(\mathrm{tt}(g)))\,\mathrm{vect}(f) - V) \\ &\leq \deg(P - \mathrm{step}(\mathrm{e}(\mathrm{tt}(f)))\,\mathrm{vect}(f) - V) \\ &\leq d. \end{aligned}$$

If $\deg(\mathrm{vect}(f)) > 0$, then

$$\begin{aligned} \deg(q'f') &= \deg(qf) \\ &= \deg(\mathrm{lt}(qf)) \\ &\leq \deg(Q) \\ &\leq \deg(P) \\ &\leq d. \end{aligned}$$

In the case where $\mathrm{tt}(f')$ divides both $\mathrm{lt}(g)$ and $\mathrm{tt}(g)$, we proceed analogously. □

4.5 Degree Bound on the Shifts for Proper Binomials with Linearly Independent Vectors as Input

Like in Section 3.3, let from now on, until stated otherwise, F consist only of proper binomials. We additionally assume that their exponent vectors are linearly independent. Then every element g of the reduced Gröbner basis is a proper binomial, whose terms are not divided by any element in $\mathrm{lt}(F)$ unless $g \in F$, and $\mathrm{supp}(g) \not\subseteq \mathrm{ideal}(F)$. Furthermore, any element in $\mathrm{supp}(g)$ is either a multiple of $\mathrm{tt}(F_1)$ or a multiple of $\mathrm{tt}(F_2)$. In Subsection 4.5.1 we investigate the case where every element in $\mathrm{supp}(g)$ is a multiple of the trailing term of the same input binomial. In Subsection 4.5.2 we use these results to give an upper degree bound on the shifts needed for computing a Gröbner basis in the case where the trailing term of one of the input binomials has step 0. This includes the case where F is saturated, i.e. where $\gcd(\mathrm{lt}(F_i), \mathrm{tt}(F_i)) = 1$ for every $i = 1, 2$.

4.5.1 Gröbner Bases Elements Whose Leading and Trailing Terms are Multiples of the Trailing Term of the Same Input Binomial

If in a Gröbner basis we exchange an element by another element in the ideal that has the same leading term, then by Lemma 2.1.7, the resulting set of polynomials is again a Gröbner basis. In this subsection we will determine for every proper binomial g in the reduced Gröbner basis of F, for which $\operatorname{supp}(g) \subseteq [X]\operatorname{tt}(f)$ for an $f \in F$, a proper binomial $g' \in \operatorname{ideal}(F)$ of a certain structure (contained in the output of Algorithm 4.1.5) such that $\operatorname{lt}(g') = \operatorname{lt}(g)$ (c.f. Theorems 4.5.2, 4.5.3, 4.5.4, 4.5.5 and, summarizing, Theorem 4.5.18). Then there exists a Gröbner basis G' of F such that every $g' \in G'$ with $\operatorname{supp}(g') \subseteq [X]\operatorname{supp}(f)$ has this special structure and we give an upper degree bound on the shifts needed for generating these g' (c.f. Theorem 4.5.27).

Definition 4.5.1. *For a shift $f \in \mathbb{N}^n + \operatorname{shifts}(F)$ we say that f lies in* $\operatorname{Aoverlap}(F)$ *iff $f_1, f_2 \in \operatorname{Aoverlap}(F)$. We say that f lies outside of* $\operatorname{Aoverlap}(F)$ *iff $f_1 \notin \operatorname{Aoverlap}(F)$ or $f_2 \notin \operatorname{Aoverlap}(F)$.*

The following theorem treats the elements g in the reduced Gröbner basis which fulfill $\operatorname{vect}(g) = k\operatorname{vect}(f)$ for some $k \in \mathbb{N} \setminus \{0\}$ and $f \in F$.

Theorem 4.5.2. *Let $h \in \operatorname{ideal}(F) \setminus \{0\}$ such that $\operatorname{vect}(h) = k\operatorname{vect}(f)$ for some $k \in \mathbb{N} \setminus \{0\}$ and $f \in F$ and such that no element in $\operatorname{lt}(F)$ divides any element in $\operatorname{supp}(h)$. Then there exists an $h' \in \operatorname{ideal}(F) \setminus \{0\}$ such that $\operatorname{lt}(h') = \operatorname{lt}(h)$ and $\operatorname{vect}(h') = \operatorname{vect}(f)$.*

Proof. Let f and k be as in the theorem, $f' \in F \setminus \{f\}$ and let z be a vpc of minimal length from $\operatorname{e}(\operatorname{lt}(h))$ to $\operatorname{e}(\operatorname{tt}(h))$. We distinguish two cases: $\operatorname{e}(\operatorname{lt}(h)) \geq \operatorname{overlap}(F)$ and $\operatorname{e}(\operatorname{lt}(h)) \ngeq \operatorname{overlap}(F)$.
Assume $\operatorname{e}(\operatorname{lt}(h)) \geq \operatorname{overlap}(F)$. If z_1 is a positive shift of f, then there cannot be any negative shifts of f inside of $\operatorname{Aoverlap}(F)$. Let $m > 0$ be the number of positive shifts of f in z. Then there have to be $m + k$ negative shifts of f in z outside of $\operatorname{Aoverlap}(F)$. Any shifts of f' have to be inside of $\operatorname{Aoverlap}(F)$ and since the number of positive shifts of f' and of negative shifts of f', respectively, have to be the same and not both kind of shifts can be inside of $\operatorname{Aoverlap}(F)$, this number is zero. But then, z consist of $m > 0$ positive shifts of f and $m + k > 0$ negative shifts of f. This contradicts the assumption that z has minimal length.
If z_1 is not a positive shift of f, then, since $\operatorname{lt}(f')$ does not divide $\operatorname{lt}(h)$, it has to be a positive shift of f'. Let $m > 0$ be the number of positive shifts of f' in z. The number of positive shifts of f' equals the number of negative shifts of f' in z, so the last m elements in z must be negative shifts of f', because there can be no positive shifts of f' inside of $\operatorname{Aoverlap}(F)$. The chain z contains exactly k negative shifts of f, all inside

of Aoverlap(F), and no positive shifts of f. Let $i \in \mathbb{N}_{m+1}$ be minimal such that z_i is a negative shift of f. We show that z', defined as

$$z'_j := \begin{cases} z_j & \text{if } 1 \leq j \leq i \\ (k-1)\operatorname{vect}(f) + z_{\operatorname{len}(z)-2i+1+j} & \text{if } i+1 \leq j \leq 2i-1 \end{cases}$$

for $j \in \mathbb{N}_{2i-1}$, is a vpc from $\operatorname{e}(\operatorname{lt}(h))$ to $\operatorname{e}(\operatorname{lt}(h)) - \operatorname{vect}(f)$. We have

$$z'_{1,1} = z_{1,1} = \operatorname{e}(\operatorname{lt}(h)),$$

$$\begin{aligned} z'_{\operatorname{len}(z'),2} &= (k-1)\operatorname{vect}(f) + z_{\operatorname{len}(z),2} \\ &= (k-1)\operatorname{vect}(f) + \operatorname{e}(\operatorname{tt}(h)) \\ &= (k-1)\operatorname{vect}(f) + (\operatorname{e}(\operatorname{lt}(h)) - k\operatorname{vect}(f)) \\ &= \operatorname{e}(\operatorname{lt}(h)) - \operatorname{vect}(f) \end{aligned}$$

and

$$\begin{aligned} z'_{i,2} &= z_{i,2} \\ &= \operatorname{e}(\operatorname{lt}(h)) + (i-1)\operatorname{vect}(f') - \operatorname{vect}(f) \\ &= (\operatorname{e}(\operatorname{tt}(h)) + k\operatorname{vect}(f)) + (i-1)\operatorname{vect}(f') - \operatorname{vect}(f) \\ &= (k-1)\operatorname{vect}(f) + (\operatorname{e}(\operatorname{tt}(h)) + (i-1)\operatorname{vect}(f')) \\ &= (k-1)\operatorname{vect}(f) + z_{\operatorname{len}(z)-i+2,\,1} \\ &= z'_{i+1,1}, \end{aligned}$$

so it remains to show that for all j with $i+1 \leq j \leq 2i-1$

$$(k-1)\operatorname{vect}(f) + z_{\operatorname{len}(z)-2i+1+j} \in \mathbb{N}^n + \operatorname{shifts}(F).$$

Suppose there is a j', $i+1 \leq j' \leq 2i-1$, such that

$$(k-1)\operatorname{vect}(f) + z_{\operatorname{len}(z)-2i+1+j'} \notin \mathbb{N}^n + \operatorname{shifts}(F).$$

Let $\tau \in \mathbb{N}^n$ such that

$$z_{\operatorname{len}(z)-2i+1+j'} = \tau + \operatorname{negshift}(f').$$

It follows that

$$\tau + (k-1)\operatorname{vect}(f) \notin \mathbb{N}^n.$$

So let $l \in \mathbb{N}_n$ be such that

$$\tau_l + (k-1)\operatorname{vect}(f)_l < 0.$$

Since $\tau_l \geq 0$, we obtain $\operatorname{vect}(f)_l < 0$ and hence $\tau_l + k \operatorname{vect}(f)_l < 0$. Therefore,

$$z_{\operatorname{len}(z)-j'+1} = (\tau + k \operatorname{vect}(f)) + \operatorname{posshift}(f') \notin \mathbb{N}^n + \operatorname{shifts}(F),$$

which contradicts the fact that z is a vpc. Hence, z' is a vpc from $\operatorname{e}(\operatorname{lt}(h))$ to $\operatorname{e}(\operatorname{lt}(h)) - \operatorname{vect}(f)$. By Theorem 3.3.17 there exists an $h' \in \operatorname{ideal}(F) \setminus \{0\}$ with $\operatorname{lt}(h') = \operatorname{lt}(h)$ and $\operatorname{tt}(h') = \frac{\operatorname{lt}(h)\operatorname{tt}(f)}{\operatorname{lt}(f)}$, hence $\operatorname{vect}(h') = \operatorname{vect}(f)$.

Now assume $\operatorname{e}(\operatorname{lt}(h)) \not\geq \operatorname{overlap}(F)$. Suppose z_1 is a positive shift of f, and let m and m' be the number of positive shifts of f and f' in z, respectively. Then, the number of negative shifts of f and f' is $m + k$ and m', respectively, and since in a vpc of minimal length there cannot be a negative shift of f right after a positive shift of f, we know $m' > 0$. The positive shifts of f' have to lie inside of $\operatorname{Aoverlap}(F)$ and the last m' shifts of z are the negative shifts of f', lying all outside of $\operatorname{Aoverlap}(F)$. If it was the other way around, this would violate our assumption that $\operatorname{lt}(f')$ does not divide $\operatorname{tt}(h)$. Furthermore, the first m elements in z are positive shifts of f. This means that all $m + k$ negative shifts of f in z lie in $\operatorname{Aoverlap}(F)$. Let $i \in \mathbb{N}_{m+m'+1}$ be minimal such that z_i is a negative shift of f. In order to prove that this case cannot occur, we show that z', defined as

$$z'_j := \begin{cases} -\operatorname{vect}(f) + z_{j+1} & \text{if } 1 \leq j \leq i-2 \\ z_{j+2} & \text{if } i-1 \leq j \leq \operatorname{len}(z)-2, \end{cases}$$

is a vpc from $\operatorname{e}(\operatorname{lt}(h))$ to $\operatorname{e}(\operatorname{tt}(h))$ with smaller length than z. We have

$$\begin{aligned} z'_{1,1} &= -\operatorname{vect}(f) + z_{2,1} \\ &= z_{1,1} \\ &= \operatorname{e}(\operatorname{lt}(h)), \end{aligned}$$

$$z'_{\operatorname{len}(z'),\,2} = z_{\operatorname{len}(z),\,2} = \operatorname{e}(\operatorname{tt}(h))$$

and

$$\begin{aligned} z'_{i-2,2} &= -\operatorname{vect}(f) + z_{i-1,2} \\ &= z_{i,2} \\ &= z_{i+1,1} \\ &= z'_{i-1,1}, \end{aligned}$$

so it remains to show that for all $j \in \mathbb{N}_{i-2}$

$$-\operatorname{vect}(f) + z_{j+1} \in \mathbb{N}^n + \operatorname{shifts}(F).$$

For $j \in \mathbb{N}_{m-1}$ this follows from the fact that in this case $-\operatorname{vect}(f) + z_{j+1} = z_j$. For the rest, suppose there is a j', $m \leq j' \leq i-2$ such that

$$-\operatorname{vect}(f) + z_{j'+1} \notin \mathbb{N}^n + \operatorname{shifts}(F).$$

Let $\tau \in \mathbb{N}^n$ such that

$$z_{j'+1} = \tau + \operatorname{posshift}(f').$$

It follows that

$$\tau - \operatorname{vect}(f) \notin \mathbb{N}^n.$$

So let $l \in \mathbb{N}_n$ be such that

$$\tau_l - \operatorname{vect}(f)_l < 0.$$

We obtain $0 \leq \tau_l < \operatorname{vect}(f)_l$, hence $\tau_l - k \operatorname{vect}(f)_l < 0$. Therefore,

$$z_{\operatorname{len}(z)+m-j'} = (\tau - k \operatorname{vect}(f)) + \operatorname{negshift}(f') \notin \mathbb{N}^n + \operatorname{shifts}(F),$$

which contradicts the fact that z is a vpc.
If z_1 is not a positive shift of f, then it has to be a positive shift of f'. If $z_{\operatorname{len}(z)}$ is a shift of f, then it has to be positive one, since otherwise $\operatorname{lt}(f)$ would divide $\operatorname{tt}(h)$. So if $z_{\operatorname{len}(z)}$ is a shift of f, let $m \in \mathbb{N}_{k-1}$ be maximal such that the last m elements in z are negative shifts of f, and if $z_{\operatorname{len}(z)}$ is a shift of f', let $m := 0$. Let m' be the number of positive shifts of f' in z. We can derive that $m < k$, because otherwise the last k entries of z would form a vpc from $\operatorname{e}(\operatorname{lt}(h))$ to $\operatorname{e}(\operatorname{tt}(h))$, which would mean that, since z has minimal length, z would only consist of k negative shifts of f, which in turn would violate the assumption that z_1 is a positive shift of f'. Let z' be defined as $z'_j := z_j$ for $j \in \mathbb{N}_{\operatorname{len}(z)-m}$. It is a vpc of minimal length from $\operatorname{e}(\operatorname{lt}(h))$ to $\operatorname{e}(\operatorname{lt}(h)) - (k-m)\operatorname{vect}(f)$ and its last element is a shift of f'. Therefore, the first m' shifts of z' are the positive shifts of f' and the rest of the shifts lie in $\operatorname{Aoverlap}(F)$, namely m' negative shifts of f' and $(m-k)$ negative shifts of f. Let $i \in \mathbb{N}_{\operatorname{len}(z')}$ be minimal such that z'_i is a negative shift of f. Analogously to the case $\operatorname{e}(\operatorname{lt}(h)) \geq \operatorname{overlap}(F)$ and z_1 is not a positive shift of f, we can prove that z'', defined as

$$z''_j := \begin{cases} z'_j & \text{if } 1 \leq j \leq i \\ (m-k-1)\operatorname{vect}(f) + z'_{\operatorname{len}(z')-2i+1+j} & \text{if } i+1 \leq j \leq 2i-1 \end{cases}$$

for $j \in \mathbb{N}_{2i-1}$, is a vpc from $\operatorname{e}(\operatorname{lt}(h))$ to $\operatorname{e}(\operatorname{lt}(h)) - \operatorname{vect}(f)$. So there exists an $h' \in \operatorname{ideal}(F) \setminus \{0\}$ such that $\operatorname{lt}(h') = \operatorname{lt}(h)$ and $\operatorname{tt}(h') = \frac{\operatorname{lt}(h)\operatorname{tt}(f)}{\operatorname{lt}(f)}$, hence $\operatorname{vect}(h') = \operatorname{vect}(f)$. □

The following theorem treats the elements g in the reduced Gröbner basis which fulfill $\operatorname{vect}(g) = k \operatorname{vect}(F_1) + k' \operatorname{vect}(F_2)$ for some $k, k' \in \mathbb{N} \setminus \{0\}$.

Theorem 4.5.3. *Let* $h \in \text{ideal}(F) \setminus \{0\}$ *such that* $\text{vect}(h) = k\,\text{vect}(F_1) + k'\,\text{vect}(F_2)$ *for some* $k, k' \in \mathbb{N} \setminus \{0\}$ *and such that no element in* $\text{lt}(F)$ *divides any element in* $\text{supp}(h)$. *Then there exists an* $h' \in \text{ideal}(F) \setminus \{0\}$ *such that* $\text{lt}(h') = \text{lt}(h)$ *and* $\text{vect}(h') = \text{vect}(F_1)$ *or* $\text{vect}(h') = \text{vect}(F_2)$.

Proof. Let k and k' be as in the theorem and z be a vpc of minimal length from $\text{e}(\text{lt}(h))$ to $\text{e}(\text{tt}(h))$. We distinguish two cases: $\text{e}(\text{lt}(h)) \geq \text{overlap}(F)$ and $\text{e}(\text{lt}(h)) \ngeq \text{overlap}(F)$. Assume $\text{e}(\text{lt}(h)) \geq \text{overlap}(F)$. If z_1 is a positive shift of F_1, then there cannot be any negative shifts of F_1 inside of $\text{Aoverlap}(F)$. Let $m > 0$ be the number of positive shifts of F_1 in z. Then the last $m + k > k$ elements in z have to be negative shifts of F_1, all outside of $\text{Aoverlap}(F)$. Consequently, z' defined as $z'_j := z_j$ for $j \in \mathbb{N}_{\text{len}(z)-k}$ is a vpc from $\text{e}(\text{lt}(h))$ to $\text{e}(\text{lt}(h)) - k'\,\text{vect}(F_2)$. By Theorems 3.3.17 and 4.5.2, there exists an $h' \in \text{ideal}(F) \setminus \{0\}$ such that $\text{lt}(h') = \text{lt}(h)$ and $\text{vect}(h') = \text{vect}(F_2)$.
If z_1 is not a positive shift of F_1, then, since $\text{lt}(F_2)$ does not divide $\text{lt}(h)$, it has to be a positive shift of F_2. This case works analogously to the first one.
Now assume $\text{e}(\text{lt}(h)) \ngeq \text{overlap}(F)$. Suppose z_1 is a positive shift of F_1, and let m and m' be the number of positive shifts of F_1 and F_2 in z, respectively. Then the number of negative shifts of F_1 and F_2 is $m + k$ and $m' + k'$, respectively. If $m' > 0$, then all the positive shifts of F_2 have to lie in $\text{Aoverlap}(F)$ and the last $m' + k' > k'$ elements in z have to be negative shifts of F_2, all outside of $\text{Aoverlap}(F)$. Consequently, z' defined as $z'_j := z_j$ for $j \in \mathbb{N}_{\text{len}(z)-k'}$ is a vpc from $\text{e}(\text{lt}(h))$ to $\text{e}(\text{lt}(h)) - k\,\text{vect}(F_1)$. By Theorems 3.3.17 and 4.5.2, there exists an $h' \in \text{ideal}(F) \setminus \{0\}$ such that $\text{lt}(h') = \text{lt}(h)$ and $\text{vect}(h') = \text{vect}(F_1)$. If $m' = 0$ then we again distinguish two cases: there is a positive shift of F_1 inside of $\text{Aoverlap}(F)$ and there is no positive shift of F_1 inside of $\text{Aoverlap}(F)$. First suppose, there is a positive shift of F_1 inside of $\text{Aoverlap}(F)$. Then there cannot be any negative shifts of F_1 inside of $\text{Aoverlap}(F)$, which means that the last $m+k > k$ elements in z are negative shifts of F_1. Consequently, z' defined as $z'_j := z_j$ for $j \in \mathbb{N}_{\text{len}(z)-k}$ is a vpc from $\text{e}(\text{lt}(h))$ to $\text{e}(\text{lt}(h)) - k'\,\text{vect}(F_2)$. By Theorems 3.3.17 and 4.5.2, there exists an $h' \in \text{ideal}(F) \setminus \{0\}$ such that $\text{lt}(h') = \text{lt}(h)$ and $\text{vect}(h') = \text{vect}(F_2)$.
Now suppose, there is no positive shift of F_1 inside of $\text{Aoverlap}(F)$. Then the only shifts in $\text{Aoverlap}(F)$ are negative shifts of F_1 and F_2 and the first m shifts in z are all the positive shifts of F_1. Let $i \in \mathbb{N}_{\text{len}(z)}$ be such that z_i is the m-th negative shift of F_1 in z. Then z' defined as $z'_j := z_j$ for $j \in \mathbb{N}_i$ is a vpc from $\text{e}(\text{lt}(h))$ to $\text{e}(\text{lt}(h)) - l\,\text{vect}(F_2)$ for some $l \in \mathbb{N}_{k'}$. By Theorems 3.3.17 and 4.5.2, there exists an $h' \in \text{ideal}(F) \setminus \{0\}$ such that $\text{lt}(h') = \text{lt}(h)$ and $\text{vect}(h') = \text{vect}(F_2)$.
If z_1 is not a positive shift of F_1, then, since $\text{lt}(F_2)$ does not divide $\text{lt}(h)$, it has to be a positive shift of F_2. This case works analogously to the case where z_1 is a positive shift of F_1. □

Theorems 4.5.4 and 4.5.5 treat the elements g in the reduced Gröbner basis which fulfill $\text{vect}(g) = k\,\text{vect}(f) - k'\,\text{vect}(f')$ for some $k, k' \in \mathbb{N} \setminus \{0\}$ and $f, f' \in F$, $f \neq f'$.

Theorem 4.5.4. *Let $\xi \in \mathrm{e}(\mathrm{tt}(F))$ and $A, B \in \mathbb{N}^n$, $A, B \geq \xi$ and $A, B \not\geq \mathrm{e}(\mathrm{lt}(h))$ for any $h \in F$, such that there is a vpc from A to B. Let $f, f' \in F$, $f \neq f'$, and $k, k' \in \mathbb{N} \setminus \{0\}$ such that $A + k\,\mathrm{vect}(f) - k'\,\mathrm{vect}(f') = B$. Furthermore, let $l \in \mathbb{N}_k$, $l' \in \mathbb{N}_{k'}$ such that $\frac{l'}{l} \geq \frac{k'}{k}$ and*

$$\begin{cases} \frac{l'}{l+1} \leq \frac{k'}{k} & \text{if } \xi = \mathrm{e}(\mathrm{tt}(f)) \\ \frac{l'-1}{l} \leq \frac{k'}{k} & \text{if } \xi = \mathrm{e}(\mathrm{tt}(f')). \end{cases}$$

Then there exists a vpc from $B - (l\,\mathrm{vect}(f) - l'\,\mathrm{vect}(f'))$ to B.

Proof. Let z be a vpc of minimal length from A to B and $v := l\,\mathrm{vect}(f) - l'\,\mathrm{vect}(f')$. The first element in z can be a positive shift of f or f', the last only a negative shift of f or f'. Assume, z does not already go through $B - v$.
We first assume that $\xi = \mathrm{tt}(f)$. Then every shift of f' lies in $\mathrm{Aoverlap}(F)$, hence there are no positive shifts of f' in z and z_1 is a positive shift of f. If there are positive shifts of f in $\mathrm{Aoverlap}(F)$, then all the negative shifts of f (if any) have to occur as the last elements of z, outside of $\mathrm{Aoverlap}(F)$. If there are negative shifts of f in $\mathrm{Aoverlap}(F)$, then all the positive shifts of f have to occur as the first elements of z and their number exceeds the number of negative shifts of f by at least k at any index greater than k. Note that $B - (l\,\mathrm{vect}(f) - l'\,\mathrm{vect}(f')) = A + (k-l)\,\mathrm{vect}(f) - (k'-l')\,\mathrm{vect}(f')$. Let $i \in \mathbb{N}_{\mathrm{len}(z)}$ be such that z_i is the $(k'-l'+1)$-th negative shift of f' in z. Let $m \in \mathbb{Z} \setminus \{0\}$ be such that $z_{i,1} - m\,\mathrm{vect}(f) = B - v$. First assume $m > 0$. We show $z_{i,1} - \mathrm{vect}(f) \geq \xi$. Let $i' \in \mathbb{N}_{i-1}$ be maximal such that $z_{i'}$ is a shift of f. Then there are $i - i' - 1$ negative shifts of f' between $z_{i'}$ and z_i (excluding z_i) and there are $(k'-l') - (i-i'-1)$ negative shifts of f' before $z_{i'}$. First assume that $z_{i'}$ is a positive shift of f. If $i = i' + 1$, then $z_{i,1} - \mathrm{vect}(f) = z_{i',1} \geq \xi$. So let now $i - i' - 1 > 0$.
If $m < l + 1$, then for

$$\begin{aligned} P &:= z_{i',1} - \left(((k-l)+m-1)\frac{k'}{k} - ((k'-l') - (i-i'-1))\right)\mathrm{vect}(f') \\ &= A + ((k-l)+m-1)\,\mathrm{vect}(f) - ((k-l)+m-1)\frac{k'}{k}\,\mathrm{vect}(f') \\ &= \left(1 - \frac{(k-l)+m-1}{k}\right)A + \frac{(k-l)+m-1}{k}B \end{aligned}$$

we have $P \in \mathrm{conn}(A, B)$ and

$$z_{i,1} - \mathrm{vect}(f) = (1-\lambda)z_{i',1} + \lambda P \in \mathrm{conn}(z_{i',1}, P),$$

where $\lambda = \frac{i-i'-1}{((k-l)+m-1)\frac{k'}{k} - ((k'-l')-(i-i'-1))} \in (0, 1]$, since, because of $\frac{l'}{l} \geq \frac{k'}{k}$, also $\frac{l'}{l-m+1} \geq \frac{k'}{k}$, hence $\frac{k'-l'}{(k-l)+m-1} \leq \frac{k'}{k}$ and therefore

$$i - i' \leq ((k-l)+m-1)\frac{k'}{k} - ((k'-l') - (i-i')).$$

From this and $i - i' - 1 > 0$ it also follows that

$$((k-l)+m-1)\frac{k'}{k} - ((k'-l') - (i-i'-1)) > 0.$$

Since $z_{i',1} \geq \xi$ and $P \geq \xi$, we get $z_{i,1} - \mathrm{vect}(f) \geq \xi$.
If $m \geq l+1$, then there is an i'' with $i+1 \leq i'' \leq \mathrm{len}(z)$ such that $z_{i''}$ is a negative shift of f and

$$z_{i',1} - m' \,\mathrm{vect}(f') = z_{i'',2}$$

for some $m' \in \mathbb{N}_{l'+(i-i'-1)}$. We then have $z_{i,1} - \mathrm{vect}(f) \in \mathrm{conn}(z_{i',1}, z_{i'',2})$ and since $z_{i',1} \geq \xi$ and $z_{i'',2} \geq \xi$, also $z_{i,1} - \mathrm{vect}(f) \geq \xi$.
Now assume that $z_{i'}$ is a negative shift of f. We first show that $z_{i,1} \geq \xi$. If $i = i'+1$, then $z_{i,1} = z_{i',2} \geq \xi$. So let now $i - i' - 1 > 0$.
If $m < l$, then for

$$\begin{aligned} P &:= z_{i',2} - \left(((k-l)+m)\frac{k'}{k} - ((k'-l') - (i-i'-1))\right)\mathrm{vect}(f') \\ &= A + ((k-l)+m)\,\mathrm{vect}(f) - ((k-l)+m)\frac{k'}{k}\,\mathrm{vect}(f') \\ &= (1 - \frac{(k-l)+m}{k})A + \frac{(k-l)+m}{k}B, \end{aligned}$$

we have $P \in \mathrm{conn}(A, B)$ and

$$z_{i,1} = (1-\lambda)z_{i',2} + \lambda P \in \mathrm{conn}(z_{i',2}, P),$$

where $\lambda = \frac{i-i'-1}{((k-l)+m)\frac{k'}{k} - ((k'-l') - (i-i'-1))} \in (0,1]$, since, because of $\frac{l'}{l} \geq \frac{k'}{k}$, also $\frac{l'}{l-m} \geq \frac{k'}{k}$, hence $\frac{k'-l'}{m+(k-l)} \leq \frac{k'}{k}$ and therefore

$$i - i' - 1 \leq ((k-l)+m)\frac{k'}{k} - ((k'-l') - (i-i'-1)).$$

From this and $i - i' - 1 > 0$, it also follows that

$$((k-l)+m)\frac{k'}{k} - ((k'-l') - (i-i'-1)) > 0.$$

Since $z_{i',2} \geq \xi$ and $P \geq \xi$, we get $z_{i,1} \geq \xi$. For

$$P' := (1 - \frac{k'-l'}{k'})A + \frac{k'-l'}{k'}B$$

we have $z_{i,1} - \mathrm{vect}(f) \in \mathrm{conn}(z_{i,1}, P')$ and since $z_{i,1} \geq \xi$ and $P' \geq \xi$, also $z_{i,1} - \mathrm{vect}(f) \geq \xi$.
If $m \geq l$, then there is an i'' with $i+1 \leq i'' \leq \mathrm{len}(z)$ such that $z_{i''}$ is a negative shift of f and

$$z_{i',2} - m' \,\mathrm{vect}(f') = z_{i'',2}$$

for some $m' \in \mathbb{N}_{l'+(i-i'-1)}$. We then have $z_{i,1} \in \mathrm{conn}(z_{i',2}, z_{i'',2})$ and since $z_{i',2} \geq \xi$ and $z_{i'',2} \geq \xi$, also $z_{i,1} \geq \xi$ and, like before, $z_{i,1} - \mathrm{vect}(f) \geq \xi$.
With the P' above we have $z_{i,1} - j\,\mathrm{vect}(f) \in \mathrm{conn}(z_{i,1} - \mathrm{vect}(f), P')$ and hence $z_{i,1} - j\,\mathrm{vect}(f) \geq \xi$ for all $j \in \mathbb{N}_m$. This shows that z' defined as

$$z'_j := \begin{cases} ((B-v) - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f) & \text{if } j = 1 \\ (z'_{j-1,2} - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f) & \text{if } 2 \leq j \leq m \\ z_{i-m-1+j} & \text{if } m+1 \leq j \leq 2m+l+l' \end{cases}$$

is a vpc from $B - v$ to B, which concludes the case $m > 0$.

Now assume $m < 0$. This means that the number of positive shifts of f exceeds the number of negative shifts of f between z_i and $z_{\mathrm{len}(z)}$ by more than l, namely by $-m + l$. It also means that if there are any negative shifts of f in z, they must be the last elements of z, outside of Aoverlap(F). So until z_i we have exactly $k + m - l \geq 1$ positive shifts of f (recall that z_1 is one of those), hence $-m + l < k$. Let i' with $i + 1 \leq i' \leq \mathrm{len}(z)$ be minimal such that $z_{i'}$ is a shift of f. With the above remark it follows that $z_{i'}$ is a positive shift of f, namely the $(m + (k-l) + 1)$-th one. With

$$\begin{aligned} P &:= A + (m + (k-l))\,\mathrm{vect}(f) - (m + (k-l))\frac{k'}{k}\,\mathrm{vect}(f') \\ &= \left(1 - \frac{m + (k-l)}{k}\right) A + \frac{m + (k-l)}{k}\, B \end{aligned}$$

we have $P \in \mathrm{conn}(A, B)$ and $z_{i,1} \in \mathrm{conn}(z_{i',1}, P)$. Since $z_{i',1} \geq \xi$ and $P \geq \xi$, we get $z_{i,1} \geq \xi$. Because of the condition $\frac{l'}{l+1} \leq \frac{k'}{k}$, every point $z_{i,1} + j\,\mathrm{vect}(f)$ for $j \in \mathbb{N}_{|m|-1}$ lies in $\mathrm{conn}(z_{i,1}, P')$ for

$$\begin{aligned} P' &:= A + (k' - l')\frac{k}{k'}\,\mathrm{vect}(f) - (k' - l')\,\mathrm{vect}(f') \\ &= \left(1 - \frac{k' - l'}{k'}\right) A + \frac{k' - l'}{k'}\, B, \end{aligned}$$

hence $z_{i,1} + j\,\mathrm{vect}(f) \geq \xi$. From this follows that z' defined as

$$z'_j := \begin{cases} ((B-v) - \mathrm{e}(\mathrm{lt}(f)) + \mathrm{negshift}(f) & \text{if } j = 1 \\ (z'_{j-1,2} - \mathrm{e}(\mathrm{lt}(f)) + \mathrm{negshift}(f) & \text{if } 2 \leq j \leq m \\ z_{i-m-1+j} & \text{if } m+1 \leq j \leq 2m+l+l' \end{cases}$$

is a vpc from $B - v$ to B, which concludes the case $\xi = \mathrm{e}(\mathrm{tt}(f))$. The case $\xi = \mathrm{e}(\mathrm{tt}(f'))$ works analogously, where instead of the condition $\frac{l'}{l+1} \leq \frac{k'}{k}$, we use $\frac{l'-1}{l} \leq \frac{k'}{k}$. □

Theorem 4.5.5. *Let $\xi \in \mathrm{e}(\mathrm{tt}(F))$ and $A, B \in \mathbb{N}^n$, $A, B \geq \xi$ and $A, B \not\geq \mathrm{e}(\mathrm{lt}(h))$ for any $h \in F$, such that there is a vpc from A to B. Let $f, f' \in F$, $f \neq f'$, and $k, k' \in \mathbb{N} \setminus \{0\}$ such that $A + k\,\mathrm{vect}(f) - k'\,\mathrm{vect}(f') = B$ and let $l \in \mathbb{N}_k$, $l' \in \mathbb{N}_{k'-1} \cup \{0\}$*

such that $\frac{l'}{l} < \frac{k'}{k}$ *and* $B - (l\,\mathrm{vect}(f) - l'\,\mathrm{vect}(f')) \geq \xi$. *Then there exists a vpc from* $B - (l\,\mathrm{vect}(f) - l'\,\mathrm{vect}(f'))$ *to* B.

Proof. We will adapt the proof of Theorem 4.5.4. Let z be a vpc of minimal length from A to B and $v := l\,\mathrm{vect}(f) - l'\,\mathrm{vect}(f')$. The first element in z can be a positive shift of f or f', the last only a negative shift of f or f'. Assume, z does not already go through $B - v$.

We first assume that $\xi = \mathrm{tt}(f)$. Then every shift of f' lies in $\mathrm{Aoverlap}(F)$, hence there are no positive shifts of f' in z and z_1 is a positive shift of f. If there are positive shifts of f in $\mathrm{Aoverlap}(F)$, then all the negative shifts of f (if any) have to occur as the last elements of z, outside of $\mathrm{Aoverlap}(F)$. If there are negative shifts of f in $\mathrm{Aoverlap}(F)$, then all the positive shifts of f have to occur as the first elements of z and their number exceeds the number of negative shifts of f by at least k at any index greater than k.

Note that $B - v = A + (k - l)\,\mathrm{vect}(f) - (k' - l')\,\mathrm{vect}(f')$. Let $r \in \mathbb{N}_{\mathrm{len}(z)}$ be such that z_r is the $(k' - l')$-th negative shift of f' in z and let $m \in \mathbb{Z} \setminus \{0\}$ be such that $z_{r,2} - m\,\mathrm{vect}(f) = B - v$. First assume $m > 0$. We show $z_{r,2} - \mathrm{vect}(f) \geq \xi$. If $\frac{k'-l'}{(k-l)+m-1} > \frac{k'}{k}$, then for

$$P := \left(1 - \frac{k' - l'}{k'}\right) A + \frac{k' - l'}{k'} B$$

we have $P \in \mathrm{conn}(A, B)$ and

$$z_{r,2} - \mathrm{vect}(f) = (1 - \lambda)(B - v) + \lambda P \in \mathrm{conn}(B - v, P),$$

where $\lambda = \frac{m-1}{(k'-l')\frac{k}{k'} - (k-l)} \in [0, 1]$, since $m - 1 < (k' - l')\frac{k}{k'} - (k - l)$ if and only if $\frac{k'-l'}{(k-l)+m-1} > \frac{k'}{k}$. Since $B - v \geq \xi$ and $P \geq \xi$, it follows that $z_{r,2} - \mathrm{vect}(f) \geq \xi$.

For the rest of case $m > 0$ assume $\frac{k'-l'}{(k-l)+m-1} \leq \frac{k'}{k}$. Let $r' \in \mathbb{N}_{r-1}$ be maximal such that $z_{r'}$ is a shift of f.

First assume that $z_{r'}$ is a positive shift of f. If $m \leq l + 1$, then for

$$\begin{aligned} P &:= z_{r',1} - \left(((k - l) + m - 1)\frac{k'}{k} - ((k' - l') - (r - r'))\right) \mathrm{vect}(f') \\ &= A + ((k - l) + m - 1)\,\mathrm{vect}(f) - ((k - l) + m - 1)\frac{k'}{k}\,\mathrm{vect}(f') \\ &= \left(1 - \frac{(k - l) + m - 1}{k}\right) A + \frac{(k - l) + m - 1}{k} B \end{aligned}$$

we have $P \in \mathrm{conn}(A, B)$ and

$$z_{r,2} - \mathrm{vect}(f) = (1 - \lambda) z_{r',1} + \lambda P \in \mathrm{conn}(z_{r',1}, P),$$

where $\lambda = \frac{r - r'}{((k-l)+m-1)\frac{k'}{k} - ((k'-l')-(r-r'))} \in (0, 1]$. Since $z_{r',1} \geq \xi$ and $P \geq \xi$, it follows that $z_{r,2} - \mathrm{vect}(f) \geq \xi$.

If $m > l+1$, then there is an r'' with $r+1 \leq r'' \leq \text{len}(z)$ such that $z_{r''}$ is a negative shift of f and

$$z_{r',1} - m' \,\text{vect}(f') = z_{r'',2}$$

for some $m' \in \mathbb{N}_{l'+(r-r')}$. We then have $z_{r,2} - \text{vect}(f) \in \text{conn}(z_{r',1}, z_{r'',2})$ and since $z_{r',1} \geq \xi$ and $z_{r'',2} \geq \xi$, also $z_{r,2} - \text{vect}(f) \geq \xi$.
Now assume that $z_{r'}$ is a negative shift of f. If $m \leq l$, then for

$$\begin{aligned} P &:= z_{r',2} - \left(((k-l)+m)\frac{k'}{k} - ((k'-l') - (r-r'))\right)\text{vect}(f') \\ &= A + ((k-l)+m)\,\text{vect}(f) - ((k-l)+m)\frac{k'}{k}\,\text{vect}(f') \\ &= (1 - \frac{(k-l)+m}{k})A + \frac{(k-l)+m}{k}B, \end{aligned}$$

we have $P \in \text{conn}(A, B)$ and

$$z_{r,2} = (1-\lambda)z_{r',2} + \lambda P \in \text{conn}(z_{r',2}, P),$$

where $\lambda = \frac{r-r'}{((k-l)+m)\frac{k'}{k} - ((k'-l')-(r-r'))} \in (0,1]$, since from $\frac{k'-l'}{(k-l)+m-1} \leq \frac{k'}{k}$ it follows that $\frac{k'-l'}{(k-l)+m} \leq \frac{k'}{k}$. Since $z_{r',2} \geq \xi$ and $P \geq \xi$, we get $z_{r,2} \geq \xi$ and since $z_{r,2} - m\,\text{vect}(f) = B - v \geq \xi$, it follows that $z_{r,2} - \text{vect}(f) \geq \xi$.
If $m > l$, then there is an r'' with $r+1 \leq r'' \leq \text{len}(z)$ such that $z_{r''}$ is a negative shift of f and

$$z_{r',2} - m' \,\text{vect}(f') = z_{r'',2}$$

for some $m' \in \mathbb{N}_{l'+(r-r'))}$. We then have $z_{r,2} \in \text{conn}(z_{r',2}, z_{r'',2})$ and since $z_{r',2} \geq \xi$ and $z_{r'',2} \geq \xi$, also $z_{r,2} \geq \xi$ and, like before, $z_{r,2} - \text{vect}(f) \geq \xi$.
So $z_{r,2} - m''\,\text{vect}(f) \geq \xi$ for every $m'' \in \mathbb{N}_m$. This shows that z' defined as

$$z'_j := \begin{cases} ((B-v) - \text{e}(\text{tt}(f)) + \text{posshift}(f) & \text{if } j = 1 \\ (z'_{j-1,2} - \text{e}(\text{tt}(f)) + \text{posshift}(f) & \text{if } 2 \leq j \leq m \\ z_{r-m-1+j} & \text{if } m+1 \leq j \leq 2m+l+l' \end{cases}$$

is a vpc from $B - v$ to B, which concludes the case $m > 0$.

Now assume $m < 0$. This means that the number of positive shifts of f exceeds the number of negative shifts of f between z_r and $z_{\text{len}(z)}$ by more than l, namely by $-m+l$. It also means that if there are any negative shifts of f in z, they must be the last elements of z, outside of Aoverlap(F). So until z_r we have exactly $k+m-l \geq 1$ positive shifts of f (recall that z_1 is one of those), hence $-m+l < k$. Let r',

$r+1 \leq r' \leq \mathrm{len}(z)$, be minimal such that $z_{r'}$ is a shift of f. With the above remark it follows that $z_{r'}$ is a positive shift of f, namely the $(m+(k-l)+1)$-th one. With

$$\begin{aligned} P &:= A + (m+(k-l))\,\mathrm{vect}(f) - (m+(k-l))\frac{k'}{k}\,\mathrm{vect}(f') \\ &= \left(1 - \frac{m+(k-l)}{k}\right) A + \frac{m+(k-l)}{k}\, B \end{aligned}$$

we have $P \in \mathrm{conn}(A,B)$ and $z_{r,2} \in \mathrm{conn}(z_{r',1}, P)$. Since $z_{r',1} \geq \xi$ and $P \geq \xi$, we get $z_{r,2} \geq \xi$. Because of the condition $\frac{l'}{l+1} \leq \frac{k'}{k}$, every point $z_{r,2} + j\,\mathrm{vect}(f)$ for $j \in \mathbb{N}_{|m|-1}$ lies in $\mathrm{conn}(z_{r,2}, P')$ for

$$\begin{aligned} P' &:= A + (k'-l')\frac{k}{k'}\,\mathrm{vect}(f) - (k'-l')\,\mathrm{vect}(f') \\ &= \left(1 - \frac{k'-l'}{k'}\right) A + \frac{k'-l'}{k'}\, B, \end{aligned}$$

hence $z_{r,2} + j\,\mathrm{vect}(f) \geq \xi$. From this follows that z' defined as

$$z'_j := \begin{cases} ((B-v) - \mathrm{e}(\mathrm{lt}(f)) + \mathrm{negshift}(f) & \text{if } j = 1 \\ (z'_{j-1,2} - \mathrm{e}(\mathrm{lt}(f)) + \mathrm{negshift}(f) & \text{if } 2 \leq j \leq m \\ z_{r-m-1+j} & \text{if } m+1 \leq j \leq 2m+l+l' \end{cases}$$

is a vpc from $B-v$ to B, which concludes the case $\xi = \mathrm{e}(\mathrm{tt}(f))$. The case $\xi = \mathrm{e}(\mathrm{tt}(f'))$ works analogously. □

While Theorems 4.5.2 and 4.5.3 give a concrete structure for the new binomial we exchange the old one with, Theorems 4.5.4 and 4.5.5 do not tell us which l and l' to choose. Algorithm 4.1.5 yields a list of possible structures and Theorem 4.5.18 tells us exactly which one of those to take. Before we state Theorem 4.5.18, we analyse the properties of the output of Algorithm 4.1.5 necessary for proving Theorem 4.5.18.

Theorem 4.5.6. *Algorithm 4.1.5 is correct and terminates.*

Proof. Correctness: Let $V(F)$ be the output of Algorithm 4.1.5 and $i \in \mathbb{N}_{\mathrm{len}(V(F))}$, $i \geq 2$. Let also E, c and c' be the corresponding values after the $(i-2)$-th iteration of the while loop. We then have

$$E = \bigcup_{j \in \mathbb{N}_i} \mathrm{negind}((V(F)_j)_2),$$

$$V(F)_{i,2} = V(F)_{i,1,1}\,\mathrm{vect}(F_1) + V(F)_{i,1,2}\,\mathrm{vect}(F_2),$$

$$V(F)_{i,2} \in \Omega_{\prec}$$

and, since $c = \max(\{j \in \mathbb{N}_{i-1} \mid V(F)_{j,1,1} > 0\})$ and $c' = \max(\{j \in \mathbb{N}_{i-1} \mid V(F)_{j,1,2} > 0\})$, also

$$V(F)_i \in \{v, -v\}$$

with v as in the output condition.
Termination: Let $l \in \mathbb{N}_n$. If $\mathrm{vect}(F_1)_l \leq 0$ or $\mathrm{vect}(F_2)_l \leq 0$, then l is added to E already before the first iteration of the while loop. Otherwise, we show that there is an $i > 2$ such that $V(F)_{i,2,l} \leq 0$, i.e. l is added to E during the $(i-2)$-th iteration of the while loop. Assume there is no such i. Then for each $i \in \mathbb{N}$ let $J^{(i)} := \{j \in \mathbb{N}_i \mid V(F)_{j,1,1} > 0\}$ and $J'^{(i)} := \{j \in \mathbb{N}_i \mid V(F)_{j,1,2} > 0\}$. We have

$$\text{for all } j, j' \in J^{(i)}, \text{ if } j < j' \text{ then } V(F)_{j,2,l} > V(F)_{j',2,l}$$

and

$$\text{for all } j, j' \in J'^{(i)}, \text{ if } j < j' \text{ then } V(F)_{j,2,l} > V(F)_{j',2,l}.$$

Since $J^{(i)} \cup J'^{(i)} = \mathbb{N}_i$ and $J^{(i)} \cap J'^{(i)} = \emptyset$ and since there are no infinitely descending chains of natural numbers, there has to be an $i > 2$ such that $V(F)_{i,2,l} \leq 0$. □

Since $\mathrm{vect}(F_1) = V(F)_{1,2}$ and $\mathrm{vect}(F_2) = V(F)_{2,2}$, the termination proof also proves an upper bound on the iterations of the while loop. Let

$$m := \max(\{\max(\mathrm{vect}(F_1)_j, \mathrm{vect}(F_2)_j) \mid j \in \mathbb{N}_n, \mathrm{vect}(F_1)_j > 0, \mathrm{vect}(F_2))_j > 0\}).$$

Then there are at most m iterations of the while loop in Algorithm 4.1.5. This number itself is bounded by

$$m' := \max(\{\mathrm{vect}(F_i)_j \mid i \in \{1, 2\}, j \in \mathbb{N}_n\}).$$

Lemma 4.5.7. *Let $V(F)$ be the output of Algorithm 4.1.5 and let us fix an iteration of the while loop in the algorithm. Let E, c and c' be the corresponding values after this iteration. Then*

$$\mathrm{negind}(V(F)_{c,2}) \cup \mathrm{negind}(V(F)_{c',2}) = E.$$

Proof. We write V for $V(F)$ and proceed by induction on $i \in \mathbb{N}_{\mathrm{len}(V)}$, $i \geq 2$. For $i = 2$, i.e. before the first iteration, we have

$$\begin{aligned} \mathrm{negind}(V_{c,2}) \cup \mathrm{negind}(V_{c',2}) &= \mathrm{negind}(V_{1,2}) \cup \mathrm{negind}(V_{2,2}) \\ &= \mathrm{negind}(\mathrm{vect}(F_1)) \cup \mathrm{negind}(\mathrm{vect}(F_2)) \\ &= E. \end{aligned}$$

Let now $i \in \mathbb{N}_{\mathrm{len}(V)}$, $i > 2$, and let c, c' and E be the current values after the $(i-2)$-th iteration of the while loop. Assume that until this iteration, i.e. for all $i' \in \mathbb{N}_{\mathrm{len}(V)}$,

$2 \leq i' < i$, the claim in the theorem holds. Clearly, $\operatorname{negind}(V_{c,2}) \cup \operatorname{negind}(V_{c',2}) \subseteq E$. Assume, there is an $l \in E$ such that $l \notin \operatorname{negind}(V_{c,2}) \cup \operatorname{negind}(V_{c',2})$. Assume w.l.o.g. $c < c'$ and let $c'' \in \mathbb{N}_{c'-1}$ such that $V_{c'} = V_{c''} - V_c$. Since $l \notin \operatorname{negind}(V_{c',2}) = \operatorname{negind}(V_{i,2})$, we know that l has been added to E in an earlier iteration than the $(i-2)$-th one. Hence, by the induction assumption, $l \in \operatorname{negind}(V_{c'',2}) \cup \operatorname{negind}(V_{c,2})$. Since $l \notin \operatorname{negind}(V_{c,2})$, we obtain $l \in \operatorname{negind}(V_{c'',2})$ and since $V_{c'} + V_c = V_{c''}$ and $V_{c'',2,l} \leq 0$, we get $V_{c',2,l} \leq 0$ or $V_{c,2,l} \leq 0$, hence $l \in \operatorname{negind}(V_{c,2}) \cup \operatorname{negind}(V_{c',2})$, which is a contradiction. □

Corollary 4.5.8. *Let $V(F)$ be the output of Algorithm 4.1.5 and $c, c' \in \mathbb{N}_{\operatorname{len}(V(F))}$ maximal such that $V(F)_{c,1,1} > 0$ and $V(F)_{c',1,2} > 0$. Then*

$$\operatorname{negind}(V(F)_{c,2}) \cup \operatorname{negind}(V(F)_{c',2}) = \mathbb{N}_n.$$

Proof. Since c and c' are the corresponding values after the last iteration of the while loop, the claim follows directly from Lemma 4.5.7 and the abort condition for the while loop in Algorithm 4.1.5. □

Let us now consider the following procedure which is simply Algorithm 4.1.5 without the termination condition. We will denote the list V' generated by the procedure as $V'(F)$.

Procedure 4.5.9.

Input: *F, a set of two proper binomials*
$V' \leftarrow (((1,0), \operatorname{vect}(F_1)), ((0,1), \operatorname{vect}(F_2)))$;
$c \leftarrow 1$;
$c' \leftarrow 2$;
while $1 = 0$
  $v \leftarrow V'_c - V'_{c'}$;
  if $v_2 \in \Omega_{\prec}$ ***then*** $V' \leftarrow \operatorname{append}(V', v)$; $c \leftarrow \operatorname{len}(V')$;
    else $V' \leftarrow \operatorname{append}(V', -v)$; $c' \leftarrow \operatorname{len}(V')$;
  end if;
end while;

In Lemmas 4.5.10 to 4.5.14 we prove a few properties of the infinite sequence generated by Procedure 4.5.9 which we will need later.

Lemma 4.5.10. *Let $V'(F)$ be the infinite list produced by Procedure 4.5.9 and $i \in \mathbb{N}$, $i \geq 3$. Let $j \in \{1,2\}$ be such that $V'(F)_{i,1,j} > 0$, and $j' \in \{1,2\}$, $j' \neq j$. Furthermore, let $i' \in \mathbb{N}_{i-1}$ be maximal such that $V'(F)_{i',1,j'} > 0$. Then*

$$V'(F)_{i',1,j'} V'(F)_{i,1,j} - V'(F)_{i',1,j} V'(F)_{i,1,j'} = 1.$$

Proof. We write V' for $V'(F)$ and proceed by induction on i. For the base case, we investigate $i = 3$. We get $(V'_{i,1,j}, V'_{i,1,j'}) = (1, -1)$ and $(V'_{i',1,j}, V'_{i',1,j'}) = (0, 1)$, hence

$$V'_{i',1,j'}V'_{i,1,j} - V'_{i',1,j}V'_{i,1,j'} = 1 \cdot 1 - 0 \cdot (-1) = 1.$$

For the induction step, let $i'' \in \mathbb{N}_{i-1}$ be maximal such that $V'_{i'',1,j} > 0$. Then $V'_i = V'_{i''} - V'_{i'}$. By the induction assumption,

$$V'_{i',1,j'}V'_{i'',1,j} - V'_{i',1,j}V'_{i'',1,j'} = 1,$$

hence

$$\begin{aligned} V'_{i',1,j'}V'_{i,1,j} - V'_{i',1,j}V'_{i,1,j'} & \\ &= V'_{i',1,j'}(V'_{i'',1,j} - V'_{i',1,j}) - V'_{i',1,j}(V'_{i'',1,j'} - V'_{i',1,j'}) \\ &= V'_{i',1,j'}V'_{i'',1,j} - V'_{i',1,j}V'_{i'',1,j'} \\ &= 1 \end{aligned}$$

□

Lemma 4.5.11. *Let $V'(F)$ be the infinite list produced by Procedure 4.5.9 and let $i \in \mathbb{N} \setminus \{0\}$ and $j, j' \in \{1, 2\}$ be such that $V'(F)_{i,1,j} > 1$ and $V'(F)_{i,1,j'} < -1$. Let $i' \in \mathbb{N}_{i-1}$ be maximal such that $V'(F)_{i',1,j'} > 0$. Then*

$$\frac{-V'(F)_{i,1,j'}}{V'(F)_{i,1,j}} < \frac{V'(F)_{i',1,j'}}{-V'(F)_{i',1,j}}.$$

Proof. From the conditions in the lemma we know that $i' \geq 3$, hence $-V'(F)_{i',1,j} > 0$. Therefore the fractions are well-defined and by Lemma 4.5.10 the claim follows. □

Lemma 4.5.12. *Let $V'(F)$ be the infinite list produced by Procedure 4.5.9 and $i \in \mathbb{N} \setminus \{0\}$. Let $j \in \{1, 2\}$ be such that $V'(F)_{i,1,j} > 0$, and $j' \in \{1, 2\}$, $j' \neq j$. Furthermore, let $i' > i$ be minimal such that $V'(F)_{i',1,j} > 0$. Then*

$$\frac{-V'(F)_{i,1,j'}}{V'(F)_{i,1,j}} < \frac{-V'(F)_{i',1,j'}}{V'(F)_{i',1,j}}.$$

Proof. We write V' for $V'(F)$. If $i \in \{1, 2\}$ then either $i' = 3$, $i = j$ and

$$(V'_{i',1,j}, V'_{i',1,j'}) = (1, -1) = (V'_{i,1,j}, -V'_{j',1,j'})$$

and so

$$\frac{-V'_{i,1,j'}}{V'_{i,1,j}} = \frac{0}{1} < \frac{-(-1)}{1} = \frac{-V'_{i',1,j'}}{V'_{i',1,j}},$$

or $i' > 3$, $i = j$ and

$$(V'_{i',1,j}, V'_{i',1,j'}) = (i-2, -1) = (V'_{i,1,j} - V'_{i'-1,1,j}, -V'_{i'-1,1,j'})$$

and so

$$\frac{-V'_{i,1,j'}}{V'_{i,1,j}} = \frac{0}{1} < \frac{-(-1)}{i-2} = \frac{-V'_{i',1,j'}}{V'_{i',1,j}}.$$

Now let $i \in \mathbb{N}$, $i \geq 3$. There exists an $i'' \in \mathbb{N}_{i'-1}$ such that $V'_{i'',1,j'} > 0$ and $V'_{i'} = V'_i - V'_{i''}$. Note that for all $a, b, c, d \in \mathbb{N} \setminus \{0\}$ we have $\frac{a+c}{b+d} > \frac{a}{b}$ if and only if $\frac{c}{d} > \frac{a}{b}$. Therefore, since $\frac{V'_{i'',1,j'}}{-V'_{i'',1,j}} > \frac{-V'_{i,1,j'}}{V'_{i,1,j}}$ and $V'_{i'',1,j'}, -V'_{i'',1,j} > 0$, we obtain by Lemma 4.5.11,

$$\frac{-V'_{i',1,j'}}{V'_{i',1,j}} = \frac{-V'_{i,1,j'} + V'_{i'',1,j'}}{V'_{i,1,j} - V'_{i'',1,j}} > \frac{-V'_{i,1,j'}}{V'_{i,1,j}}.$$

□

Lemma 4.5.13. *Let $V'(F)$ be the infinite list produced by Procedure 4.5.9 and let $i \in \mathbb{N} \setminus \{0\}$ and $j, j' \in \{1, 2\}$ be such that $V'(F)_{i,1,j} > 1$ and $V'(F)_{i,1,j'} < -1$. Let $i' \in \mathbb{N}_{i-1}$ be maximal such that $V'(F)_{i',1,j'} > 0$. Then*

$$\frac{V'(F)_{i',1,j'} - 1}{-V'(F)_{i',1,j}} \leq \frac{-V'(F)_{i,1,j'} - 1}{V'(F)_{i,1,j}}$$

and

$$\frac{V'(F)_{i',1,j'}}{-V'(F)_{i',1,j} + 1} \leq \frac{-V'(F)_{i,1,j'}}{V'(F)_{i,1,j} + 1}.$$

Proof. We write V' for $V'(F)$. We know that $i' \geq 3$, hence $-V'_{i',1,j} > 0$. So the fractions are well-defined. We have

$$\frac{V'_{i',1,j'} - 1}{-V'_{i',1,j}} \leq \frac{-V'_{i,1,j'} - 1}{V'_{i,1,j}}$$

if and only if

$$V'_{i',1,j'}V'_{i,1,j} - V'_{i,1,j} \leq V'_{i',1,j}V'_{i,1,j'} + V'_{i',1,j}$$

if and only if

$$V'_{i',1,j'}V'_{i,1,j} - V'_{i',1,j}V'_{i,1,j'} \leq V'_{i,1,j} + V'_{i',1,j}. \tag{4.6}$$

There exists an $i'' \in \mathbb{N}_{i-1}$, $i'' \geq 3$, such that $V'_{i'',1,j} > 0$ and $V'_i = V'_{i''} - V'_{i'}$, hence

$$V'_{i,1,j} + V'_{i',1,j} = V'_{i'',1,j} \geq 1,$$

and by Lemma 4.5.10,

$$V'_{i',1,j'}V'_{i,1,j} - V'_{i',1,j}V'_{i,1,j'} = 1,$$

which proves (4.6).

Similarly,

$$\frac{V'_{i',1,j'}}{-V'_{i',1,j}+1} \leq \frac{-V'_{i,1,j'}}{V'_{i,1,j}+1}$$

if and only if

$$V'_{i',1,j'}V'_{i,1,j} + V'_{i',1,j'} \leq V'_{i',1,j}V'_{i,1,j'} - V'_{i,1,j'}$$

if and only if

$$V'_{i',1,j'}V'_{i,1,j} - V'_{i',1,j}V'_{i,1,j'} \leq -V'_{i,1,j'} - V'_{i',1,j'}. \tag{4.7}$$

With the same i'' as above, we get

$$-V'_{i,1,j'} - V'_{i',1,j'} = -V'_{i'',1,j'} \geq 1,$$

which proves (4.7). □

Lemma 4.5.14. *Let $V'(F)$ be the infinite list produced by Procedure 4.5.9 and let $i \in \mathbb{N} \setminus \{0\}$ and $j, j' \in \{1,2\}$ be such that $V'(F)_{i,1,j} > 1$ and $V'(F)_{i,1,j'} < -1$. Let $i' \in \mathbb{N}_{i-1}$ be maximal such that $V'(F)_{i',1,j} > 0$. Then*

$$\frac{-V'(F)_{i',1,j'}}{V'(F)_{i',1,j}} \geq \frac{-V'(F)_{i,1,j'}-1}{V'(F)_{i,1,j}}$$

and

$$\frac{-V'(F)_{i',1,j'}}{V'(F)_{i',1,j}} \leq \frac{-V'(F)_{i,1,j'}}{V'(F)_{i,1,j}+1}.$$

Proof. We write V' for $V'(F)$. Let $i'' \in \mathbb{N}_{i-1}$ be maximal such that $V'_{i'',1,j'} > 0$. We have $V'_i = V'_{i'} - V'_{i''}$, hence

$$\frac{-V'_{i',1,j'}}{V'_{i',1,j}} \geq \frac{-V'_{i,1,j'}-1}{V'_{i,1,j}}$$

if and only if

$$-V'_{i',1,j'}V'_{i,1,j} \geq -V'_{i,1,j'}V'_{i',1,j} - V'_{i',1,j}$$

if and only if

$$(-V'_{i,1,j'} - V'_{i'',1,j'})V'_{i,1,j} \geq -V'_{i,1,j'}(V'_{i,1,j} + V'_{i'',1,j}) - (V'_{i,1,j} + V'_{i'',1,j})$$

if and only if

$$-V'_{i'',1,j'}V'_{i,1,j} \geq -V'_{i,1,j'}V'_{i'',1,j} - V'_{i,1,j} - V'_{i'',1,j}$$

if and only if

$$(-V'_{i,1,j'} - 1)(-V'_{i'',1,j}) \geq (V'_{i'',1,j'} - 1)V'_{i,1,j}$$

if and only if

$$\frac{-V'_{i,1,j'}-1}{V'_{i,1,j}} \geq \frac{V'_{i'',1,j'}-1}{-V'_{i'',1,j}},$$

which follows from Lemma 4.5.13.

Likewise,

$$\frac{-V'_{i',1,j'}}{V'_{i',1,j}} \geq \frac{-V'_{i,1,j'}}{V'_{i,1,j}+1}$$

if and only if

$$\frac{-V'_{i,1,j'}}{V'_{i,1,j}+1} \geq \frac{V'_{i'',1,j'}}{-V'_{i'',1,j}+1},$$

which again follows from Lemma 4.5.13. □

The following lemma takes care of a special case in the proof of Theorem 4.5.18.

Lemma 4.5.15. *Let $V'(F)$ be the infinite list produced by Procedure 4.5.9, $j \in \{1,2\}$ such that $V'(F)_{3,1,j} = 1$, $j' \in \{1,2\}$ such that $j' \neq j$, and $i \in \mathbb{N}$, $i \geq 4$, minimal such that $V'(F)_{i,1,j} = -1$. Let $l, l' \in \mathbb{Z} \setminus \{0\}$, one being positive and one being negative, and let $\xi \in \mathrm{e}(\mathrm{tt}(F))$ and $A, B \in \mathbb{N}^n$, $A, B \geq \xi$, $A, B \not\geq \mathrm{e}(\mathrm{lt}(F_i))$ for any $i \in \{1,2\}$, such that $A + l\,\mathrm{vect}(F_j) + l'\,\mathrm{vect}(F_{j'}) = B$ and such that there is a vpc from A to B. If $l > 0$ and $1 \geq \frac{-l'}{l}$, then there exists a vpc from $B - V'(F)_{3,2}$ to B. If $l < 0$ and $\frac{1}{i-2} \geq \frac{-l}{l'}$, then there exists a vpc from $B - V'(F)_{i,2}$ to B.*

Proof. We write V' for $V'(F)$. Assume $\xi = \mathrm{e}(\mathrm{tt}(F_j))$. Consider first the case $l < 0$ and $\frac{1}{i-2} \geq \frac{-l}{l'}$. We have $1 \leq -l$ and because of $l' \geq (i-2)(-l)$ also $i - 2 \leq l'$, so we can use Theorem 4.5.4. Since

$$\frac{-V'_{i,1,j}}{V'_{i,1,j'}} = \frac{-(-1)}{i-2} \geq \frac{-l}{l'}$$

and

$$\frac{-V'_{i,1,j}-1}{V'_{i,1,j'}} = \frac{0}{i-2} < \frac{-l}{l'},$$

there exists a vpc from $B - V'_{i,2}$ to B.
Now consider $l > 0$ and $1 \geq \frac{-l'}{l}$. We have

$$\frac{-V'_{3,1,j'}}{V'_{3,1,j}} = \frac{-(-1)}{1} \geq \frac{-l'}{l}$$

but in general, $\frac{-V'_{3,1,j'}}{V'_{3,1,j}+1} = \frac{1}{2}$ is not necessarily smaller than or equal to $\frac{-l'}{l}$. So let z be a vpc of minimal length from A to B and assume that it does not already go through $B - V'_{3,2}$. All the shifts of $F_{j'}$ are negative ones. Let $r \in \mathbb{N}_{len(z)}$ be such that z_r is the last negative shift of $F_{j'}$ in z. Let $m \in \mathbb{Z} \setminus \{0\}$ such that $z_{r,1} - m\,\mathrm{vect}(F_j) = B - V'_{3,2}$. Recall that in the proof of Theorem 4.5.4, condition

$$\frac{-V'_{3,1,j'}}{V'_{3,1,j}+1} = \frac{1}{2} \leq \frac{-l'}{l}$$

was only needed for the case $m < 0$. After z_r there can only be negative shifts of F_j. Since $z_{r,1} - m\,\mathrm{vect}(F_j) = B - V'_{3,2}$, their number is at most $m + V'_{3,1,j}$. But

$m + V'_{3,1,j} = m + 1 \leq 0$, so $r = \text{len}(z)$. But then $B - V'_{3,2} = z_{r,1} - \text{vect}(F_j)$, hence $m = 1$ which contradicts $m < 0$. So the case $m < 0$ can actually not occur and by Theorem 4.5.4 there exists a vpc from $B - V'_{3,2}$ to B. The case $\xi = \text{e}(\text{tt}(F_{j'}))$ works analogously. □

The following lemma is needed in the proof of Theorem 4.5.18 and connects the output of Procedure 4.5.9 to the question if a certain vector generated by $\text{vect}(F_1)$ and $\text{vect}(F_2)$ lies in $\Omega_\prec$ or not.

Lemma 4.5.16. *Let $V'(F)$ be the infinite list produced by Procedure 4.5.9 and $j, j' \in \{1,2\}$, $j \neq j'$. Let $l, l' \in \mathbb{Z}$ such that $l > 0$ and $l' < 0$. Let $i \in \mathbb{N}$ be maximal such that $0 < V'(F)_{i,1,j} \leq l$ and $-V'(F)_{i,1,j'} \leq -l'$. If $\frac{-V'(F)_{i,1,j'}}{V'(F)_{i,1,j}} < \frac{-l'}{l}$, then $l\,\text{vect}(F_j) + l'\,\text{vect}(F_{j'}) \notin \Omega_\prec$.*

Proof. We write V' for $V'(F)$ and proceed by induction on i. For the base case we either have $l = 1$ or $l' = -1$. If $l = 1$, then $V'_{i,1,j} = 1$ and $-V'_{i,1,j'} < -l'$. But then

$$(V'_{i+1,1,j}, V'_{i+1,1,j'}) = (-1, -V'_{i,1,j'} + 1)$$

and

$$(-l, -l') = (-1, -l') = (V'_{i+1,1,j}, V'_{i+1,1,j'}) + (-l' + V'_{i,1,j'} - 1)(0,1).$$

Since $-l' + V'_{i,1,j'} - 1 \geq 0$, $V'_{i+1,2} \in \Omega_\prec$ and $(V'_{j',1,j}, V'_{j',1,j'}) = (0,1)$ and $V'_{j',2} \in \Omega_\prec$, it follows that

$$-l\,\text{vect}(F_j) - l'\,\text{vect}(F_{j'}) = V'_{i+1,2} + (-l' + V'_{i,1,j'} - 1)V'_{j',2} \in \Omega_\prec,$$

hence

$$l\,\text{vect}(F_j) + l'\,\text{vect}(F_{j'}) \notin \Omega_\prec.$$

If $l' = -1$, then $V'_{i,1,j'} \in \{0, -1\}$. If $V'_{i,1,j'} = -1$, then from $\frac{-V'_{i,1,j'}}{V'_{i,1,j}} < \frac{-l'}{l}$ we get $V'_{i,1,j} > l$, which contradicts the condition $V'_{i,1,j} \leq l$. So $V'_{i,1,j'} = 0$ and $V'_{i,1,j} = 1$, hence $i = j$. Let $i' \in \mathbb{N}$ be such that $V'_{i',1,j'} = -1$. This i' is unique and $i' > i$. Also, $V'_{i',1,j} > l$. It follows that $i' > l + 2$ and hence,

$$(V'_{l+2,1,j}, V'_{l+2,1,j'}) = (-l, 1) = (-l, -l').$$

We obtain

$$-l\,\text{vect}(F_j) - l'\,\text{vect}(F_{j'}) = V'_{l+2,2} \in \Omega_\prec,$$

hence

$$l\,\text{vect}(F_j) + l'\,\text{vect}(F_{j'}) \notin \Omega_\prec.$$

We now proceed with the induction step. We know $l > 1$ and $l' < -1$. Let $i' \in \mathbb{N}$ be maximal such that $V'_{i',1,j'} > 0$, $-V'_{i',1,j} \leq l$ and $V'_{i',1,j'} \leq -l'$. In the lemma we assume

$$\frac{-V'_{i,1,j'}}{V'_{i,1,j}} < \frac{-l'}{l}, \tag{4.8}$$

and by Lemma 4.5.10 we have

$$V'_{i,1,j}V'_{i',1,j'} - V'_{i,1,j'}V'_{i',1,j} = 1. \tag{4.9}$$

If $-V'_{i',1,j} = l$ and $V'_{i',1,j'} = -l'$, then $-l\,\mathrm{vect}(F_j) - l'\,\mathrm{vect}(F_{j'}) = V'_{i',2} \in \Omega_{\prec}$, hence $l\,\mathrm{vect}(F_j) + l'\,\mathrm{vect}(F_{j'}) \notin \Omega_{\prec}$.
If $-V'_{i',1,j} < l$ and $V'_{i',1,j'} = -l'$, then from (4.8) we get

$$\frac{-V'_{i,1,j'}}{V'_{i,1,j}} < \frac{V'_{i',1,j'}}{l},$$

which, by (4.9) is equivalent to

$$-V'_{i,1,j'}(l + V'_{i',1,j}) < V'_{i,1,j}V'_{i',1,j'} - V'_{i,1,j'}V'_{i',1,j} = 1.$$

Since $-V'_{i,1,j'}$ and $(l + V'_{i',1,j})$ are both positive natural numbers, this cannot be. Therefore this case cannot occur.
If $-V'_{i',1,j} = l$ and $V'_{i',1,j'} < -l'$, then

$$(l, l') = (-V'_{i',1,j}, -V'_{i',1,j'}) + (0, l' + V'_{i',1,j'})$$

and since $-V'_{i',2} \notin \Omega_{\prec}$ and, because of $l' + V'_{i',1,j'} < 0$, also $(l' + V'_{i',1,j'})\,\mathrm{vect}(F_{j'}) \notin \Omega_{\prec}$, we get

$$l\,\mathrm{vect}(F_j) + l'\,\mathrm{vect}(F_{j'}) = -V'_{i',2} + (l' + V'_{i',1,j'})\,\mathrm{vect}(F_{j'}) \notin \Omega_{\prec}.$$

Now assume $-V'_{i',1,j} < l$ and $V'_{i',1,j'} < -l'$. We prove

$$l\,\mathrm{vect}(F_j) + l'\,\mathrm{vect}(F_{j'}) + V'_{i',2} \notin \Omega_{\prec}$$

by using the induction hypothesis. For this we first show

$$\frac{-V'_{i,1,j'}}{V'_{i,1,j}} < \frac{-l' - V'_{i',1,j'}}{l + V'_{i',1,j}}. \tag{4.10}$$

The inequality in (4.10) holds if and only if

$$V'_{i,1,j}V'_{i',1,j'} - V'_{i,1,j'}V'_{i',1,j} < V'_{i,1,j}(-l') + V'_{i,1,j'}l,$$

which by (4.9) is equivalent to

$$1 < V'_{i,1,j}(-l') + V'_{i,1,j'}l. \tag{4.11}$$

From (4.8) we obtain $0 < V'_{i,1,j}(-l') + V'_{i,1,j'}l$, hence

$$V'_{i,1,j}(-l') + V'_{i,1,j'}l \in \mathbb{N} \setminus \{0\}.$$

So in order to prove (4.11), it remains to show that

$$V'_{i,1,j}(-l') + V'_{i,1,j'}l \neq 1.$$

Assume for a contradiction that $V'_{i,1,j}(-l') + V'_{i,1,j'}l = 1$. The linear Diophantine equation

$$V'_{i,1,j}\, x + V'_{i,1,j'}\, y = 1 \tag{4.12}$$

has $(\tilde{x}, \tilde{y}) = (V'_{i',1,j'}, -V'_{i',1,j})$ as a particular solution. All the other solutions (x, y) are given by

$$\begin{aligned}(x, y) &= (\tilde{x} + mV'_{i,1,j'},\ \tilde{y} - mV'_{i,1,j}) \\ &= (V'_{i',1,j'} + mV'_{i,1,j'},\ -V'_{i',1,j} - mV'_{i,1,j})\end{aligned}$$

for $m \in \mathbb{Z}$. Since $(-l', l)$ is also a solution to 4.12, there is an $m \in \mathbb{Z}$ such that

$$(-l', l) = (V'_{i',1,j'} + mV'_{i,1,j'}, -V'_{i',1,j} - mV'_{i,1,j}).$$

Since $-l' \geq V'_{i',1,j'}$ and $l \geq -V'_{i',1,j}$, it follows that $m \leq 0$, and since

$$-l' < |V'_{\max(i,i')+1,\,1,\,j'}| = V'_{i',1,j'} - V'_{i,1,j'}$$

and

$$l < |V'_{\max(i,i')+1,\,1,\,j}| = -V'_{i',1,j} + V'_{i,1,j},$$

it follows that $m > -1$. Therefore, $m = 0$ and

$$(-l', l) = (V'_{i',1,j'}, -V'_{i',1,j}),$$

which contradicts the assumption that $-V'_{i',1,j} < l$ and $V'_{i',1,j'} < -l'$. This concludes the proof for (4.10).

We have $0 < -l' - V'_{i',1,j'} < -V'_{i,1,j'}$ and $0 < l + V'_{i',1,j} < V'_{i,1,j}$ and so there exists a maximal $i'' \in \mathbb{N}_{i-1}$ such that $V'_{i'',1,j} > 0$, $V'_{i'',1,j} \leq l + V'_{i',1,j}$ and $-V'_{i'',1,j'} \leq -l' - V'_{i',1,j'}$. By Lemma 4.5.12 we have

$$\frac{-V'_{i'',1,j'}}{V'_{i'',1,j}} < \frac{-V'_{i,1,j'}}{V'_{i,1,j}}$$

and so by (4.10),

$$\frac{-V'_{i'',1,j'}}{V'_{i'',1,j}} < \frac{-l' - V'_{i',1,j'}}{l + V'_{i',1,j}}.$$

Now we can use the induction assumption, which yields

$$l\,\mathrm{vect}(F_j) + l'\,\mathrm{vect}(F_{j'}) + V'_{i',2} \notin \Omega_{\prec}.$$

Since $-V'_{i',2} \notin \Omega_{\prec}$, it follows that

$$l\,\mathrm{vect}(F_j) + l'\,\mathrm{vect}(F_{j'}) = (l\,\mathrm{vect}(F_j) + l'\,\mathrm{vect}(F_{j'}) + V'_{i',2}) - V'_{i',2} \notin \Omega_{\prec}.$$

□

Lemma 4.5.17. *Let $V(F)$ be the output of Algorithm 4.1.5 and $V'(F)$ the infinite list produced by Procedure 4.5.9. Let $j \in \{1,2\}$ and let $i \in \mathbb{N}_{\mathrm{len}(V(F))}$ be maximal such that $V(F)_{i,1,j} > 0$. Let $i' \in \mathbb{N}$, $i' > i$, such that $V'(F)_{i',1,j} > 0$ and let $r \in \mathbb{N}_n$. If $V(F)_{i,2,r} > 0$, then $V'(F)_{i',2,r} \geq V(F)_{i,2,r}$.*

Proof. Let $j' \in \{1,2\}$ such that $j' \neq j$ and let $i'' \in \mathbb{N}_{\mathrm{len}(V(F))}$ be maximal such that $V(F)_{i'',1,j'} > 0$. We have $V'(F)_{i'} = mV(F)_i - m'V(F)_{i''}$ for some $m, m' \in \mathbb{N} \setminus \{0\}$. Since $V(F)_{i,2,r} > 0$, it follows from Corollary 4.5.8 that $V(F)_{i'',2,r} \leq 0$. Hence,

$$V'(F)_{i',2,r} = mV(F)_{i,2,r} - m'V(F)_{i'',2,r} \geq V(F)_{i,2,r}.$$

□

Now comes the first of the two main theorems in this subsection (the other one being Theorem 4.5.27). It says that for every binomial g in the reduced Gröbner basis such that $\mathrm{supp}(g) \subseteq [X]\,\mathrm{tt}(f)$ for some $f \in F$, there exists an $h \in \mathrm{ideal}(F)$ such that $\mathrm{lt}(h) = \mathrm{lt}(g)$ and $\mathrm{vect}(h)$ is contained in the output of Algorithm 4.1.5.

Theorem 4.5.18. *Let $V(F)$ be the output of Algorithm 4.1.5 and $\xi \in \mathrm{e}(\mathrm{tt}(F))$. Let $A, B \in \mathbb{N}^n$, $A, B \geq \xi$, $A, B \not\geq \mathrm{e}(\mathrm{lt}(F_r))$ for any $r \in \{1,2\}$, $B - A \in \Omega_{\prec}$, such that there exists a vpc from A to B. Then there exists an $i \in \mathbb{N}_{\mathrm{len}(V(F))}$ such that there is a vpc from $B - V(F)_{i,2}$ to B.*

Proof. Since there is a vpc from A to B, there exist $k, k' \in \mathbb{Z}$ such that

$$A + k\,\mathrm{vect}(F_1) + k'\,\mathrm{vect}(F_2) = B.$$

If $k = 0$ or $k' = 0$, then we have $k' > 0$ or $k > 0$, respectively, and the claim follows from Theorem 4.5.2. If $k, k' \geq 1$, then the claim follows from Theorem 4.5.3. The

numbers k and k' cannot both be negative, since this would contradict $B - A \in \Omega_\prec$. Now assume that $k, k' \neq 0$ and that they have different sign. Let w.l.o.g. $k > 0$ and $k' < 0$ and let $V'(F)$ be the infinite list produced by Procedure 4.5.9. We write V and V' for $V(F)$ and $V'(F)$, respectively. Since $B - A \in \Omega_\prec$, we get by Lemma 4.5.16 the existence of an $i' \in \mathbb{N} \setminus \{0\}$ such that $0 < V'_{i',1,1} \leq k$, $-V'_{i',1,2} \leq -k'$ and

$$\frac{-V'_{i',1,2}}{V'_{i',1,1}} \geq \frac{-k'}{k}.$$

We choose i' to be minimal with these properties and first show the existence of a vpc from $B - V'_{i',2}$ to B. Note that $i' \geq 3$. First assume $V'_{i',1,1}, -V'_{i',1,2} > 1$. If $\frac{-V'_{i',1,2}-1}{V'_{i',1,1}} > \frac{-k'}{k}$ or $\frac{-V'_{i',1,2}}{V'_{i',1,1}+1} > \frac{-k'}{k}$, then let $i'' \in \mathbb{N}_{i'-1}$ be maximal such that $V'_{i'',1,1} > 0$. By Lemma 4.5.14,

$$\frac{-V'_{i'',1,2}}{V'_{i'',1,1}} \geq \frac{-V'_{i',1,2} - 1}{V'_{i',1,1}}$$

and

$$\frac{-V'_{i'',1,2}}{V'_{i'',1,1}} \geq \frac{-V'_{i',1,2}}{V'_{i',1,1} + 1},$$

hence

$$\frac{-V'_{i'',1,2}}{V'_{i'',1,1}} > \frac{-k'}{k}.$$

Since also $0 < V'_{i'',1,1} \leq k$, $-V'_{i'',1,2} \leq -k'$, this contradicts the minimality of i'. So in fact we have

$$\frac{-V'_{i',1,2} - 1}{V'_{i',1,1}} \leq \frac{-k'}{k}$$

and

$$\frac{-V'_{i',1,2}}{V'_{i',1,1} + 1} \leq \frac{-k'}{k}$$

and with Theorem 4.5.4 we get the existence of a vpc from $B - V'_{i',2}$ to B.
Now assume $V'_{i',1,1} = 1$ and $V'_{i',1,2} < -1$. If $\frac{-V'_{i',1,2}}{V'_{i',1,1}+1} > \frac{-k'}{k}$, then since

$$V'_{i'-1,1} = V'_{i',1} + (0, 1),$$

also

$$\frac{-V'_{i'-1,1,2}}{V'_{i'-1,1,1}} > \frac{-k'}{k},$$

which contradicts the minimality of i'. So also in this case we can use Theorem 4.5.4 to get the existence of a vpc from $B - V'_{i',2}$ to B.
If $i' = 3$ or $-V'_{i',1,2} = 1$, then the conditions of Lemma 4.5.15 are fulfilled and we get the existence of a vpc from $B - V'_{i',2}$ to B.
Now we prove the existence of a vpc from $B - V_{i,2}$ to B for an $i \in \mathbb{N}_{\text{len}(V)}$. If $i' \leq \text{len}(V)$, this follows with $i := i'$. So now assume $i' > \text{len}(V)$. Let $i \in \mathbb{N}_{\text{len}(V)}$ be maximal such

that $V_{i,1,1} > 0$. We show that $B - V_{i,2} \geq \xi$. Let $r \in \mathbb{N}_n$. If $V_{i,2,r} \leq 0$, then from $B_r \geq \xi_r$ follows $B_r - V_{i,2,r} \geq \xi_r$. If $V_{i,2,r} > 0$, then by Lemma 4.5.17 we get

$$V'_{i',2,r} - V_{i,2,r} \geq 0. \tag{4.13}$$

Since $V_{i,1,1} \leq V'_{i',1,1} \leq k$, $-V_{i,1,2} < -V'_{i',1,2} \leq -k'$, $\frac{-V'_{i',1,2}}{V'_{i',1,1}} \geq \frac{-k'}{k}$ and $\frac{-V_{i,1,2}}{V_{i,1,1}} < \frac{-k'}{k}$, there exists a unique $P \in \mathrm{conn}(A, B) \cap \mathrm{conn}(B - V'_{i',2}, B - V_{i,2})$. For this P, we have $P \geq \xi$ (hence $P_r \geq \xi_r$) and either

$$B_r - V_{i,2,r} \leq P_r \leq B_r - V'_{i',2,r}$$

or

$$B_r - V'_{i',2,r} \leq P_r \leq B_r - V_{i,2,r}.$$

Because of (4.13), the latter is the case and we get $B_r - V_{i,2,r} \geq \xi_r$. Finally, by Theorem 4.5.5, there exists a vpc from $B - V_{i,2}$ to B. □

Definition 4.5.19. *For $A, B \in \mathbb{N}^n$ we define*

$$\mathrm{par}(A, B) := \{A + \lambda(B - A) + \lambda'(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \mid \lambda, \lambda' \in [0, 1]\}.$$

Note that $\mathrm{par}(A, B)$ is a parallelogram with delimiter points A, B, $A + \mathrm{vect}(F_1) + \mathrm{vect}(F_2)$ and $B + \mathrm{vect}(F_1) + \mathrm{vect}(F_2)$.

We extend Definitions 3.3.2, 3.3.4, 3.3.6 and the definition of $\mathrm{Aoverlap}(F)$ from $\mathbb{N}^n$ to $(\mathbb{R}_0^+)^n$.

Definition 4.5.20. *For any $\tau \in (\mathbb{R}_0^+)^n$ and any $\xi, \xi' \in (\mathbb{R}_0^+)^n$, we define*

$$\tau + (\xi, \xi') := (\tau + \xi, \tau + \xi').$$

For any set H of proper binomials we define

$$(\mathbb{R}_0^+)^n + \mathrm{shifts}(H) := \{\tau + h \mid \tau \in (\mathbb{R}_0^+)^n \text{ and } h \in \mathrm{shifts}(H)\}.$$

Definition 4.5.21 (Vpc in $(\mathbb{R}_0^+)^n$)**.** *Let $A, B \in (\mathbb{R}_0^+)^n$, $A \neq B$. We call a finite sequence z of elements in $(\mathbb{R}_0^+)^n + \mathrm{shifts}(F)$ a* valid polygon chain (vpc) in $(\mathbb{R}_0^+)^n$ *(from A to B) if $z_{k,2} = z_{k+1,1}$ for all $k \in \mathbb{N}_{\mathrm{len}(z)-1}$ (and $z_{1,1} = A$ and $z_{\mathrm{len}(z),2} = B$).*

Definition 4.5.22 (Degree of a vpc in $(\mathbb{R}_0^+)^n$)**.** *The degree of an $A \in (\mathbb{R}_0^+)^n$ is the sum of its components, the degree of a $\xi = (\xi_1, \xi_2) \in (\mathbb{R}_0^+)^n \times (\mathbb{R}_0^+)^n$ is defined as* $\deg(\xi) := \max(\deg(\xi_1), \deg(\xi_2))$. *For a vpc z in $(\mathbb{R}_0^+)^n$,* $\deg(z) := \max(\{\deg(z_k) \mid k \in \mathbb{N}_{\mathrm{len}(z)}\})$.

Definition 4.5.23 ($\mathrm{Aoverlap}_{\mathbb{R}}(F)$)**.** *We define*

$$\mathrm{Aoverlap}_{\mathbb{R}}(F) := \{P \in (\mathbb{R}_0^+)^n \mid P \geq \mathrm{overlap}(F)\}.$$

Definition 4.5.24 ($\lfloor A \rfloor$). *For $A \in (\mathbb{R}_0^+)^n$ we define $(\lfloor A \rfloor)_i := \lfloor A_i \rfloor$ for all $i \in \mathbb{N}_n$.*

The following theorem gives sufficient conditions for the existence of a vpc inside of Aoverlap(F) together with an upper bound on its degree.

Theorem 4.5.25. *Let $A, B \geq \text{overlap}(F)$ and $k, k' \in \mathbb{N} \setminus \{0\}$ such that $A + k\,\text{vect}(F_1) - k'\,\text{vect}(F_2) = B$, $A + \text{vect}(F_1) + \text{vect}(F_2) \geq \text{overlap}(F)$ and $B + \text{vect}(F_1) + \text{vect}(F_2) \geq \text{overlap}(F)$. Let $A', B' \in \text{par}(A, B)$ such that $B' - A' = B - A$. Then there exists a vpc z in $(\mathbb{R}_0^+)^n$ from A' to B' such that $z_{i,2} \in \text{par}(A, B)$ for all $i \in \mathbb{N}_{\text{len}(z)}$ and hence $deg(z) \leq \text{maxdeg}(A, B) + \max(\deg(\text{vect}(F_1) + \text{vect}(F_2)), 0)$.*

Proof. Let z be defined as

$$z_j := \begin{cases} (A' - \text{e}(\text{tt}(F_1)) + \text{posshift}(F_1) & \text{if } j = 1 \text{ and } A' + \text{vect}(F_1) \in \text{par}(A, B) \\ (A' - \text{e}(\text{lt}(F_2)) + \text{negshift}(F_2) & \text{if } j = 1 \text{ and } A' + \text{vect}(F_1) \notin \text{par}(A, B) \\ (z_{j-1,2} - \text{e}(\text{tt}(F_1)) + \text{posshift}(F_1) & \text{if } 2 \leq j \leq k + k' \text{ and } \phi \\ (z_{j-1,2} - \text{e}(\text{lt}(F_2)) + \text{negshift}(F_2) & \text{if } 2 \leq j \leq k + k' \text{ and not } \phi, \end{cases}$$

where ϕ is the condition

$$z_{j-1,2} + \text{vect}(F_1) \in \text{par}(A, B) \text{ and}$$
$$z_{j-1,2} = A' + l\,\text{vect}(F_1) - l'\,\text{vect}(F_2) \text{ for some } l \in \mathbb{N}_{k-1} \cup \{0\}, l' \in \mathbb{N}_{k'} \cup \{0\}.$$

It is easy to see that $z_{i,2} = z_{i+1,1}$ for all $i \in \mathbb{N}_{\text{len}(z)-1}$. We show that for all $i \in \mathbb{N}_{\text{len}(z)}$ we have

$$z_{i,2} \in \text{par}(A, B)$$

and

$$z_{i,2} = A' + l\,\text{vect}(F_1) - l'\,\text{vect}(F_2)$$

for some $l \in \mathbb{N}_k \cup \{0\}$, $l' \in \mathbb{N}_{k'} \cup \{0\}$ by induction on i. Let $\lambda \in [0, 1]$ such that

$$A' = A + \lambda(\text{vect}(F_1) + \text{vect}(F_2)).$$

If $A' + \text{vect}(F_1) \in \text{par}(A, B)$, then $z_{1,2} = A' + \text{vect}(F_1) \in \text{par}(A, B)$ and $1 \in \mathbb{N}_k \cup \{0\}$ and $0 \in \mathbb{N}_{k'} \cup \{0\}$. If $A' + \text{vect}(F_1) \notin \text{par}(A, B)$, then

$$\begin{aligned} A' + \text{vect}(F_1) &= A' + \frac{1}{k + k'}(B - A) + \frac{k'}{k + k'}(\text{vect}(F_1) + \text{vect}(F_2)) \\ &= A + \frac{1}{k + k'}(B - A) + (\lambda + \frac{k'}{k + k'})(\text{vect}(F_1) + \text{vect}(F_2)), \end{aligned}$$

hence $\lambda + \frac{k'}{k+k'} \in (1, 2]$. So

$$A' - \text{vect}(F_2) = A' + \frac{1}{k + k'}(B - A) + \frac{-k}{k + k'}(\text{vect}(F_1) + \text{vect}(F_2))$$

$$= A + \frac{1}{k+k'}(B-A) + (\lambda + \frac{-k}{k+k'})(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)),$$

and $\lambda + \frac{-k}{k+k'} = \lambda + \frac{k'}{k+k'} - 1 \in (0,1]$. Hence $z_{1,2} = A' - \mathrm{vect}(F_2) \in \mathrm{par}(A,B)$ and $0 \in \mathbb{N}_k \cup \{0\}$ and $1 \in \mathbb{N}_{k'} \cup \{0\}$.
Let now i be such that $2 \leq i \leq k+k'$ and assume

$$z_{i-1,2} \in \mathrm{par}(A,B)$$

and

$$z_{i-1,2} = A' + l\,\mathrm{vect}(F_1) - l'\,\mathrm{vect}(F_2)$$

for some $l \in \mathbb{N}_k \cup \{0\}$, $l' \in \mathbb{N}_{k'} \cup \{0\}$. Let again $\lambda \in [0,1]$ such that

$$A' = A + \lambda(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)).$$

So we have

$$\begin{aligned} z_{i-1,2} &= A' + \mu(B-A) + \mu'(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \\ &= A + \zeta(B-A) + \zeta'(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)), \end{aligned}$$

where $\mu = \frac{l+l'}{k+k'}$, $\mu' = \frac{lk'-l'k}{k+k'}$, $\zeta = \mu \in [0,1]$ and $\zeta' = \lambda + \mu' \in [0,1]$. If the condition ϕ holds, then

$$z_{i,2} = z_{i-1,2} + \mathrm{vect}(F_1) \in \mathrm{par}(A,B)$$

and

$$z_{i,2} = A' + (l+1)\,\mathrm{vect}(F_1) - l'\,\mathrm{vect}(F_2)$$

where $l+1 \in \mathbb{N}_k$, $l' \in \mathbb{N}_{k'} \cup \{0\}$. If the condition ϕ does not hold, then either $z_{i-1,2} + \mathrm{vect}(F_1) \notin \mathrm{par}(A,B)$ or $l = k$. Suppose, $z_{i-1,2} + \mathrm{vect}(F_1) \notin \mathrm{par}(A,B)$. Note that $l + l' = i - 1 < k + k'$. Then

$$\begin{aligned} z_{i-1,2} + \mathrm{vect}(F_1) &= z_{i-1,2} + \frac{1}{k+k'}(B-A) + \frac{k'}{k+k'}(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \\ &= A + \left(\zeta + \frac{1}{k+k'}\right)(B-A) + \left(\zeta' + \frac{k'}{k+k'}\right)(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \end{aligned}$$

with $\zeta + \frac{1}{k+k'} = \frac{l+l'+1}{k+k'} \in [0,1]$ and $\zeta' + \frac{k'}{k+k'} \in (1,2]$. So

$$\begin{aligned} z_{i-1,2} - \mathrm{vect}(F_2) &= z_{i-1,2} + \frac{1}{k+k'}(B-A) + \frac{-k}{k+k'}(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \\ &= A + \left(\zeta + \frac{1}{k+k'}\right)(B-A) + \left(\zeta' + \frac{-k}{k+k'}\right)(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \end{aligned}$$

with $\zeta + \frac{1}{k+k'} = \frac{l+l'+1}{k+k'} \in [0,1]$ and $\zeta' + \frac{-k}{k+k'} = \zeta' + \frac{k'}{k+k'} - 1 \in (0,1]$. Hence

$$z_{i,2} = z_{i-1,2} - \mathrm{vect}(F_2) \in \mathrm{par}(A,B)$$

and

$$z_{i,2} = A' + l\,\mathrm{vect}(F_1) - (l'+1)\,\mathrm{vect}(F_2),$$

where $l \in \mathbb{N}_k \cup \{0\}$. If $l'+1 \notin \mathbb{N}_{k'} \cup \{0\}$, then $l' = k'$ and $B' = z_{i-1,2} + (k-l)\,\mathrm{vect}(F_1)$. Since $z_{i-1,2} \in \mathrm{par}(A,B)$ and $B' \in \mathrm{par}(A,B)$, also $z_{i-1,2} + \mathrm{vect}(F_1) \in \mathrm{par}(A,B)$, which contradicts the assumption that $z_{i-1,2} + \mathrm{vect}(F_1) \notin \mathrm{par}(A,B)$. Hence, also $l'+1 \in \mathbb{N}_{k'} \cup \{0\}$.
Suppose now, $l = k$. Then $l' < k'$ and $B' = z_{i-1,2} - (k'-l')\,\mathrm{vect}(F_2)$. Since $z_{i-1,2} \in \mathrm{par}(A,B)$ and $B' \in \mathrm{par}(A,B)$, also

$$z_{i,2} = z_{i-1,2} - \mathrm{vect}(F_2) \in \mathrm{par}(A,B)$$

and

$$z_{i,2} = A' + l\,\mathrm{vect}(F_1) - (l'+1)\,\mathrm{vect}(F_2),$$

where $l \in \mathbb{N}_k \cup \{0\}$ and $l' \in \mathbb{N}_{k'} \cup \{0\}$. This proves that $z_{i,2} \in \mathrm{par}(A,B)$ for all $i \in \mathbb{N}_{\mathrm{len}(z)}$. And since $z_{\mathrm{len}(z),2} = A' + l\,\mathrm{vect}(F_1) - l'\,\mathrm{vect}(F_2)$ with $l \in \mathbb{N}_k \cup \{0\}$, $l' \in \mathbb{N}_{k'} \cup \{0\}$ and $k + k' = \mathrm{len}(z) = l + l'$, it follows that $l = k$ and $l' = k'$ and hence, $z_{len(z),2} = B'$.
Note that $\mathrm{par}(A,B) \subseteq \mathrm{Aoverlap}_{\mathbb{R}}(F)$. Therefore by Lemma 3.3.21, which can be trivially extended to the case $(\mathbb{R}_0^+)^n$, z is a vpc in $(\mathbb{R}_0^+)^n$. Finally,

$$\begin{aligned}\deg(z) &\leq \mathrm{maxdeg}(\mathrm{par}(A,B)) \\ &= \mathrm{maxdeg}(A,B) + \max(\deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)), 0).\end{aligned}$$

□

Theorem 4.5.26 gives an upper bound on the degree of a vpc connecting points $P', Q' \in \mathbb{N}_n$ that lie in a certain area inside of $\mathrm{Aoverlap}(F)$, fulfill $P' - Q' = V(F)_{i,2}$, where $V(F)$ is the output of Algorithm 4.1.5 and $i \in \mathbb{N}_{\mathrm{len}(V(F))}$, and are minimal w.r.t. $\leq$ among all points satisfying the above conditions. This theorem is needed for the proof of Theorem 4.5.27.

Theorem 4.5.26. *Let $V(F)$ be the output of Algorithm 4.1.5, $T \in \mathbb{N}^n$ such that $T \geq \mathrm{overlap}(F)$, and*

$$T' := \gcd(T + (\mathrm{vect}(F_1) + \mathrm{vect}(F_2)),\, \mathrm{overlap}(F)) - (\mathrm{vect}(F_1) + \mathrm{vect}(F_2)).$$

Let $i \in \mathrm{len}(V(F))$ and $P \in \mathbb{N}^n$, $P \geq T$, with $P + V(F)_{i,2} \geq T$ such that there exists a vpc from P to $P + V(F)_{i,2}$. Then there is a $P' \in \mathbb{N}^n$, $P' \geq T$, with $P' + V(F)_{i,2} \geq T$ and $P' \leq P$ such that there exists a vpc z from P' to $P' + V(F)_{i,2}$ with

$$\begin{aligned}\deg(z) \leq\, &\mathrm{maxdeg}(T' + (V(F)_{i,2})^-, T' + (V(F)_{i,2})^+) \\ &+ \max(0, \deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))).\end{aligned}$$

Proof. We write V for $V(F)$. Note that T' is minimal w.r.t. $\leq$ such that $T' \geq T$ and $T' + (\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \geq \mathrm{overlap}(F)$. Let $A := T' + (V_{i,2})^-$ and $B := T' + (V_{i,2})^+$. Note that $\mathrm{par}(A, B) \subseteq \mathrm{Aoverlap}_{\mathbb{R}}(F)$ and

$$\begin{aligned}\mathrm{maxdeg}(\mathrm{par}(A, B)) = &\mathrm{maxdeg}(T' + (V_{i,2})^-, T' + (V_{i,2})^+) \\ &+ \max(0, \deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))).\end{aligned}$$

First suppose, $\mathrm{vect}(F_1) + \mathrm{vect}(F_2) \geq 0$. Then $T' = T$. Let $P' := A$. Note that $P' + V_{i,2} = B$ and $P' \leq P$, so it suffices to show that there exists a vpc z from P' to $P' + V_{i,2}$ with $\deg(z) \leq \mathrm{maxdeg}(\mathrm{par}(A, B))$. This follows from Theorem 4.5.25.

Now suppose, $\mathrm{vect}(F_1) + \mathrm{vect}(F_2) \not\geq 0$. Then $T' \geq T$, but not necessarily $T' = T$. We can assume that

$$P = T + (V_{i,2})^- + \lambda(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))^- + \mu(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)),$$

where $\lambda \in \mathbb{R}_0^+$ and $\mu \in [0, \lambda]$, otherwise there would exist a $P'' \leq P$ of this form with $P'' \geq T$ and $P'' + V_{i,2} \geq T$. There exists a $\lambda' \in [0, 1]$ such that

$$T' + (V_{i,2})^- = T + (V_{i,2})^- + \lambda'(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))^-.$$

If $\lambda = \lambda'$, then let the claim follows with Theorem 4.5.25. If $\lambda > \lambda'$, then

$$\begin{aligned}P'' &:= T + (V_{i,2})^- + \lambda'(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))^- + \frac{\mu\,\lambda'}{\lambda}(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \\ &= P - ((\lambda - \lambda')(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))^- + (\mu - \frac{\mu\,\lambda'}{\lambda})(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))) \\ &\leq P.\end{aligned}$$

Since P'', $P'' + V_{i,2} \in \mathrm{par}(A, B)$, by Theorem 4.5.25 there exists a vpc z' from P'' to $P'' + V_{i,2}$ with

$$\deg(z') \leq \mathrm{maxdeg}(\mathrm{par}(A, B)).$$

Let $P' := \lfloor P'' \rfloor$ and $\tau := P'' - P' \geq 0$. Then $z := -\tau + z'$ is a vpc from P' to $P' + V_{i,2}$ with

$$\deg(z) = \deg(-\tau) + \deg(z') \leq \mathrm{maxdeg}(\mathrm{par}(A, B)).$$

If $\lambda < \lambda'$, then let z be a minimal vpc from P to $P + V_{i,2}$. Assume that $\deg(z) > \mathrm{maxdeg}(\mathrm{par}(A, B))$. We distinguish two cases: $\deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \geq 0$ and $\deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) < 0$. If $\deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \geq 0$, let

$$A' := T + (V_{i,2})^- + \lambda(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))^-$$

and

$$B' = A' + V_{i,2}$$

and consider $\mathrm{par}(A', B')$. We have P, $P + V_{i,2} \in \mathrm{par}(A', B')$. Note that

$$\mathrm{par}(A', B') + (\lambda' - \lambda)(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))^- = \mathrm{par}(A, B),$$

hence

$$\mathrm{maxdeg}(\mathrm{par}(A', B')) < \mathrm{maxdeg}(\mathrm{par}(A, B)).$$

If $\deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) = 0$, then

$$\begin{aligned} \deg(z) &= \mathrm{maxdeg}(P, P + V_{i,2})) \\ &= \mathrm{maxdeg}(\mathrm{par}(A', B')) \\ &< \mathrm{maxdeg}(\mathrm{par}(A, B)), \end{aligned}$$

which contradicts the assumption that $\deg(z) > \mathrm{maxdeg}(\mathrm{par}(A, B))$. So assume now that $\deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) > 0$. Since $\deg(z) > \mathrm{maxdeg}(\mathrm{par}(A, B))$, there exists an $r \in \mathbb{N}_{\mathrm{len}(z)}$ such that

$$\deg(z_{r,2}) = \deg(z).$$

This means that $z_{r,2} \notin \mathrm{par}(A', B')$ and

$$z_{r,2} - m(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \in \mathrm{par}(A', B')$$

for some $m \in \mathbb{N} \setminus \{0\}$. Note that $z_{r,2} \geq \mathrm{overlap}(F)$ and that $z_{r,2}$ is a peak. Like in the proof of Theorem 3.3.26 we can construct a vpc z' that differs from z only in that z' goes through $z_{r,2} - (\mathrm{vect}(F_1) + \mathrm{vect}(F_2))$ instead of $z_{r,2}$. If there is another $r' \in \mathbb{N}_{\mathrm{len}(z')}$ such that $\deg(z'_{r',2}) = \deg(z)$, we repeat the process. This can only happen a finite number of times and the resulting vpc z'' goes from P to $P + V_{i,2}$ and has degree $\deg(z'') < \deg(z)$. This contradicts the minimality of z.
The case $\deg(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) < 0$ works analogously to this, but with

$$A' := T + (V_{i,2})^- + (\lambda' - \lambda)(\mathrm{vect}(F_1) + \mathrm{vect}(F_2))^-$$

and $m \in \mathbb{N} \setminus \{0\}$ such that

$$z_{r,2} + m(\mathrm{vect}(F_1) + \mathrm{vect}(F_2)) \in \mathrm{par}(A', B').$$

□

We now state the second main theorem in this subsection. It says that there exists a Gröbner basis G of F such that every $g \in G$ with $\mathrm{supp}(g) \subseteq [X]\,\mathrm{supp}(f)$ for some $f \in F$ can be generated by shifts with degree at most the bound given in (4.14).

Theorem 4.5.27. *Let $V(F)$ be the output of Algorithm 4.1.5 and $f \in F$. There is a Gröbner basis G of F such that for every $g \in G$ with $\mathrm{supp}(g) \subseteq [X]\,\mathrm{supp}(f)$ there exists a vpc z from $\mathrm{e}(\mathrm{tt}(g))$ to $\mathrm{e}(\mathrm{lt}(g))$ with*

$$\begin{aligned}\deg(z) \leq\, & \operatorname{maxdeg}(T',\, T' + \operatorname{vect}(F_1) + \operatorname{vect}(F_2)) \\ & + \max(\{\operatorname{maxdeg}((V(F)_{i,2})^-, (V(F)_{i,2})^+) \mid i \in \mathbb{N}_{\operatorname{len}(V(F))}\}) \\ & + \max(0,\, \operatorname{step}(\operatorname{e}(\operatorname{tt}(f)))\deg(-\operatorname{vect}(f))),\end{aligned} \tag{4.14}$$

where

$$T' = \gcd(T + \operatorname{vect}(F_1) + \operatorname{vect}(F_2),\, \operatorname{overlap}(F)) - (\operatorname{vect}(F_1) + \operatorname{vect}(F_2))$$

and

$$T = \gcd(\operatorname{e}(\operatorname{tt}(f)) + \operatorname{step}(\operatorname{e}(\operatorname{tt}(f)))\operatorname{vect}(f),\, \operatorname{overlap}(F)).$$

Proof. We write V for $V(F)$. From Theorem 4.5.18 follows that we need only consider the cases where $\operatorname{e}(\operatorname{lt}(g)) \geq \operatorname{e}(\operatorname{tt}(f))$ and $\operatorname{e}(\operatorname{lt}(g)) - \operatorname{e}(\operatorname{tt}(g)) = V_{i,2}$ for an $i \in \mathbb{N}_{\operatorname{len}(V)}$. So let $i \in \mathbb{N}_{\operatorname{len}(V)}$ and let $A \in \mathbb{N}^n$ such that $A \geq \operatorname{e}(\operatorname{tt}(f))$, $A - V_{i,2} \in \mathbb{N}^n + \operatorname{e}(\operatorname{supp}(f))$ and such that there exists a vpc from A to $A - V_{i,2}$. First consider the case that $A - V_{i,2} \geq \operatorname{e}(\operatorname{tt}(f))$. Suppose, $\operatorname{step}(A) = \operatorname{step}(A - V_{i,2})$. Let $P := \operatorname{overlapshift}(A)$. Then $P = A + \operatorname{step}(A)\operatorname{vect}(f) \geq T''$ and

$$P - V_{i,2} = \operatorname{overlapshift}(A - V_{i,2}) = A - V_{i,2} + \operatorname{step}(A)\operatorname{vect}(f) \geq T'',$$

where

$$T'' := \gcd(\operatorname{e}(\operatorname{tt}(f)) + \operatorname{step}(A)\operatorname{vect}(f),\, \operatorname{overlap}(F)).$$

Let

$$T''' := \gcd(T'' + \operatorname{vect}(F_1) + \operatorname{vect}(F_2),\, \operatorname{overlap}(F)).$$

With Theorem 4.5.26 follows that there exists a $P' \geq T''$ with $P' - V_{i,2} \geq T''$ and $P' \leq P$ such that there exists a vpc z' from P' to $P' - V_{i,2}$ with

$$\begin{aligned}\deg(z') \leq\, & \operatorname{maxdeg}(T''' + (V_{i,2})^-, T''' + (V_{i,2})^+) \\ & + \max(0, \deg(\operatorname{vect}(F_1) + \operatorname{vect}(F_2))).\end{aligned}$$

Because of Lemma 4.3.1 we have $T''' \leq T'$ and hence

$$\begin{aligned}\deg(z') \leq\, & \operatorname{maxdeg}(T' + (V_{i,2})^-, T' + (V_{i,2})^+) \\ & + \max(0, \deg(\operatorname{vect}(F_1) + \operatorname{vect}(F_2))).\end{aligned}$$

Let $A' := P' - \operatorname{step}(A)\operatorname{vect}(f)$. Then z defined as

$$z_j := \begin{cases} (A' - \operatorname{e}(\operatorname{tt}(f)) + \operatorname{posshift}(f) & \text{if } j = 1 \\ (z_{j-1,2} - \operatorname{e}(\operatorname{tt}(f)) + \operatorname{posshift}(f) & \text{if } j \in \mathbb{N}_{\operatorname{step}(A)} \setminus \{1\} \\ z'_{j-\operatorname{step}(A)} & \text{if } j \in \mathbb{N}_{\operatorname{step}(A)+\operatorname{len}(z')} \setminus \mathbb{N}_{\operatorname{step}(A)} \\ (z_{j-1,2} - \operatorname{e}(\operatorname{lt}(f)) + \operatorname{negshift}(f) & \text{if } j \in \mathbb{N}_{2\operatorname{step}(A)+\operatorname{len}(z')} \setminus \mathbb{N}_{\operatorname{step}(A)+\operatorname{len}(z')} \end{cases}$$

is a vpc from A' to $A' - V_{i,2}$ with an upper bound for $\deg(z)$ as in the theorem. Suppose now, $\operatorname{step}(A) \neq \operatorname{step}(A - V_{i,2})$. Let w.l.o.g. $\operatorname{step}(A) > \operatorname{step}(A - V_{i,2})$ and

$$T'' := \gcd(\mathrm{e}(\mathrm{tt}(f)) + \operatorname{step}(A)\operatorname{vect}(f), \operatorname{overlap}(F))$$

and

$$T''' := \gcd(T'' + \operatorname{vect}(F_1) + \operatorname{vect}(F_2), \operatorname{overlap}(F)).$$

Note that $A \geq T''$. Let $P := \operatorname{overlapshift}(A)$. If

$$P - V_{i,2} + (\operatorname{step}(A) - \operatorname{step}(A - V_{i,2}))\operatorname{vect}(f) \geq T'',$$

then we proceed like before. If

$$P - V_{i,2} + (\operatorname{step}(A) - \operatorname{step}(A - V_{i,2}))\operatorname{vect}(f) \not\geq T'',$$

then let z be a minimal vpc from A to $A - V_{i,2}$. Consider the vpc z' defined by

$$z'_j := z_{j+\operatorname{step}(A)}$$

for $j \in \mathbb{N}_{\operatorname{len}(z)-\operatorname{step}(A)}$. Analogously to the case $\lambda < \lambda'$ in the proof of Theorem 4.5.26 we can show that

$$\begin{aligned}\deg(z') \leq\, &\operatorname{maxdeg}(T''' + (V_{i,2})^-, T''' + (V_{i,2})^+) \\ &+ \max(0, \deg(\operatorname{vect}(F_1) + \operatorname{vect}(F_2))),\end{aligned}$$

and like before,

$$\begin{aligned}\deg(z') \leq\, &\operatorname{maxdeg}(T' + (V_{i,2})^-, T' + (V_{i,2})^+) \\ &+ \max(0, \deg(\operatorname{vect}(F_1) + \operatorname{vect}(F_2))).\end{aligned}$$

We obtain that $\deg(z)$ is not bigger than the bound given in the theorem. This concludes the case that $A - V_{i,2} \geq \mathrm{e}(\mathrm{tt}(f))$. Now suppose that $A - V_{i,2} \not\geq \mathrm{e}(\mathrm{tt}(f))$. Then $A - V_{i,2} \geq \mathrm{e}(\mathrm{lt}(f))$ and $A - V_{i,2} \geq \operatorname{overlap}(F)$. This case works analogously to the first case with 0 instead of $\operatorname{step}(A - V_{i,2})$. □

4.5.2 Degree Bound on the Shifts if the Trailing Term of One Input Polynomial Has Step 0

We use the results from Subsection 4.5.1 to give a degree bound on the cofactors for a Gröbner basis in the case where the trailing term of one of the input binomials has step 0. This includes the case where F is saturated, i.e. where $\gcd(\mathrm{lt}(F_i), \mathrm{tt}(F_i)) = 1$ for every $i = 1, 2$.

The following two theorems are adaptations of Theorems 4.5.4 and 4.5.18 for the case where A and B are multiples of the trailing terms of different input polynomials and where $A \in \text{Aoverlap}(F)$ or $B \in \text{Aoverlap}(F)$.

Theorem 4.5.28. *Let $f, f' \in F$, $f \neq f'$, and let $A, B \in \mathbb{N}^n$, $A \neq B$, with $A \geq \text{e}(\text{tt}(f))$, $B \geq \text{e}(\text{tt}(f'))$, $A, B \not\geq \text{e}(\text{lt}(h))$ for any $h \in F$, and $A \geq \text{overlap}(F)$ or $B \geq \text{overlap}(F)$, such that there is a vpc from A to B. Also, let $k, k' \in \mathbb{N} \setminus \{0\}$ such that $A + k\,\text{vect}(f) - k'\,\text{vect}(f') = B$, and $l \in \mathbb{N}_k$, $l' \in \mathbb{N}_{k'}$ such that $\frac{l'}{l} \geq \frac{k'}{k}$ and*

$$\begin{cases} \frac{l'}{l+1} \leq \frac{k'}{k} & \text{if } k > k' \\ \frac{l'-1}{l} \leq \frac{k'}{k} & \text{if } k \leq k'. \end{cases}$$

Furthermore, let $v := l\,\text{vect}(f) - l'\,\text{vect}(f')$. Then there exists a vpc from $B - v$ to B and either $B - v \in \text{Aoverlap}(F)$ or

$$B - v \geq \begin{cases} \text{e}(\text{tt}(f)) & \text{if } B \geq \text{overlap}(F) \\ \text{e}(\text{tt}(f')) & \text{if } A \geq \text{overlap}(F). \end{cases}$$

Proof. Assume that $B \geq \text{overlap}(F)$. The other case proceeds analogously. Let z be a vpc of minimal length from A to B. It consists of exactly k positive shifts of f and exactly k' negative shifts of f', z_1 being a shift of f and $z_{\text{len}(z)}$ one of f'. If there is an $r \in \mathbb{N}_{\text{len}(z)}$ such that $z_{r,2} = B - v$, then $B - v \in \text{Aoverlap}(F)$ and z' defined by

$$z'_j := z_{j+r}$$

for $j \in \mathbb{N}_{\text{len}(z)-r}$ is a vpc from $B - v$ to B.
Now assume that z does not go through $B - v$. Let $r \in \mathbb{N}_{\text{len}(z)}$ such that z_r is the $(k' - l' + 1)$-th shift of f' in z. There exists an $m \in \mathbb{Z} \setminus \{0\}$ such that $z_{r,1} - m\,\text{vect}(f) = B - v$. First assume, $m > 0$. We show $B - v \geq \text{e}(\text{tt}(f))$. For

$$P := (1 - \frac{k' - l'}{k'})A + \frac{k' - l'}{k'}B \in \text{conn}(A, B) \tag{4.15}$$

we get

$$B - v = (1 - \mu)z_{r,1} + \mu P,$$

where $\mu = \frac{1}{m + \frac{kl' - k'l}{k'}}$. Since $\frac{l'}{l} \geq \frac{k'}{k}$, we obtain $kl' - k'l \geq 0$, which together with $m > 0$ yields $\mu \in [0, 1]$, hence

$$B - v \in \text{conn}(z_{r,1},\, P). \tag{4.16}$$

Let now $i \in \mathbb{N}_n$. We show $(B - v)_i \geq \text{e}(\text{tt}(f))_i$. If $\text{vect}(f)_i \leq 0$, then

$$\text{e}(\text{lt}(f))_i \leq \text{overlap}(F)_i \leq z_{r,1,i}$$

and so

$$\begin{aligned}(B-v)_i &= z_{r,1,i} - m\,\mathrm{vect}(f)_i \\ &= z_{r,1,i} - \mathrm{vect}(f)_i - (m-1)\,\mathrm{vect}(f)_i \\ &\geq \mathrm{e}(\mathrm{tt}(f))_i - (m-1)\,\mathrm{vect}(f)_i \\ &\geq \mathrm{e}(\mathrm{tt}(f))_i.\end{aligned}$$

If $\mathrm{vect}(f)_i > 0$, then

$$\mathrm{e}(\mathrm{tt}(f))_i \leq \mathrm{overlap}(F)_i \leq z_{r,1,i}. \tag{4.17}$$

With $\mathrm{overlap}(F)_i \leq B_i$, it follows from this that $\mathrm{e}(\mathrm{tt}(f))_i \leq B_i$. Because of (4.15), either $A_i \leq P_i \leq B_i$ or $B_i \leq P_i \leq A_i$, so $\mathrm{e}(\mathrm{tt}(f))_i \leq P_i$. Because of (4.16) we have $P_i \leq (B-v)_i \leq z_{r,1,i}$, so together with (4.17) we get $\mathrm{e}(\mathrm{tt}(f))_i \leq (B-v)_i$. We conclude, $B - v \geq \mathrm{e}(\mathrm{tt}(f))$. So together with Lemma 3.3.21, we obtain that z' defined by

$$z'_j := \begin{cases} (B - v - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f) & \text{if } j = 1 \\ (z'_{j-1,2} - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f) & \text{if } 2 \leq j \leq m \\ z_{r+j-m-1} & \text{if } m+1 \leq j \leq m + \mathrm{len}(z) - (r-1), \end{cases}$$

is a vpc from $B - v$ to B.

Now assume, $m < 0$. We show $B - v \geq \mathrm{overlap}(F)$. Let $i \in \mathbb{N}_n$. If $\mathrm{vect}(f)_i \geq 0$, then

$$\begin{aligned}(B-v)_i &= z_{r,1,i} - m\,\mathrm{vect}(f)_i \\ &\geq z_{r,1,i} \\ &\geq \mathrm{overlap}(F)_i.\end{aligned}$$

Now assume, $\mathrm{vect}(f)_i < 0$. If $k = 1$, then also $l = 1$, and since $\frac{l'}{l} \geq \frac{k'}{k}$, we have $l' = k'$. So in this case, $B - v = A$, which contradicts the assumption, that z does not go through $B - v$. So in fact, we have $k > 1$. One can show that from the conditions on l and l', it follows that $\frac{l'-1}{l} \leq \frac{k'-1}{k-1}$, and hence, that $B - v$ lies in the quadrangle defined by the points A, $A + \mathrm{vect}(f)$, $B + \mathrm{vect}(f')$ and B, all four of them lying in the same plane. Since $A + \mathrm{vect}(f)$, $B + \mathrm{vect}(f')$ and B are all in $\mathrm{Aoverlap}(F)$, we know

$$(A + \mathrm{vect}(f))_i \geq \mathrm{overlap}(F)_i,$$

$$(B + \mathrm{vect}(f'))_i \geq \mathrm{overlap}(F)_i$$

and

$$B_i \geq \mathrm{overlap}(F)_i.$$

Since $\mathrm{vect}(f)_i < 0$, we also get

$$A_i = (A + \mathrm{vect}(f))_i) - \mathrm{vect}(f))_i \geq \mathrm{overlap}(F)_i.$$

Therefore, $(B-v)_i \geq \text{overlap}(F)_i$. We conclude, $B-v \geq \text{overlap}(F)$. By Lemma 3.3.21 we obtain that z' defined by

$$z'_j := \begin{cases} (B - v - \text{e}(\text{lt}(f)) + \text{negshift}(f) & \text{if } j = 1 \\ (z'_{j-1,2} - \text{e}(\text{lt}(f)) + \text{negshift}(f) & \text{if } 2 \leq j \leq m \\ z_{r+j-m-1} & \text{if } m+1 \leq j \leq m + \text{len}(z) - (r-1) \end{cases}$$

is a vpc from $B - v$ to B. □

Theorem 4.5.29. *Let $V(F)$ be the output of Algorithm 4.1.5, $f, f' \in F$, $f \neq f'$, and let $A, B \in \mathbb{N}^n$, $A \neq B$, with $A \geq \text{e}(\text{tt}(f))$, $B \geq \text{e}(\text{tt}(f'))$, $A, B \not\geq \text{e}(\text{lt}(h))$ for any $h \in F$, $B - A \in \Omega_{\prec}$, and $A \geq \text{overlap}(F)$ or $B \geq \text{overlap}(F)$, such that there exists a vpc from A to B. Then there exists an $i \in \mathbb{N}_{\text{len}(V(F))}$ such that there is a vpc from $B - V(F)_{i,2}$ to B.*

Proof. The proof of the theorem is mostly the same as the proof for Theorem 4.5.18, except that we use Theorem 4.5.28 instead of Theorem 4.5.4. Let $V'(F)$ be the output of Procedure 4.5.9. We again write V and V' for $V(F)$ and $V'(F)$, respectively. As in the proof of Theorem 4.5.18, let w.l.o.g. $k \in \mathbb{N} \setminus \{0\}$, $k' \in \mathbb{Z} \setminus \mathbb{N}$ such that

$$A + k\,\text{vect}(f) + k'\,\text{vect}(f') = B$$

and let $i' \in \mathbb{N} \setminus \{0\}$ be minimal such that $0 < V'_{i',1,1} \leq k$, $-V'_{i',1,2} \leq -k'$ and

$$\frac{-V'_{i',1,2}}{V'_{i',1,1}} \geq \frac{-k'}{k}.$$

The only changes that we have to make are the cases $i' = 3$ and $-V'_{i',1,2} = 1$ for the proof that there exists a vpc from $B - V'_{i',2}$ to B, and the proof that there exists a vpc from $B - V_{i,2}$ to B for an $i \in \mathbb{N}_{\text{len}(z)}$.

Let z be a vpc of minimal length from A to B. Like in Theorem 4.5.28 it consists of exactly k positive shifts of f and exactly $-k'$ negative shifts of f', z_1 being a shift of f and $z_{\text{len}(z)}$ one of f'. If $i' = 3$, then it follows from $\frac{1}{1} = \frac{-V'_{i',1,2}}{V'_{i',1,1}} \geq \frac{-k'}{k}$ that $-k' \leq k$. We do not necessarily have $\frac{1}{2} \leq \frac{-k'}{k}$, so we can only use Theorem 4.5.28 if we prove that this condition is not needed. The last shift of f' in z is $z_{\text{len}(z)}$. We have $B - V'_{i',2} = z_{\text{len}(z)} - m\,\text{vect}(f)$ with $m = 1$. In the proof of Theorem 4.5.28 the condition in question was only needed for the case $m < 0$. So in fact we can apply Theorem 4.5.28 also here. So there exists a vpc from $B - V'_{i',2}$ to B.
If $-V'_{i',1,2} = 1$, then from $\frac{1}{V'_{i',1,1}} \geq \frac{-k'}{k}$ it follows again that $-k' \leq k$. We have $B - V'_{i',2} = z_{\text{len}(z)} - m\,\text{vect}(f)$ with $m = V'_{i',1,1} > 0$. So like above, the condition $\frac{1}{V'_{i',1,1}+1} \leq \frac{-k'}{k}$ is not needed and we can apply Theorem 4.5.28 to get a vpc from $B - V'_{i',2}$ to B.

Now we prove the existence of a vpc from $B-V_{i,2}$ to B for an $i \in \mathbb{N}_{\mathrm{len}(V)}$. If $i' \leq \mathrm{len}(V)$, this follows with $i := i'$. So now assume $i' > \mathrm{len}(V)$. Let $i \in \mathbb{N}_{\mathrm{len}(V)}$ be maximal such that $V_{i,1,1} > 0$. Let z be a vpc of minimal length from $B - V'_{i',2}$ to B. It consists of exactly $V'_{i',1,1}$ positive shifts of f and exactly $-V'_{i',1,2}$ negative shifts of f'. Note that $V_{i,1,1} \in \mathbb{N}_{V'_{i',1,1}}$ and $-V_{i,1,2} \in \mathbb{N}_{-V'_{i',1,2}} \cup \{0\}$. Since also

$$\frac{-V_{i,1,2}}{V_{i,1,1}} < \frac{-V'_{i',1,2}}{V'_{i',1,1}}$$

we conclude that in fact $V_{i,1,2} \neq V'_{i',1,2}$. We assume that z does not already go through $B - V_{i,2}$. By Theorem 4.5.28, $B - V'_{i',2} \geq \mathrm{overlap}(F)$ or $B - V'_{i',2} \geq \mathrm{e}(\mathrm{tt}(f))$.
First assume $B - V'_{i',2} \geq \mathrm{overlap}(F)$. We show that $B - V_{i,2} \geq \mathrm{overlap}(F)$. Let $j \in \mathbb{N}_n$. If $V_{i,2,j} \leq 0$, then from $B_j \geq \mathrm{overlap}(F)_j$ follows $B_j - V_{i,2,j} \geq \mathrm{overlap}(F)_j$. If $V_{i,2,j} > 0$, then by Lemma 4.5.17 we get

$$V'_{i',2,j} - V_{i,2,j} \geq 0 \tag{4.18}$$

and so, since $B_j - V'_{i',2,j} \geq \mathrm{overlap}(F)_j$, also

$$B_j - V_{i,2,j} = B_j - V'_{i',2,j} + (V'_{i',2,j} - V_{i,2,j}) \geq \mathrm{overlap}(F)_j.$$

Let $r \in \mathbb{N}_{\mathrm{len}(z)}$ such that z_r is the $(k' - V_{i,2,j}) - th$ negative shift of f' in z. There exists an $m \in \mathbb{Z} \setminus \{0\}$ such that $z_{r,2} - m\,\mathrm{vect}(f) = B - V_{i,2}$. By Lemma 3.3.21 we obtain that, if $m > 0$, then z' defined by

$$z'_{j'} := \begin{cases} (B - V_{i,2} - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f) & \text{if } j' = 1 \\ (z'_{j'-1,2} - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f) & \text{if } 2 \leq j' \leq m \\ z_{r+j'-m} & \text{if } m+1 \leq j' \leq m + \mathrm{len}(z) - r \end{cases}$$

is a vpc from $B - V_{i,2}$ to B, and if $m < 0$, then z' defined by

$$z'_{j'} := \begin{cases} (B - V_{i,2} - \mathrm{e}(\mathrm{lt}(f)) + \mathrm{negshift}(f) & \text{if } j' = 1 \\ (z'_{j'-1,2} - \mathrm{e}(\mathrm{lt}(f)) + \mathrm{negshift}(f) & \text{if } 2 \leq j' \leq m \\ z_{r+j'-m} & \text{if } m+1 \leq j' \leq m + \mathrm{len}(z) - r \end{cases}$$

is a vpc from $B - V_{i,2}$ to B.
Now assume $B - V'_{i',2} \geq \mathrm{e}(\mathrm{tt}(f))$. Let $r \in \mathbb{N}_{\mathrm{len}(z)}$ such that z_r is the $(k' - V_{i,1,2}) - th$ negative shift of f' in z. There exists an $m \in \mathbb{Z}\setminus\{0\}$ such that $z_{r,2} - m\,\mathrm{vect}(f) = B - V_{i,2}$. Assume $m > 0$. We show $B - V_{i,2} \geq \mathrm{e}(\mathrm{tt}(f))$. Let $j \in \mathbb{N}_n$. If $\mathrm{vect}(f)_j \leq 0$, then

$$\mathrm{e}(\mathrm{lt}(f))_j \leq \mathrm{overlap}(F)_j \leq z_{r,2,j}$$

and so

$$\begin{aligned}(B - V_{i,2})_j &= z_{r,2,j} - m\,\mathrm{vect}(f)_j \\ &= z_{r,2,j} - \mathrm{vect}(f)_j - (m-1)\,\mathrm{vect}(f)_j \\ &\geq \mathrm{e}(\mathrm{tt}(f))_j - (m-1)\,\mathrm{vect}(f)_j \\ &\geq \mathrm{e}(\mathrm{tt}(f))_j.\end{aligned}$$

If $\mathrm{vect}(f)_j > 0$, then

$$\mathrm{e}(\mathrm{tt}(f))_j \leq \mathrm{overlap}(F)_j \leq B_j.$$

If here $V_{i,2,j} \leq 0$, then

$$B_j - V_{i,2,j} \geq \mathrm{e}(\mathrm{tt}(f))_j,$$

and if $V_{i,2,j} > 0$, then we obtain from Lemma 4.5.17 that $V'_{i',2,j} \geq V_{i,2,j}$, so with $(B - V'_{i',2})_j \geq \mathrm{e}(\mathrm{tt}(f))_j$ also

$$(B - V_{i,2})_j = B_j - V'_{i',2,j} + (V'_{i',2,j} - V_{i,2,j}) \geq \mathrm{e}(\mathrm{tt}(f))_j.$$

We conclude $B - V_{i,2} \geq \mathrm{e}(\mathrm{tt}(f))$. So z' defined by

$$z'_{j'} := \begin{cases} (B - V_{i,2} - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f) & \text{if } j' = 1 \\ (z'_{j'-1,2} - \mathrm{e}(\mathrm{tt}(f)) + \mathrm{posshift}(f) & \text{if } 2 \leq j' \leq m \\ z_{r+j'-m} & \text{if } m+1 \leq j' \leq m + \mathrm{len}(z) - r, \end{cases}$$

is a vpc from $B - V_{i,2}$ to B.
Now assume $m < 0$. We show $B - V_{i,2} \geq \mathrm{overlap}(F)$. Let $j \in \mathbb{N}_n$. If $\mathrm{vect}(f)_j \geq 0$, then

$$\begin{aligned}(B - V_{i,2})_j &= z_{r,2,j} - m\,\mathrm{vect}(f)_j \\ &\geq z_{r,2,j} \\ &\geq \mathrm{overlap}(F)_j.\end{aligned}$$

Assume now $\mathrm{vect}(f)_j < 0$. If here $V_{i,2,j} \leq 0$, then $B_j - V_{i,2,j} \geq \mathrm{overlap}(F)_j$. For the case $V_{i,2,j} > 0$ note that since there exists a vpc from $B - V'_{i',2}$ to B, we have $B - V'_{i',2} + \mathrm{step}(B - V'_{i',2})\,\mathrm{vect}(f) \geq \mathrm{overlap}(F)$, where $\mathrm{step}(B - V'_{i',2}) \in \mathbb{N}$. Since $\mathrm{vect}(f)_j < 0$, we get $(B - V'_{i',2})_j \geq \mathrm{overlap}(F)_j$. By Lemma 4.5.17 we get

$$V'_{i',2,j} - V_{i,2,j} \geq 0,$$

hence

$$B_j - V_{i,2,j} = (B_j - V'_{i',2,j}) + (V'_{i',2,j} - V_{i,2,j}) \geq \mathrm{overlap}(F)_j$$

and we conclude $B - V_{i,2} \geq \text{overlap}(F)$. So z' defined by

$$z'_{j'} := \begin{cases} (B - V_{i,2} - \text{e}(\text{lt}(f)) + \text{negshift}(f) & \text{if } j' = 1 \\ (z'_{j'-1,2} - \text{e}(\text{lt}(f)) + \text{negshift}(f) & \text{if } 2 \leq j' \leq m \\ z_{r+j'-m} & \text{if } m+1 \leq j' \leq m + \text{len}(z) - r \end{cases}$$

is a vpc from $B - V_{i,2}$ to B. □

The following theorem gives a solution for Problem 4.1.2 for the case where the trailing term of one of the input binomials has step 0.

Theorem 4.5.30. *Let $f, f' \in F$, $f \neq f'$, such that* $\text{step}(\text{e}(\text{tt}(f'))) = 0$. *Let $V(F)$ be the output of Algorithm 4.1.5 and*

$$T = \gcd(\text{e}(\text{tt}(f)) + \text{step}(\text{e}(\text{tt}(f)))\,\text{vect}(f), \text{overlap}(F))$$

and

$$T' = \gcd(T + \text{vect}(f) + \text{vect}(f'), \text{overlap}(F)) - (\text{vect}(f) + \text{vect}(f')).$$

Then

$$\begin{aligned} d = &\,\text{maxdeg}(T',\, T' + \text{vect}(f) + \text{vect}(f')) \\ &+ \max(\{\text{maxdeg}((V(F)_{i,2})^-, (V(F)_{i,2})^+) \mid i \in \mathbb{N}_{\text{len}(V(F))}\}) \\ &+ \max(0,\, \text{step}(\text{e}(\text{tt}(f)))\,\deg(-\text{vect}(f))) \end{aligned}$$

solves Problem 4.1.2.

Proof. We write V for $V(F)$. Recall that we only need to consider elements $h \in \text{ideal}(F)$ such that $t \in [X]\,\text{tt}(F)$ and $t \notin [X]\,\text{lt}(F)$ for any $t \in \text{supp}(h)$. Since $\text{step}(\text{e}(\text{tt}(f'))) = 0$, for any such h different from f' with $t \in [X]\{\text{tt}(f')\}$ for a $t \in \text{supp}(h)$, we have $\text{e}(t) \geq \text{overlap}(F)$. By Theorems 4.5.18 and 4.5.29 it follows that for each such h there exists a $g \in \text{ideal}(F)$ such that $\text{e}(\text{lt}(g)) - \text{e}(\text{tt}(g)) = V_{i,2}$ for an $i \in \mathbb{N}_{\text{len}(V)}$ and $\text{e}(\text{lt}(g)) = \text{e}(\text{lt}(h))$ and $\text{e}(\text{tt}(g)) \geq R$ for a $R \in \text{e}(\text{supp}(f)) \cup \text{Aoverlap}(F)$. The cases $\text{supp}(g) \subseteq \text{supp}(f)$ and $\text{supp}(g) \subseteq \text{supp}(f')$ follow from Theorem 4.5.27. The only case that remains is $\text{e}(t) \geq \text{e}(\text{tt}(f))$ and $\text{e}(t') \geq \text{lcm}(\text{e}(\text{tt}(f'), \text{overlap}(F)))$ for $t, t' \in \text{supp}(g)$, $t \neq t'$. So let $i \in \mathbb{N}_{\text{len}(V)}$ and let w.l.o.g. $P \in \mathbb{N}^n$, $P \geq \text{e}(\text{tt}(f))$ such that $P - V_{i,2} \geq \text{lcm}(\text{e}(\text{tt}(f'), \text{overlap}(F)))$ and such that there exists a vpc from P to $P - V_{i,2}$. If $P \in \text{Aoverlap}(F)$, then with Theorem 4.5.26 it follows that there exists a $P' \in \text{Aoverlap}(F)$ with $P' - V_{i,2} \in \text{Aoverlap}(F)$ and $P' \leq P$ such that there exists a vpc z' from P' to $P' - V_{i,2}$ with

$$\begin{aligned} \deg(z') \leq &\,\text{maxdeg}(T'' + (V_{i,2})^-, T'' + (V_{i,2})^+) \\ &+ \max(0, \deg(\text{vect}(f) + \text{vect}(f'))) \leq d, \end{aligned}$$

where $T'' := \text{overlap}(F) + (\text{vect}(f) + \text{vect}(f'))^- \leq T'$. If $P \notin \text{Aoverlap}(F)$, then the proof proceeds analogously to the case $\text{step}(A) \neq \text{step}(A - V_{i,2})$ in the proof of Theorem 4.5.27. □

Corollary 4.5.31. *Assume F is saturated. Let $V(F)$ be the output of Algorithm 4.1.5 and $T := (\text{vect}(F_1) + \text{vect}(F_2))^-$. Then*

$$\begin{aligned} d = &\,\text{maxdeg}(T,\, T + \text{vect}(F_1) + \text{vect}(F_2)) \\ &+ \max(\{\text{maxdeg}(((V(F)_i)_2)^-, ((V(F)_i)_2)^+) \mid i \in \mathbb{N}_{\text{len}(V(F))}\}) \end{aligned}$$

solves Problem 4.1.2.

4.5.3 Degree Bound on the Shifts if the Trailing Terms of Both Input Polynomials Have Step Greater than 0

The general case, where the trailing terms of both input binomials have step greater than 0 is intricate, because there may occur an element g in the reduced Gröbner basis where one term of g is a multiple of $\text{tt}(F_1)$ and the other term of g is a multiple of $\text{tt}(F_2)$. The structure of g depends highly on the positioning of the support of the input binomials in $\mathbb{N}^n$ with respect to each other. In our experiments we discovered that $\text{vect}(g)$ is a linear combination of the vectors given by the output of Algorithm 4.1.5. Unfortunately we cannot give a better bound for the Sylvester matrix for this case as of yet.

References

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases.* Amer Mathematical Society, 7 1994.

[2] M. Albrecht, C. Cid, J.C. Faugére, and L. Perret. On the Relation Between the MXL Family of Algorithms and Gröbner Bases Algorithms. *Journal of Symbolic Computation*, 47:926–941, 2012.

[3] A. Arri and J. Perry. The F5 Criterion Revised. *Journal of Symbolic Computation*, 46:1017–1029, 2011.

[4] G. Ars, J.C. Faugére, H. Imai, M. Kawazoe, and M. Sugita. Comparison Between XL and Gröbner Basis Algorithms. *Advances in Cryptology - ASIACRYPT'2004*, pages 338–353, 2004.

[5] Stephen Barnett. *Polynomials and Linear Control Systems.* Marcel Dekker, Inc., New York, NY, USA, 1983.

[6] A.M. Bigatti, R. Scala, and L. Robbiano. Computing Toric Ideals. *Journal of Symbolic Computation*, 27:351–365, 1999.

[7] W.S. Brown. The Subresultant PRS Algorithm. *ACM Trans. Math. Software*, 4:237–249, 1978.

[8] W.S. Brown and J.F. Traub. On Euclid's Alogrithm and the Theory of Subresultants. *J. ACM*, 18:505–514, 1971.

[9] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal).* PhD thesis, Mathematical Institute, University of Innsbruck, Austria, 1965. English Translation in Journal of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions. 41:475-511, 2006.

[10] B. Buchberger. Ein Algorithmisches Kriterium für die Lösbarkeit eines Algebraischen Gleichungssystems (An Algorithmic Criterion for the Solvability of Algebraic Systems of Equations). *Aequationes Mathematicae*, 3:374–383, 1970. English translation in B. Buchberger, F. Winkler: Gröbner Bases and Applications, Proc. of the International Conference "33 Years of Gröbner Bases", 1998, RISC, Austria, London Math. Society Lecture Note Series 251, Cambridge Univ. Press, pages 535–545, 1998.

[11] B. Buchberger. Some Properties of Gröbner Bases for Polynomial Ideals. *ACM SIGSAM Bull*, 10:19–24, 1976.

[12] B. Buchberger. A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases. *In Proceedings of EUROSAM'79*, pages 3–21, 1979.

[13] B. Buchberger. Gröbner bases, Gaussian Elimination and Euclidean algorithm. Invited colloquium talk at University of Grenoble, IMAG Institute, 1983.

[14] B. Buchberger. Miscellaneous Results on Gröbner Bases for Polynomial Ideals II. Technical Report 83/1, University of Delaware, Department of Computer and Information Sciences, 1983.

[15] B. Buchberger. Gröbner Bases and Determinant Polynomials. Talk at COCOA workshop, Genova, May 29–June 3, 1989.

[16] B. Buchberger et al. Computational Mathematics: Numerical Analysis and Symbolic Computation. *FWF-Doktoratskolleg (DK), Oct. 2008–Sept. 2011, Johannes Kepler University Linz*, 2007.

[17] J. Buchmann, D. Cabarcas, J. Ding, and M. Mohamed. Flexible Partial Enlargement to Accelerate Gröbner Bases Computation over F2. *AFRICACRYPT'2010*, pages 69–81, 2010.

[18] J. Buchmann, J. Ding, M.S.E. Mohamed, and W.S.A.E. Mohamed. MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis. *Symmetric Cryptography. In: Dagstuhl Seminar Proceedings 09031, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany*, 2009.

[19] G.E. Collins. Polynomial Remainder Sequences and Determinants. *Amer. Math. Monthly*, 73:708–712, 1966.

[20] G.E. Collins. Subresultants and Reduced Polynomial Remainder Sequences. *J. ACM*, 14:128–142, 1967.

[21] P. Conti and C. Traverso. Buchberger Algorithm and Integer Programming. In *Proceedings of the 9th International Symposium, on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, AAECC-9, pages 130–139, London, UK, UK, 1991. Springer-Verlag.

[22] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. *Eurocrypt'2000*, 1807:392–407, 2000.

[23] N. Courtois and J. Patarin. About the XL Algorithm over GF(2). *In: Topics in Cryptology - CT-RSA 2003*, pages 141–157, 2003.

[24] N. Courtois and J. Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. *In: Advances in Cryptology - ASIACRYPT 2002*, pages 267–287, 2002.

[25] D.A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, NY, 1998.

[26] D.A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3rd Edition*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[27] P. Diaconis and B. Sturmfels. Algebraic Algorithms for Sampling from Conditional Distributions. *The Annals of Statistics*, 26:363–397, 1998.

[28] T.W. Dubé. The Structure of Polynomial Ideals and Gröbner Bases. *SIAM Journal on Computing*, 19(4):750–773, 1990.

[29] C. Eder and J. Perry. F5C: A Variant of Faugére's F5 Algorithm with Reduced Gröbner Bases. *Journal of Symbolic Computation*, 45:1442–1458, 2010.

[30] D. Eisenbud and B. Sturmfels. Binomial Ideals. *Duke Math. J.*, 84:1–45, 1996.

[31] J.C. Faugére. A New Efficient Algorithm for Computing Gröbner Bases (F4). *Journal of Pure and Applied Algebra*, 139:61–88, 1999.

[32] J.C. Faugére. A New Efficient Algorithm for Computing Gröbner Bases Without Reductions to Zero (F5). *ISSAC'02*, pages 75–83, 2002.

[33] J.C. Faugére and S. Lachartre. Parallel Gaussian Elimination for Gröbner Bases Computations in Finite Fields. *PASCO'10*, pages 89–97, 2010.

[34] S. Gao, Y. Guan, and F. Volny. A New Incremental Algorithm for Computing Gröbner Bases. *ISSAC'10*, pages 13–19, 2010.

[35] S. Gao, F. Volny IV, and M. Wang. A New Algorithm for Computing Gröbner Bases. Cryptology ePrint Archive, Report 2010/641, 2010.

[36] D. Grigoriev and N. Vorobjov. Bounds on Numbers of Vectors of Multiplicities for Polynomials Which Are Easy to Compute. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, ISSAC '00, pages 137–146, New York, NY, USA, 2000. ACM.

[37] W. Habicht. Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens (English: A Generalization of Sturm's Root Counting Method). *Comm. Math. Helvetici*, 21:99–116, 1948.

[38] A. Hashemi and G. Ars. Extended F5 Criteria. *Journal of Symbolic Computation*, 45:1330–1340, 2010.

[39] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale (The Question of Finitely Many Steps in Polynomial Ideal Theory). *Mathematische Annalen*, 95:736–788, 1926. English translation in ACM SIGSAM Bull. 32(3), pages 8–30, 1998.

[40] S. Hosten and R. Thomas. Gröbner Bases and Integer Programming. In: B. Buchberger, F. Winkler: Gröbner Bases and Applications, Proc. of the International Conference "33 Years of Gröbner Bases", 1998, RISC, Austria, London Math. Society Lecture Note Series 251, Cambridge Univ. Press, pages 144–158, 1998.

[41] I. Hoveijn. *Aspects of Resonance in Dynamical Systems*. PhD thesis, University of Utrecht, Netherlands, 1992.

[42] D. Kesh. *Computations of Binomial Ideals*. PhD thesis, Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, February 2012.

[43] U. Koppenhagen and E.W. Mayr. Optimal Gröbner Base Algorithms for Binomial Ideals. Tech. Rep. TUM-I9604, Institut für Informatik, Technische Universität München, 1996.

[44] U. Koppenhagen and E.W. Mayr. An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals. *Journal of Symbolic Computation*, 28:317–338, 1999.

[45] K. Kühnle and E. W. Mayr. Exponential Space Computation of Gröbner Bases. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, ISSAC '96, pages 63–71, New York, NY, USA, 1996. ACM.

[46] M.A. Laidacker. Another Theorem Relating Sylvester's Matrix and the Greatest Common Divisor. *Math. Mag.*, 42:126–128, 1969.

[47] D. Lazard. Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations. *In Proceedings of EUROCAL*, pages 146–156, 1983.

[48] R. Loos. Generalized Polynomial Remainder Sequences. *Computer Algebra: Symbolic and Algebraic Computation*, pages 115–137, 1982.

[49] A. Mandache. The Gröbner Basis Algorithm and Subresultant Theory. *In Proceedings of ISSAC'94*, pages 123–128, 1994.

[50] A. Mandache. *Gröbner Bases Computation and Gaussian Elimination.* PhD thesis, RISC, Johannes Kepler University Linz, 1995.

[51] E.W. Mayr and A.R. Meyer. The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals. *Advances in Mathematics*, 46:305–329, 1982.

[52] M.S.E. Mohamed, D. Cabarcas, J. Buchmann, and S. Bulygin. MXL3: An Efficient Algorithm for Computing Gröbner Bases of Zero-Dimensional Ideals. *ICISC'2009*, pages 87–100, 2009.

[53] M.S.E. Mohamed, W.S.A.E. Mohamed, J. Ding, and J. Buchmann. MXL2: Solving Polynomial Equations Over GF(2) Using an Improved Mutant Strategy. *Post-Quantum Cryptography*, pages 203–215, 2008.

[54] S. Pan, Y. Hu, and B. Wang. The Termination of the F5 Algorithm Revisited. *ISSAC'13*, pages 291–298, 2013.

[55] S. Ritscher. *Degree Bounds and Complexity of Gröbner Bases of Important Classes of Polynomial Ideals.* PhD thesis, Chair for Efficient Algorithms, Technical University Munich, Germany, 2012.

[56] A. Schrijver. *Theory of Linear and Integer Programming.* John Wiley & Sons, Inc., New York, NY, USA, 1986.

[57] B. Sturmfels. Gröbner Bases of Toric Varieties. *Tohoku Math. J.*, 43:249–261, 1991.

[58] B. Sturmfels. Gröbner Bases and Convex Polytopes. *AMS, Providence RI*, 1996.

[59] B. Sturmfels, R. Weismantel, and G.M. Ziegler. Gröbner Bases of Lattices, Corner Polyhedra, and Integer Programming, 1995.

[60] Y. Sun and D.K. Wang. A New Proof for the Correctness of the F5 Algorithm. *Science China Mathematics*, 56:745–756, 2012.

[61] A. Suzuki. Computing Gröbner Bases within Linear Algebra. *CASC 2009*, pages 310–321, 2009.

[62] J.J. Sylvester. On a Theory of the Syzygetic Relations of Two Rational Integral Functions, Comprising an Application to the Theory of Sturm's Functions, and That of the Greatest Algebraical Common Measure. *Philosophical Trans.*, 143:407–548, 1853.

[63] R.R. Thomas. A Geometric Buchberger Algorithm for Integer Programming. *Mathematics of Operations Research*, 20:864–884, 1995.

[64] R.R. Thomas. Applications to Integer Programming. In *Proceedings of Symposia in Applied Mathematics*, pages 119–141, 1997.

[65] A.I.G. Vardulakis and P.N.R. Stoyle. Generalized Resultant Theorem. *IMA Journal of Applied Mathematics*, 22:331–335, 1978.

[66] J. von zur Gathen and T. Lücking. Subresultants Revisited. *Theoretical Computer Science*, 297:199–239, 2003.

[67] A.I. Zobnin. Generalization of the F5 Algorithm for Calculating Gröbner Bases for Polynomial Ideals. *Programming and Computer Software*, 36:75–82, 2010.

Curriculum Vitae

Personal data

Name: Manuela Wiesinger-Widi

e-mail: Manuela.Wiesinger@risc.jku.at

Date of birth: 20th of February, 1985 (Rohrbach, Upper Austria)

Citizenship: Austria

Affiliation

Research Institute for Symbolic Computation (RISC)
Johannes Kepler Universität Linz
Altenbergerstraße 69
A–4040 Linz, AUSTRIA

Education

2003: High school diploma (Matura), BORG Bad Leonfelden, Upper Austria.

2003–2007: Bachelor Studies in Technical Mathematics, Johannes Kepler University, Linz; degree: Bakkalaurea Technicae (with distinction; 06.03.2007). Advisor: Dr. Jürgen Ecker.

2007–2009: Master Studies in Computer Mathematics, Johannes Kepler University, Linz; degree: Diplom Ingenieurin (with distinction; 25.02.2009). Topic of the master thesis: "Contributions to MacMahon's Partition Analysis"; Advisor: Univ.-Prof. Dr. Peter Paule.

2009–2015: Ph.D. studies at the Research Institute for Symbolic Computation (RISC) via the Doktoratskolleg Computational Mathematics, Johannes Kepler University Linz.