



Gröbner Bases and Their Complexity

MASTER'S THESIS (online version)

in the field of Computer Science

submitted by

Leo Kayser

October 19, 2022

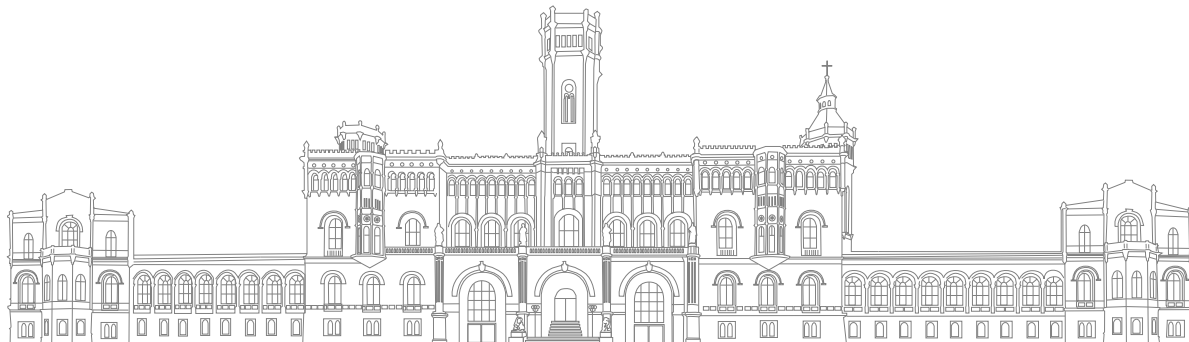
First examiner: Prof. Dr. Heribert Vollmer

Second examiner: PD Dr. Arne Meier

Advisor: Sabrina Gaube

Matriculation no.: 10006908

Institute of Theoretical Computer Science
Gottfried Wilhelm Leibniz Universität Hannover



This work is licensed under a [Creative Commons “Attribution-NonCommercial-ShareAlike 4.0 International”](https://creativecommons.org/licenses/by-nc-sa/4.0/) license.



Abstract

Polynomial equations and their solutions play a ubiquitous role both for theoretical and practical applications. A closely related problem is that of ideal membership, i. e. deciding whether a polynomial is a linear combination of other polynomials. Gröbner bases provide a well-developed machinery to deal with these problems symbolically as a part of computer algebra systems. In this thesis we give an introduction to the theory of Gröbner bases with a view towards computational complexity. In particular, we discuss algorithmic aspects and upper bounds depending on the classes of polynomials considered. Furthermore, lower bounds on the size and computational complexity of Gröbner bases and related problems are presented. While often useful in practice, the worst-case complexity of Gröbner bases is located in EXPSPACE.

Contents

Abstract	i
Introduction	1
Acknowledgment	2
1 Polynomial ideals and Gröbner bases	3
1.1 Motivating examples	3
1.2 The ideal membership problem	5
1.3 Polynomial division	8
1.4 The normal form algorithm and Gröbner bases	11
1.5 Reduced Gröbner bases and uniqueness	15
1.6 The case of binomial ideals	18
1.7 Representing polynomials	19
2 Algorithms and upper bounds	23
2.1 S-Polynomials	23
2.2 Buchberger's algorithm	26
2.3 Degree bounds	28
2.4 From polynomials to linear algebra	31
2.5 Fast linear algebra on PRAMs	34
2.6 Upper bounds on ideal membership	36
2.7 Computing a Gröbner basis in EXPSPACE	37
3 Lower bounds	41
3.1 Thue systems	42
3.2 Counter machines	46
3.3 Simulating counter machines with CSG	50
3.4 Producing words of double-exponential length	54
3.5 Hardness of the ideal membership problem	60
3.6 Church-Rosser systems	62
3.7 The size of a reduced Gröbner basis	64
3.8 Hardness results of Gröbner bases	67
Conclusion	70

A Appendix	73
A.1 Commutative Algebra	73
A.2 Commutative semigroups	74
Index	77
List of Symbols	79
List of Definitions and Theorems	81
List of Figures	83
Bibliography	85

Introduction

Whether a particular Gröbner basis computation is feasible is usually hard to predict in advance, so Gröbner basis computations are still an adventurous business.

GREGOR KEMPER [24, p. 127]

Many real-world problems can be modeled using systems of polynomial equations. While numerical algorithms can approximate real solutions with floating point arithmetic, some applications such as cryptography require exact manipulation or benefit from closed-form solutions. This motivates the study of symbolic algorithms to examine solvability and other properties of systems of polynomial equations. An important question which arises in this context is that of *ideal membership*: Given polynomials $f_1, \dots, f_B \in \mathbb{K}[x_1, \dots, x_n]$, decide whether a given polynomial f is a linear combination of the f_j :

$$f = \alpha_1 f_1 + \dots + \alpha_B f_B \quad \alpha_j \in \mathbb{K}.$$

The set of such f is called the ideal generated by the f_j . Hilbert's Nullstellensatz asserts that the system of equations $f_1 = \dots = f_B = 0$ has a solution $G \in \mathbb{K}^n$ if and only if $1 \in I$, thus the ideal membership problem "contains" consistency questions about polynomial equations.

In the case of polynomials in one variable $f \in \mathbb{K}[x]$, the familiar division algorithm can be used to determine a quotient q and remainder A such that

$$f = q \cdot g + A \quad \deg A < \deg g.$$

In particular $A = 0$ if and only if f is a multiple of g , so this solves the ideal membership problem. When generalizing this algorithm to several multivariate polynomials, problems of non-uniqueness of the remainder arise. This leads to the notion of a Gröbner basis, a special set of ideal generators which can be characterized as "behaving well" with respect to the division algorithm. A lot of problems about polynomials and ideals can be solved by first calculating a Gröbner basis, for example the aforementioned ideal membership problem.

In this thesis we will explore the computational complexity of ideal membership, Gröbner bases and related problems. The three chapters each deal with mathematical foundations, algorithmic upper bounds and lower bounds respectively. The first chapter introduces various notions from commutative algebra such as various classes of polynomials, monomial orders

and the division algorithm in its general form. Gröbner bases and normal forms are defined, various characterizations are presented and questions about uniqueness will be answered.

Chapter two is divided into two parts: The first part deals with Buchberger's algorithm, the first and most influential algorithm for Gröbner basis computation. The rest of the chapter is dedicated to upper bounds on the complexity of the ideal membership problem and Gröbner bases, culminating in a rather involved EXPSPACE-algorithm for both problems.

The final chapter provides a chain of complexity theoretic reductions from a generic EXPSPACE-complete problem to both ideal membership and Gröbner bases. The main protagonist here are (commutative) Thue systems, close relatives of formal grammars, whose structure can be cleverly embedded into binomial ideals. We also show that for some polynomials $f_1 - \dots - f_B$, a Gröbner basis of the corresponding ideal consists of double-exponentially many elements, which shows that in the worst case Gröbner bases are too large to be useful.

The aim of this thesis is to introduce the reader to the rich theory of Gröbner bases with its connections to symbolic algorithms, combinatorial problems and interesting complexity-theoretic results. Along the way we will mention many related results and give pointers to the literature.

Acknowledgment

I would like to thank my supervisor Sabrina for her encouragement and for providing useful ideas and resources. Also thanks to my fellow students Jan and Tobias for helpful discussions along the way. Last but not the least I would also like to thank my family and friends for encouraging and supporting me whenever I needed them.

Gröbner bases

In this first chapter we introduce the main protagonists of this thesis: Polynomial ideals and their Gröbner bases. We start by describing several interesting problems from both theoretical and applied sciences which can be reduced to solving a system of polynomial equations or more generally to the problem of ideal membership. Motivated by these problems we then generalize the familiar polynomial division algorithm to several polynomials in several variables, which naturally leads to the definition of a Gröbner basis. We discuss the topic of uniqueness of normal forms and Gröbner bases, and apply these techniques to the class of binomial ideals.

Most of the material presented here is standard and contained in any textbook on computational commutative algebra; we loosely follow von zu Gathen & Gerhard [23, Chapter 21] and occasionally other texts [19, Chapter 1], [24, Chapter 9], [28, Chapter 1&2].

1.1 Motivating examples

Many interesting problems from the sciences and engineering can be modeled by polynomial equations. We give an example from robotics [23, Example 21.1].

Example 1.1 (The reachability problem in robotics). We model a simple robotic arm operating in the plane \mathbb{R}^2 . It consists of two straight line segments \overline{OQ} and \overline{QE} of length 3 and 1 respectively, with the origin $O = (0, 0)$ and two variable points $Q = (G, H)$, $E = (I, F)$. The length of the parts constrain the possible configurations of the joints Q and E and enforce the following two equations

$$G^2 + H^2 = 9, \quad (G - I)^2 + (H - F)^2 = 1. \quad (1.1)$$

Consider the line parameterized by $L = \{(c - 5 + 2c^2, 2 + B^2) \mid c \in \mathbb{R}\}$. Can the robot reach L , i. e. is there a configuration with $E \in L$? In this case the answer is yes, for example with $Q = (0, 3)$, $E = (1, 3)$. On the other hand, the line $L^0 = \{(c - 10 + 2c^2, 2 + B^2) \mid c \in \mathbb{R}\}$ seems out of reach, but it is not immediately obvious how to prove the *non-solvability* of such a problem (in this case, L^0 has distance $\sqrt{74}$ from the origin).

More generally, one can parameterize $L_c = \{(c - c^2, 2 + B^2) \mid c \in \mathbb{R}\}$ and ask: for which values of c is there a solution? Of course, more complicated robots can be modeled with multiple joints and other constraints, then the number of equations which must be satisfied

simultaneously increases.

y

Nonlinear algebra is the broad field of mathematics studying polynomial equations, their structure and how to solve them, using techniques from various disciplines such as algebraic geometry, computer algebra, optimization and representation theory. An overview of several interesting applications of different flavors such as biochemical reactions, computer visions or statistics is presented by Breiding et al. [7]. The solutions to the preceding problems are mostly defined over the real or complex numbers, on the other hand applications in cryptography are often interested in solutions defined over \mathbb{F}_q or finite fields.

Another interesting application is that of “automatic” theorem proving, adapted from [23, Example 21.2].

Example 1.2 (Proving theorems in euclidean geometry). Consider a triangle with vertices A, B, C in the plane, an elementary theorem states that the perpendicular bisectors of the three sides all meet in a common point, the *circumcenter*. After scaling and rotating the triangle we may assume $A = (0, 0)$, $B = (1, 0)$ and $C = (G, H)$ for $G \in [0, 1]$ ($H > 0$). The three bisectors can be

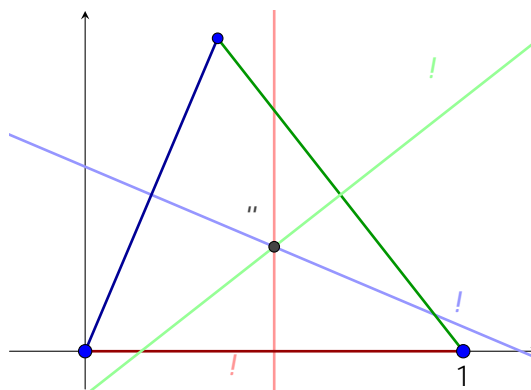


Figure 1.1: The perpendicular bisectors of a triangle intersecting in the circumcenter O .

parametrized as

$$\begin{aligned} \ell_1 &= \{x = \frac{1}{2}\} \\ \ell_2 &= \{y = \frac{H}{2} + \frac{H-G}{2}x\} \\ \ell_3 &= \{y = \frac{H}{2} + \frac{H+G}{2}x\} \end{aligned}$$

Let $O = (D, E)$ be a point, the condition that O lies on each of these lines can be described as an equation

$$x - \frac{1}{2} = 0 \tag{1.2}$$

$$y - \frac{H}{2} - \frac{H-G}{2}x = 0 \tag{1.3}$$

$$y - \frac{H}{2} - \frac{H+G}{2}x = 0 \tag{1.4}$$

Clearly two of the three equations can be satisfied (for fixed G, H) at the same time, as two non-parallel lines intersect. The question is whether there is a solution to $f = g = h = 0$ at the same time. The answer is yes, since we have

$$f = g = h$$

and hence if two of the polynomials vanish, then so does the third. Other geometric properties of the triangle can also be described using polynomial equations, and one may hope to similarly prove more involved statements. y

The previous problem was solved by showing that a given polynomial is a linear combination of other polynomials. The coefficients (here $1 - 1$) may even be polynomials themselves, the conclusion is still valid. This is an instance of the polynomial ideal membership, one of the central problems of this thesis.

1.2 The ideal membership problem

We now formally introduce the notion of polynomial ideals and the membership problem. Let $\mathbb{Z} = \{0, 1, 2, \dots\}$ denote the natural numbers and let \mathbb{k} be a field such as \mathbb{R}, \mathbb{C} and \mathbb{F}_q and $\mathbb{k}[x] = \{f_0 + f_1x + \dots + f_nx^n\}$.

Definition 1.3 (Polynomial). A *polynomial* over \mathbb{k} is an expression

$$f = \sum_{j=0}^n a_j x^j \quad a_j \in \mathbb{k} \quad \deg f = n \text{ if } a_n \neq 0 \text{ and } a_j = 0 \text{ for finitely many } j \in \mathbb{Z}^+$$

the ring of polynomials is $\mathbb{k}[x] = \mathbb{k}[x_1, \dots, x_n]$. The expression x^j is a *monomial*, the set of monomials will be denoted as $\text{Mon}(\mathbb{k}[x])$ or Mon_x . The a_j are the coefficients of f . If $a_n \neq 0$, then x^j is a *term* of f , the set $\text{supp}(f) = \{j \in \mathbb{Z}^+ \mid a_j \neq 0\}$ is the *support* of f . The *(total) degree* of $f \in \mathbb{k}[x]$ is the number

$$\deg f = \max\{j \mid a_j \neq 0\} = \max \text{supp}(f)$$

The zero polynomial has degree $-\infty$ by convention. y

The previous definition makes sense not only over a field \mathbb{k} but rather over any commutative ring, for example $\mathbb{Z}[x]$ is the ring of polynomials with integer coefficients. In concrete examples we will use variables such as x, y, z instead, for example

$$f = 4x^3 + \frac{5}{42}x^2 + 12x + 14 \in \mathbb{Z}[x] \quad \text{supp}(f) = \{0, 1, 2, 3\} \quad \deg f = 3$$

If $G_1, \dots, G_r \in \mathcal{G}(\kappa)$ are elements of the base field, then we can evaluate a polynomial f as

$$f(G_1, \dots, G_r) = \sum_{\alpha \in \mathbb{N}^n} c_\alpha G_1^{\alpha_1} \cdots G_r^{\alpha_r}$$

Remark. In this way f defines a function $f: \kappa^n \rightarrow \kappa$ and this function uniquely determines f as long as $\deg f_j \leq j$ (for example if κ is infinite). Therefore, it is generally harmless to identify polynomials with polynomial functions, but we will treat polynomials as abstract sums most of the time.

Appendix A.1 defines some basic notions of ring theory; we will only need the polynomial ring. Let $\kappa \llbracket x_1, \dots, x_n \rrbracket$ be a set of polynomials; the ideal generated by κ is the set of (polynomial) linear combinations of elements of κ :

$$\langle \kappa \rangle = \left\{ \sum_{i=1}^r h_i g_i \mid h_i \in \kappa \llbracket x_1, \dots, x_n \rrbracket, g_i \in \kappa \right\}$$

If the ring $\kappa \llbracket x_1, \dots, x_n \rrbracket$ is understood in the context, then the subscript will be omitted. Assuming for a second that we fix a suitable representation of multivariate polynomials over κ (we will do this in section 1.7). The ideal membership problem is the following decision problem.

Definition 1.4 (Ideal membership problem, IM_κ).

Input: $f, g_1, \dots, g_r \in \kappa \llbracket x_1, \dots, x_n \rrbracket$ multivariate polynomials from $\kappa \llbracket x_1, \dots, x_n \rrbracket$

Output: Decide whether $f \in \langle g_1, \dots, g_r \rangle$ y

Example 1.5. A monomial ideal is an ideal $\langle \kappa \rangle$ generated by a set of monomials Mon_κ . In this case, ideal membership is an easy task: y

Lemma 1.6. If \mathfrak{I} is an ideal generated by monomials then $f \in \mathfrak{I}$ if and only if each monomial $m \in \text{supp}(f)$ is divided by some $m \in \text{Mon}_\kappa$.

Proof. Indeed, this is clearly sufficient, conversely write $f \in \mathfrak{I}$ as $f = \sum_{i=1}^r h_i g_i$, $h_i \in \kappa \llbracket x_1, \dots, x_n \rrbracket$. If $m \in \text{supp}(f)$ doesn't occur in g_i , then all such terms can be omitted from the sum, leaving only terms $m \in \text{supp}(h_i g_i)$ occurring in f . If furthermore $m = m' \cdot g_i$, then we can combine the two terms to $h_i g_i$, $h_i' g_i$ so that we have exactly one summand for each term in f . This presentation proves the claim.

This yields a trivial polynomial time algorithm for deciding monomial ideal membership; just compare the exponents of each term $m \in \text{supp}(f)$ to each g_i and check if $g_i \mid m$ for $i=1, \dots, r$. We will see that ideal membership is, in general, much harder, but it is interesting to restrict the polynomials to various classes of polynomials and explore their complexity. Interesting classes include

Input: All polynomials (IM_κ)

- ^ Monomials - (the previous example)
- ^ Binomials 0 - , 1 - or even pure binomials -
- ^ Homogeneous polynomials $\sum_{j=3}^1 5$ - , this case will be denoted by $IM_{h\rightarrow}$.

In the homogeneous case ideal membership can also be simplified: For a polynomial 5 denote its homogeneous components by $5^{(j)} = \sum_{j=0}^{\deg 5} B_j 5^{(j)}$, then we have

Lemma 1.7. If \mathfrak{I} consists of homogeneous polynomials, then $5 \in \mathfrak{I}$ if and only if $5^{(j)} \in \mathfrak{I}$ for $j = 0, \dots, \deg 5$. Furthermore, if 5 is homogeneous and

$$5 = \sum_{i=1}^r \alpha_i \mathfrak{I}_i, \quad \mathfrak{I}_i \in \mathfrak{I}, \quad \deg \mathfrak{I}_i = \deg 5 - \deg \alpha_i$$

then the \mathfrak{I}_i may be chosen to be homogeneous of degree $\deg \mathfrak{I}_i = \deg 5 - \deg \alpha_i$.

The proof is similar to Lemma 1.6, see for example [19, Lemma 2.2.7]. Such degree bounds can be used to find the \mathfrak{I}_i , this will be exploited in chapter 2.

The ideal membership problem can be used to decide whether a set of polynomial equations $\mathfrak{I} = \mathfrak{I}_1 = \dots = \mathfrak{I}_r = 0$ has a solution. The following theorem holds true for any algebraically closed field, for simplicity we specialize to the complex field.

Theorem 1.8 (Hilbert's Nullstellensatz). A set of polynomials $\mathfrak{I}_1, \dots, \mathfrak{I}_r \in \mathbb{C}[x_1, \dots, x_n]$ has a simultaneous zero in \mathbb{C}^n if and only if $1 \notin \mathfrak{I}_1 + \dots + \mathfrak{I}_r$.

If $1 = \sum_{i=1}^r \alpha_i \mathfrak{I}_i$ and $G \in \mathfrak{I}$, then $1 = \sum_{i=1}^r \alpha_i \mathfrak{I}_i + G \mathfrak{I}$, hence at least one of the \mathfrak{I}_i does not vanish on G . The proof of the other direction is much more involved, see for example [19, Theorem 3.5.2] or [24, Corollary 1.8]. This motivates the following variant of the ideal membership problem:

Definition 1.9 (Nullstellensatz, HNST_r).

- ^ Input: $\mathfrak{I}_1, \dots, \mathfrak{I}_r \in \mathbb{C}[x_1, \dots, x_n]$ multivariate polynomials from $\mathbb{C}[x_1, \dots, x_n]$
- ^ Output: Decide whether $1 \in \mathfrak{I}_1 + \dots + \mathfrak{I}_r$ y

Remark. One might ask why we don't define HNST_r to ask about solutions in \mathbb{C}^n but rather in f . The reason is that this problem is computationally tractable (in the Turing model), while it is not known if the existence of rational solutions is even decidable! The (negative) answer to Hilbert's tenth problem shows that the set

$$\{G \in \mathbb{Z}[x_1, \dots, x_n] \mid G = 1 \text{ and } G \mathfrak{I} = 0 \text{ for some } \mathfrak{I} \in \mathbb{Z}[x_1, \dots, x_n]\}$$

is undecidable. On the other hand, solvability in the ground field is NP_r-complete in the Blum Shub Smale model of computation, in analogy to how SAT is NP-complete in the bit model [5, Chapter 5].

1.3 Polynomial division

We now review the familiar notion of polynomial division with remainder. Let $f, g \in \mathbb{A}[x]$ be univariate polynomials, $g \neq 0$, then there exist unique $q, r \in \mathbb{A}[x]$ satisfying

$$f = gq + r \quad \deg r < \deg g$$

The polynomials q, r can be obtained algorithmically: For a polynomial of the form

$$f = a_n x^n + \dots + a_1 x + a_0 \quad a_n \neq 0$$

let $lt(f) = a_n x^n$ be its leading term (this notion will be formally introduced for multivariate polynomials in a moment). The procedure is described in Algorithm 1.

Algorithm 1 Univariate polynomial division

Require: $f, g \in \mathbb{A}[x]$, $g \neq 0$

Ensure: $f = gq + r$, $\deg r < \deg g$

1: $q \leftarrow 0, r \leftarrow f$

2: while $\deg r \geq \deg g$ do

3: $q \leftarrow q + lt(r) \cdot lt(g)^{-1}$

4: $r \leftarrow r - qg$

5: $r \leftarrow r - qg$

6: end while

› The equation $f = gq + r$ is a loop invariant.

› The degree of r strictly decreases.

We wish to generalize this procedure to multivariate polynomial division. At first glance there are two obvious obstacles:

- ^ In order to even specify quotient and remainder of a division, we need to be able to compare the degree of multivariate polynomials. The total degree is not an useful measure of size here: Consider $f = x^2y$, $g = xy^2$, then there do not exist polynomials $q, r \in \mathbb{A}[x, y]$ with $f = gq + r$ such that r has total degree ≤ 1 .
- ^ In order to extend the univariate division algorithm we would like to talk about the leading term of a polynomial f . Again, there might be several valid choices, even of the same total degree as f .

We can solve both problems at once by introducing monomial orderings. Recall that monomials are in natural bijection with tuples of natural numbers:

$$\check{Z}^n = \{x_1^{a_1} \cdots x_n^{a_n} \mid (a_1, \dots, a_n) \in \mathbb{N}^n\} = \text{Mon}_n$$

If we choose a suitable ordering on the set Mon_n , then we can talk about the largest monomial occurring in a polynomial f , and use this to define the leading term and degree $\deg f = \check{Z}(f)$.

Clearly such an order should be a total order (also called a linear order), and it should be compatible with the monoid structure of $\text{Mon}_=$. This leads to the following definition

Definition 1.10 (Monomial ordering). A monomial ordering is an order on the set $\check{Z} =$ (equivalently, on the set of monomials $\text{Mon}_=$) with the following properties:

- (i) \check{Z} is a total order For all $f, g \in \check{Z}$ we have $f < g$ or $g < f$.
- (ii) For $f, g \in \check{Z}$ with $f < g$ we also have $hf < hg$, $hf < hg$.
- (iii) $f^0 \dots \theta^0 < f^1 \dots \theta^0 g$ for all $f \in \check{Z}$.

It turns out that under assumption (i)+(ii), condition (iii) is equivalent to \check{Z} being a well-ordering [23, Corollary 21.20]:

- (iii') \check{Z} is a well-order Every non-empty set $S \subseteq \check{Z}$ has a minimal element with respect to $<$.

We can (and will) assume that a monomial ordering sorts the variables themselves in descending order $x_1 > x_2 > \dots$.

Example 1.11. The following are examples of monomial orderings:

- (i) The lexicographic ordering $_{\text{lex}}$ is defined as

$$f <_{\text{lex}} g \text{ if and only if the first nonzero entry in } f - g \text{ is negative.}$$

In other words, $f <_{\text{lex}} g$ if the number of x_1 's in f is less than in g , or they are equal and the number of x_2 's in f is less than in g , or they are equal too and so on.

- (ii) The graded lexicographic ordering $_{\text{grlex}}$ is defined as

$$f <_{\text{grlex}} g \text{ if and only if } \deg(f) < \deg(g) \text{ or } \deg(f) = \deg(g) \text{ and } f <_{\text{lex}} g.$$

In other words, the graded lexicographic ordering first sorts by total degree, and then uses lexicographic ordering as a tie-breaker.

- (iii) The graded reverse lexicographic order $_{\text{grevlex}}$ is defined as

$$f <_{\text{grevlex}} g \text{ if and only if } \deg(f) < \deg(g) \text{ or } \deg(f) = \deg(g) \text{ and } f <_{\text{lex}} g.$$

For example with $\check{Z} = \mathbb{Z}^2 /$ we have

$$x^3 <_{\text{lex}} x^2y <_{\text{lex}} xy^2 <_{\text{grlex}} x^2 <_{\text{grlex}} xy^2 <_{\text{grevlex}} x^3 <_{\text{grevlex}} xy^2.$$

From now on we will consider polynomial rings equipped with a monomial ordering, denoted as \prec (omitting the subscript if no confusion may occur). We now generalize the notions of degree and leading term to such polynomial rings. For this we add the formal symbol α to our set of multiindices with the properties

$$\alpha + \beta = \gamma \iff \alpha = \gamma - \beta, \quad \alpha \geq \beta \iff \alpha - \beta \geq 0.$$

Definition 1.12. Let $f = \sum_{\alpha} c_{\alpha} x^{\alpha}$ be a polynomial. If $c_{\alpha} \neq 0$, then we define $\deg f = \alpha$, otherwise $\deg f < 0$ and we define:

- (i) The multidegree $\deg f$ of f is the largest exponent α among the terms with respect to \prec .
- (ii) If $\alpha = \deg f$, then we define the leading term of f as $\text{lt } f = c_{\alpha} x^{\alpha}$ with leading coefficient $\text{lc } f = c_{\alpha}$ and leading monomial $\text{lm } f = x^{\alpha}$.

The multidegree enjoys properties similar to the usual degree: Let f, g be polynomials, then

- $\deg(f + g) \leq \max\{\deg f, \deg g\}$,
- $\deg(f \cdot g) = \deg f + \deg g$, with equality if $\deg f < \deg g$,
- if $f \neq 0$, then $\text{lt}(f \cdot g) = \text{lt } f \cdot \text{lt } g$ and similarly for lm, lc .

With this notion we can describe a division algorithm for multivariate polynomials which is very similar to algorithm 1. Our goal here is slightly different from before: In the univariate case we searched for $f = qg + r$ with small remainder, measured by the degree. Here we ask for the remainder to contain no terms divisible by the leading term of g , which is a weaker condition than having a smaller multidegree.

Algorithm 2 Multivariate polynomial division (single divisor)

Require: $f \in R[x_1, \dots, x_n], g \neq 0$

Ensure: $f = qg + r, \text{lm } r \prec \text{lm } g$ for all monomials $C \in \text{supp } r$.

```

1:  $q \leftarrow 0, r \leftarrow f$ 
2: while  $\text{lm } r \succeq \text{lm } g$  do
3:   if  $\text{lm } g \mid \text{lm } r$  then
4:      $q \leftarrow q + \frac{\text{lc } r}{\text{lc } g} \frac{\text{lm } r}{\text{lm } g} g$ 
5:      $r \leftarrow r - \frac{\text{lc } r}{\text{lc } g} \frac{\text{lm } r}{\text{lm } g} g$ 
6:   else
7:      $r \leftarrow r - \frac{\text{lc } r}{\text{lc } g} \frac{\text{lm } r}{\text{lm } g} g$ 
8:   end if
9: end while
10: end while
11: end while

```

Lemma 1.13. Algorithm 2 terminates, more specifically $\text{mdeg}^1 f^{(i)}$ strictly decreases each iteration if $f \neq 0$. It produces $A \in \mathbb{A}$ with $f = \sum_{i=0}^s a_i g_i$ such that the leading term of A does not divide any term in \mathbb{A} and $\text{mdeg}^1 A < \text{mdeg}^1 f$.

Proof. We first show that $\text{mdeg}^1 f_{\text{new}} < \text{mdeg}^1 f$; this is clear in the else-branch, as the leading term is removed. In the other case

$$\begin{aligned} \text{mdeg}^1 f_{\text{new}} &= \text{mdeg}^1 (f - \text{lt}(f) \cdot \text{lt}(g)^{-1} g) \\ &= \max\{\text{mdeg}^1 f - \text{mdeg}^1 g, \text{mdeg}^1 f - \text{mdeg}^1 g\} = \text{mdeg}^1 f. \end{aligned}$$

But $\text{lt}(f - \text{lt}(f) \cdot \text{lt}(g)^{-1} g) = \text{lt}(f)$, so we must have a strict inequality.

The assignments in line 5/6 and in line 8/9 preserve the loop invariant

$$f = \sum_{i=0}^s a_i g_i.$$

Also, s is only incremented by monomials g_i such that $\text{mdeg}^1 g_i < \text{mdeg}^1 f - \text{mdeg}^1 g$, so $\text{mdeg}^1 g_i < \text{mdeg}^1 f$. Furthermore, the if-condition in line 3 ensures that only terms indivisible by $\text{lt}(g)$ are added to A in line 8. When the algorithm terminates we have $f = 0$ and hence the claimed identities are ensured.

The remainder is denoted as $A = \text{rem}^1 f; g$, it assigns any such f a (unique) representative of f modulo g . This solves the divisibility problem for multivariate polynomials, as

$$g \mid f \text{ if and only if } \text{rem}^1 f; g = 0.$$

Proof. If $\text{rem}^1 f; g = 0$, then $f = \sum_{i=0}^s a_i g_i$. Conversely if $g \mid f$, then $f = \sum_{i=0}^s a_i g_i$ i.e. $A = \sum_{i=0}^s a_i g_i$. Assume $A < 0$, then this means $\text{lt}(A) = \text{lt}(g) \cdot \text{lt}(A)$, contradicting $\text{lt}(g) > \text{lt}(A)$.

1.4 The normal form algorithm and Gröbner bases

The previous observation may be rephrased as a simple case of the ideal membership problem: $f \in \langle g \rangle$ if and only if $\text{rem}^1 f; g = 0$. In general, ideals in polynomial rings need not be principal, but require several generators. For example $\langle x^2 - y^2, x^2 - z^2 \rangle$ cannot be generated by less than 2 elements. In order to solve the ideal membership problem we would like to extend the division algorithm to take as input both f and the generators g_1, \dots, g_s such that

$$f \in \langle g_1, \dots, g_s \rangle \text{ if and only if } \text{rem}^1 f; g_1, \dots, g_s = 0.$$

This will turn out to be a more involved task and leads to the notion of Gröbner bases. We first formalize the notion of a normal form.

Definition 1.14 (Normal form, NF). Let (\mathcal{A}, \prec) and (\mathcal{B}, \prec) be two well-orderings on \mathcal{A} and \mathcal{B} respectively. Let $f \in \mathcal{A}$ be in normal form with respect to (\mathcal{A}, \prec) if $\text{lm}(f) \in \mathcal{A} \setminus \text{supp}(\mathcal{B})$ and $\text{deg}(f) \in \mathcal{A} \setminus \mathcal{B}$.

The set of normal forms of f with respect to a finite set $\mathcal{B} = \{g_1, \dots, g_n\}$ is the set $\text{NF}(f, \mathcal{B})$ of \mathcal{A} such that

- (i) f is in normal form with respect to \mathcal{B} ;
- (ii) $f = \sum_{g \in \mathcal{B}} a_g g$ for suitable $a_g \in \mathcal{A}$ with $\text{deg}(a_g) < \text{deg}(g)$.

Notice that $\text{deg}(f) = \text{deg}(f) = \max_{g \in \mathcal{B}} \{\text{deg}(a_g) + \text{deg}(g)\} = \text{deg}(f)$.

In analogy to multivariate polynomial division with a single divisor we want to find a normal form f together with the \mathcal{B} from the previous definition. This is actually not much harder to achieve than in case $B = 1$, a slight modification of the previous algorithm yields the normal form algorithm 3. The key idea is to check the condition $\text{lm}(f) \in \mathcal{A} \setminus \mathcal{B}$ against all $g \in \mathcal{B}$ and then proceed in the same way.

Algorithm 3 The normal form algorithm

Require: $f \in \mathcal{A}$, $\mathcal{B} = \{g_1, \dots, g_n\} \subset \mathcal{A}$, $\mathcal{A} \setminus \text{supp}(\mathcal{B}) \neq \emptyset$

Ensure: $f = \sum_{g \in \mathcal{B}} a_g g$, $A \in \mathcal{A} \setminus \text{supp}(\mathcal{B})$ and all $\text{deg}(a_g) < \text{deg}(g)$

```

1:  $A \leftarrow \text{lm}(f)$ ,  $i \leftarrow 1$ 
2: while  $A \in \mathcal{B}$  do
3:   if  $\text{lm}(f) \in \mathcal{B}$  for some  $g$  then
4:     Choose such an  $g \in \mathcal{B}$  ▷ e.g. the smallest such  $i$ 
5:      $q \leftarrow \text{lt}(f) \cdot \text{lt}(g)^{-1}$ 
6:      $r \leftarrow f - qg$ 
7:      $f \leftarrow r$ 
8:   else
9:      $A \leftarrow \text{lm}(f)$ 
10:     $i \leftarrow i + 1$ 
11:  end if
12: end while
```

With this in mind the following lemma is proven exactly the same way as before.

Lemma 1.15. Algorithm 3 terminates and $\text{deg}(f)$ strictly decreases each iteration if $\mathcal{B} \neq \emptyset$. It produces $\sum_{g \in \mathcal{B}} a_g g$ as in Definition 1.14.

Algorithm 3 allows us to define $\text{rem}(f; \mathcal{B})$ as before (if we always choose the least possible i in line 4), but unfortunately this fails to solve the ideal membership problem in general!

Example 1.16 Consider $f = x^2 - y$, $g_1 = x - 1$, $g_2 = x^2 - 1$ and \prec_{lex} , then $\text{rem}(f; \mathcal{B}) = x - 1$, but $f = (x - 1)^2 + 2(x - 1) - 1$. Of course, this does not happen if we chose $i = 2$ in line 4 of the algorithm, indeed $\text{rem}(f; \mathcal{B}) = 0$.

We would like to consider generating sets of \mathcal{B} behaving well with this ambiguity in the division algorithm, it turns out that Gröbner bases have this property.

Definition 1.17. The initial ideal of $\langle \succ \rangle_{\mathbb{A}}^1$ is the monomial ideal

$$\text{in}^1 \mathfrak{I} = \langle \text{lm}^1 f \mid f \in \mathfrak{I} \rangle$$

We have the following characterizations:

Theorem 1.18 (Characterizations of Gröbner bases). Let \mathfrak{I} be an ideal and $\succ = \langle \succ \rangle_{\mathbb{A}}^1$. The following are equivalent:

- (a) $\text{in}^1 \mathfrak{I} = \text{Ht}^1 \mathfrak{I}$
- (b) For all $f \in \mathfrak{I}$ there is a unique A with $\deg A \leq \deg f$ such that $\text{lm}^1 A$ divides $\text{lm}^1 f$.
- (c) For all $f \in \mathfrak{I}$ we have $\text{rem}^1 f = 0$ if and only if $\text{lm}^1 f = 0$.

Moreover, if any of these properties is satisfied, then for any \succ the result A of algorithm 3 is independent of the choices on line 5.

Proof. (a) (b): Algorithm 3 guarantees the existence of a normal form $A \in \mathfrak{I}$ which satisfies the condition by definition. Now consider two decompositions $f = g_1 + A_1 = g_2 + A_2$, $\deg g_1 \leq \deg g_2$. Then $A_1 - A_2 = g_2 - g_1$, hence $\text{lm}^1 A_1 - \text{lm}^1 A_2 \in \text{in}^1 \mathfrak{I} = \langle \text{lm}^1 g \mid g \in \mathfrak{I} \rangle$. Assume $A_1 < A_2$, then by Lemma 1.6 some monomial in $A_1 - A_2$ is divisible by some $\text{lm}^1 g$, hence such a monomial must occur in either A_1 or A_2 , a contradiction.

(b) (c): Let $f \in \mathfrak{I}$. If $\text{rem}^1 f = 0$, then $\text{lm}^1 f \in \text{in}^1 \mathfrak{I}$. Conversely let $f \in \mathfrak{I}$, then the Algorithm yields a decomposition $f = g + A$, $\deg g < \deg A$, $\text{rem}^1 f = g$ such that A has the desired properties from (ii). But $A = 0$ also has these properties (recall $\deg 0 = -\infty$), so by uniqueness we must have $A = 0$. This also shows the independence of choices in Algorithm 3 in line 5.

(c) (a): In order to show that $\text{in}^1 \mathfrak{I} = \langle \text{lm}^1 f \mid f \in \mathfrak{I} \rangle$ it suffices to check that $\text{lm}^1 f \in \langle \text{lm}^1 g \mid g \in \mathfrak{I} \rangle$ for any $f \in \mathfrak{I}$. Write such a f as $f = g + A$, $\deg g < \deg A$ (by assumption the remainder is zero). Lemma 1.15 tells us that $\text{mdeg}^1 g \leq \text{mdeg}^1 f$ for each g and we must have equality for some g since otherwise $\text{mdeg}^1 g < \text{mdeg}^1 f$. Pick such an g then $\text{lm}^1 f = \text{lm}^1 g = \text{lm}^1 g \in \langle \text{lm}^1 g \mid g \in \mathfrak{I} \rangle$.

Definition 1.19 (Gröbner basis). A Gröbner basis of an ideal $\mathfrak{I} \subseteq \mathbb{A}[x_1, \dots, x_n]$ is a finite set $\{g_1, \dots, g_r\} \subseteq \mathfrak{I}$ satisfying any of the equivalent conditions in Theorem 1.18, in particular, $\text{Ht}^1 \mathfrak{I} = \langle \text{lm}^1 g_i \mid 1 \leq i \leq r \rangle$.

Remark. Characterization (a) is often used in the literature as the definition of a Gröbner basis, as it applies in the more general setting where \mathbb{A} is replaced with an arbitrary commutative ring [24, Remark 9.11] or a non-global monomial ordering is used [19, Section 1.2, 1.6]. Another reason is that we can prove existence of Gröbner bases easily, see the following corollary.

If we slightly modify the normal form algorithm 3, then independence of choice in said algorithm is actually also equivalent to being a Gröbner basis. This leads to the notion of conuence of rewrite relations and is, for example, explored in the book by Kreuzer & Robbiano, where even more characterizations of Gröbner bases are presented [28, Theorem 2.4.1].

Corollary 1.20. Any ideal $\langle \succ_{\leq} \rangle$ admits a Gröbner basis.

Proof. The set $\text{Im}^{>0}$ generates the ideal in $\mathbb{K}[x_1, \dots, x_n]$ (by definition). As the ring $\mathbb{K}[x_1, \dots, x_n]$ is Noetherian (Hilbert's basis theorem A.1), any generating set contains a finite generating subset $\{f_1, \dots, f_r\} \subset \text{Im}^{>0}$. Then $\{f_1, \dots, f_r\}$ is a Gröbner basis of $\langle \succ_{\leq} \rangle$ by characterization (a).

Example 1.21. Any finite set of monomials is a Gröbner basis for the ideal $\langle \succ_{\leq} \rangle$. The polynomials $f_1 = x_1 - 1$, $f_2 = x_1^2 - 1$ from example 1.16 are not a Gröbner basis (they violate (c)).

Theorem 1.18 and its proof have revealed that normal forms with respect to Gröbner bases are unique, and suggests that there is a normal form with respect to the whole ideal $\langle \succ_{\leq} \rangle$.

Theorem 1.22 (The normal form map NF). Let $\langle \succ_{\leq} \rangle$ be an ideal.

- (i) For each $f \in \mathbb{K}[x_1, \dots, x_n]$ there exists a unique $\text{NF}(f)$ such that $f - \text{NF}(f) \in \langle \succ_{\leq} \rangle$ and $\text{NF}(f)$ is in normal form with respect to $\langle \succ_{\leq} \rangle$.

We denote this element $\text{NF}(f) = \text{NF}(f)$.

- (ii) If G is a Gröbner basis of $\langle \succ_{\leq} \rangle$ then $\text{NF}(f) = \text{NF}(f)$, in particular, any two Gröbner bases of $\langle \succ_{\leq} \rangle$ define the same (unique) normal form.

- (iii) The map $\text{NF} : \mathbb{K}[x_1, \dots, x_n] \rightarrow \mathbb{K}[x_1, \dots, x_n]$ is \mathbb{K} -linear with kernel $\ker \text{NF} = \langle \succ_{\leq} \rangle$.

We note that the map NF is not multiplicative, for example $\text{NF}(x_1 - 1)(x_1 + 1) = \text{NF}(x_1^2 - 1) = 0$.

Proof. (i) Let G be a Gröbner basis of $\langle \succ_{\leq} \rangle$, then by 1.18(a) being in normal form with respect to G is equivalent to being in normal form with respect to $\langle \succ_{\leq} \rangle$. Hence by 1.18(b) there is a unique $A \in \mathbb{K}[x_1, \dots, x_n]$ in normal form with respect to G and with $f - A \in \langle \succ_{\leq} \rangle$.

- (ii) We just showed that the polynomial(s) in $\text{NF}(f)$ satisfy the condition in (i).

(iii) For linearity consider $f = 5x_1^2 + 6x_1$, $5 = \text{NF}(5x_1^2)$, $6 = \text{NF}(6x_1)$. Then 5 and 6 are also in normal form with respect to G (the monomials which occur must also occur in 5 or 6). We also have

$$5 - \text{NF}(5) = 5 - 5x_1^2 \in \langle \succ_{\leq} \rangle \quad \text{and} \quad 6 - \text{NF}(6) = 6 - 6x_1 \in \langle \succ_{\leq} \rangle$$

so $\text{NF}(5 + 6) = 5 + 6$ and $\text{NF}(5x_1^2 + 6x_1) = 5 + 6$. The fact that $\ker \text{NF} = \langle \succ_{\leq} \rangle$ is a reformulation of Theorem 1.18(c).

We can characterize the normal form by a minimality condition: We can extend $\text{Mon}_=$ to finite sets of monomials Mon_\neq by looking for the largest element not in the other set

$$m \in \text{Mon}_\neq \text{ if and only if } \max \{m\} \neq \max \{m\} \cup \text{Mon}_=.$$

The order \prec_P is still a well-order [43, Lemma 2.4].

Lemma 1.23. Let $\langle G \rangle$ be an ideal in R and set $B = \{f_1, \dots, f_r\}$. Then $\text{NF}_P(f)$ is the unique element of $\langle G \rangle$ with minimal support (with respect to \prec_P).

Proof. Consider a $f \in \langle G \rangle$ with minimal support (exists since \prec_P is a well-order). Any reduction step in the normal form algorithm strictly decreases the support with respect to \prec_P , so by assumption $f = \text{NF}_P(f) = \text{NF}_P(f)$.

1.5 Reduced Gröbner bases and uniqueness

If G is a Gröbner basis of some ideal I , then $\{f + g\}$ is also a Gröbner basis for any polynomial $f \in I$. Hence there are many Gröbner bases for the same ideal. A first step towards making Gröbner bases unique is the observation that if $f = g + h$ with $\text{lm}(f) \neq \text{lm}(g)$, then $\{h\}$ is still a Gröbner basis (see below). This leads to the following definition:

Definition 1.24 (Interreduced Gröbner basis). A set of polynomials $G = \{g_1, \dots, g_r\}$ is normalized if $\text{lc}(g_i) = 1$ for all $g_i \in G$.

A Gröbner basis G is interreduced if it is normalized and for each $g_i \in G$ we have $\text{lm}(g_i) \notin \langle \text{lm}(g_j) \mid j \neq i \rangle$.

Lemma 1.25. Let G be a Gröbner basis of I .

- (i) If there is a $g \in G$ such that $\text{lm}(g) \in \langle \text{lm}(g_j) \mid j \neq i \rangle$, then $\{g_j \mid j \neq i\}$ is also a Gröbner basis of I .
- (ii) Assume that G is normalized. Then G is interreduced if and only if it is minimal, i. e. it does not properly contain a Gröbner basis of I . In particular, G contains an interreduced Gröbner basis.
- (iii) Any two interreduced Gröbner bases G of I have the same length and $\text{lt}(g_i) = \text{lt}(h_i)$.

Proof. (i) Using the definition of a Gröbner basis, we have

$$\text{lt}(g_i) = h_i = f + \text{lt}(g_j) \in \langle \text{lt}(g_j) \mid j \neq i \rangle = \langle \text{lm}(g_j) \mid j \neq i \rangle.$$

By Theorem 1.18(a), this is again a Gröbner basis of I .

(ii) If G is minimal, then by (i) it must be interreduced. Conversely, if G is a Gröbner basis for I and $g \in G$, then $\text{lm}(g) \notin \langle \text{lm}(g_j) \mid j \neq i \rangle$.

(iii) Let $f \in I$, then $\text{lm}(f) \in I$. Since this is a monomial ideal, we have $\text{lm}(f) \in I$ for some $f \in I$ (Lemma 1.6). Repeating this argument with f yields a $f \in I$ with $\text{lm}(f) \in I$, so $\text{lm}(f) \in I$. As f is interreduced, we get that $f = f$ and hence $\text{lt}(f) = \text{lt}(f) = \text{lt}(f)$ (here we use that f and f are normalized). Thus $f \in I$, as f was arbitrary we have $\text{lt}(f) \in I$ and by symmetry $\text{lt}(f) \in I$. Since all leading terms are distinct (again by interreducedness) we have $f_j = f_j$.

Example 1.26 If I is a monomial ideal generated by f_1, \dots, f_n , then I is interreduced if and only if none of the monomials divide each other. By Lemma 1.6 these monomials are precisely the minimal monomials in $\text{Mon}(R) \setminus I$ with respect to divisibility.

Unfortunately, interreduced Gröbner bases are not unique either, for example f_1, \dots, f_n and f_1, \dots, f_n are both interreduced Gröbner bases for $I = (f_1, \dots, f_n)$ (since they have the same leading monomial). This indicates that the lower terms must also be considered, which leads to the correct definition.

Definition 1.27 (Reduced Gröbner basis). A Gröbner basis G is reduced if it is normalized and for all $f \in G$ and any $g \in G$ we have $\text{supp}(f) \not\subseteq \text{supp}(g)$.

Theorem 1.28. Any ideal $I \subseteq R$ admits a unique reduced Gröbner basis.

Proof. Existence: By the previous lemma there exists an interreduced Gröbner basis f_1, \dots, f_n for I . For f_1, \dots, f_n we inductively

$$f_i = \text{rem}(f_i, f_1, \dots, f_{i-1})$$

We claim that $\text{lt}(f_i) = \text{lt}(f_i)$ by induction on i . By construction we can write

$$f_i = \sum_{j=1}^{i-1} c_j f_j + f_i \quad (1.5)$$

By induction $\text{lt}(f_j) = \text{lt}(f_j)$ for $j = 1, \dots, i-1$, but by interreducedness none of the terms $\text{lt}(f_j)$ can equal $\text{lt}(f_i)$. In order for (1.5) to hold, we must therefore have $\text{lt}(f_i) = \text{lt}(f_i)$.

Now f_1, \dots, f_n is a reduced Gröbner basis for I : By construction $f_i \in I$ and by the claim $\text{lt}(f_i) \in I$, so f_i is a Gröbner basis for I . Clearly it is normalized, and by construction no term in f_i is divisible by any leading monomial of any other f_j (coinciding with the leading monomials of the respective f_j).

Uniqueness: Let $G = \{f_1, \dots, f_n\}$ be two reduced Gröbner bases for I . By the previous lemma we get $f_i = f_i + f_i$ with $\text{lt}(f_i) = \text{lt}(f_i)$. No monomial in $f_i - f_i$ is divisible by any $\text{lm}(f_j)$: This is clear for $\text{lm}(f_i)$ by reducedness of G and f_i , and $\text{lm}(f_i) - \text{lt}(f_i) \in I$, as $\text{lm}(f_i) \in I$. This shows that $f_i - f_i$ coincides with its remainder $\text{rem}(f_i - f_i, f_1, \dots, f_{i-1})$, which vanishes since $f_i - f_i \in I$. So $f_i = f_i$ as i was arbitrary we get $G = G$.

Thus ideals of polynomials are uniquely characterized by their reduced Gröbner basis. They can also be used to find the minimal size of a Gröbner basis for \mathfrak{a} :

Corollary 1.29. The reduced Gröbner basis of an ideal has minimal length (number of elements) and minimal largest multidegree among all Gröbner bases of \mathfrak{a} .

Proof. Any Gröbner basis of \mathfrak{a} can be transformed into the reduced Gröbner basis \mathfrak{a}_0 by following the steps in Theorem 1.28. These steps never increase the number or multidegree of the elements, hence the claim follows.

We use this uniqueness property to define a decision problem associated to Gröbner bases:
 Definition 1.30 (Reduced Gröbner basis membership problem, GROEBM).

- ^ Input: f_1, \dots, f_m multivariate polynomials from $\mathbb{K}[x_1, \dots, x_n]$
- ^ Output: Decide whether or not g is contained in the unique reduced Gröbner basis of $\mathfrak{a} = \langle f_1, \dots, f_m \rangle$.

The normal form map NF can also be used to characterize the unique reduced Gröbner basis directly. We follow the notation of [30, Section 5].

Definition 1.31 ((Ir)reducible, minimally reducible). Let $\mathfrak{a} = \langle f_1, \dots, f_m \rangle$ be an ideal.

- (i) A polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$ is reducible with respect to $NF_{\mathfrak{a}}$ if $NF_{\mathfrak{a}}(f) \neq f$, and otherwise irreducible with respect to \mathfrak{a} .
- (ii) A monomial $\langle \alpha \rangle$ is called minimally reducible with respect to \mathfrak{a} if it is reducible, but all proper divisors $\langle \alpha_j \rangle < \langle \alpha \rangle$ are irreducible with respect to \mathfrak{a} .

A polynomial f is reducible with respect to \mathfrak{a} if and only if for any Gröbner basis \mathfrak{a}_0 there is a $g \in \mathfrak{a}_0$ with $\text{lm}(g) \leq \text{lm}(f)$.

Theorem 1.32. The unique reduced Gröbner basis of \mathfrak{a} is given by the set

$$\{ f \in \mathfrak{a} \mid \text{lm}(f) \in \text{Mon}_n \text{ is minimally reducible} \}.$$

Proof. Let \mathfrak{a}_0 be the reduced Gröbner basis of \mathfrak{a} and \mathcal{M} the set defined in the theorem.

If $f \in \mathfrak{a}_0$, $\text{lm}(f) \in \text{Mon}_n$, then f is in normal form with respect to \mathfrak{a}_0 (as \mathfrak{a}_0 is reduced), so $NF_{\mathfrak{a}_0}(f) = f$. In particular f is irreducible and $f \in \mathfrak{a}_0 \subseteq \mathfrak{a}$. Assume that some proper divisor $\langle \alpha_j \rangle < \langle \alpha \rangle$ were reducible, i. e. $\text{lm}(f) \leq \text{lm}(g)$ for some $g \in \mathfrak{a}_0$, then $\text{lm}(f) \leq \text{lm}(g)$, which is impossible for \mathfrak{a}_0 interreduced. We conclude $f \in \mathcal{M}$.

On the other hand, let $f \in \mathfrak{a}$, $\text{lm}(f) \in \text{Mon}_n$, then $\text{lm}(f) \in \mathcal{M}$. Since f is minimally reducible, we must have $\text{lm}(f) \in \mathcal{M}$. Applying the normal form algorithm 3 to f yields the remainder r , since no term of $\text{lt}(f)$ is in $\text{Ht}(\mathfrak{a}_0)$ by reducedness of \mathfrak{a}_0 . So $r = f$ as desired.

Thus, it is (in theory) possible to enumerate the reduced Gröbner basis by enumerating all monomials $<$ and calculating normal forms of (divisors of) $<$. This will be crucial in proving an exponential space lower bound on the task of calculating the reduced Gröbner basis.

1.6 The case of binomial ideals

To illustrate the theory we have introduced so far, we apply it to binomial ideals. This serves both as an interesting example as well as a fundamental ingredient in proving lower bound on the length of Gröbner bases in chapter 3. We partially follow Koppenhagen & Mayr [27], for a detailed exposition of binomial ideals and their properties consider the article by Eisenbud & Sturmfels [15].

Let $= \{0_1-^1, 1_1-^1-\dots-\beta_0^B, 1_B-^B\}$ and $= \{h_i\}$ be a binomial ideal; if all $0_8 = 1$, $1_8 = 1$, then we have a pure difference ideal. We start by showing that both the normal form algorithm and the (reduced) Gröbner basis associated to resp. again produce binomials and pure differences.

Lemma 1.33. Let $<$ be a monomial and δ a binomial.

- (i) $\text{rem}^1 <; \delta$ is a term and $\text{rem}^1 \delta; \delta$ is a binomial.
- (ii) The reduced Gröbner basis α consists of binomials.
- (iii) $\text{NF}^1 < \delta$ is a term and $\text{NF}^1 \delta$ is a binomial.

If δ and $\text{NF}^1 \delta$ consist of pure binomials, then the preceding statements hold true if binomial δ is replaced with pure binomial and term by monomial.

Proof. (i) If δ is a monomial, then each time a reduction in line 4-7 is applied, the resulting δ is a term again, and even a monomial if $\text{NF}^1 \delta$ consists of pure binomials. If no $\text{lt}^1 \delta \in \text{NF}^1 \delta$, then $A = \delta$ is the remainder.

Similarly, if δ is a binomial and $\text{lt}^1 \delta \in \text{NF}^1 \delta$, then $\delta - \frac{\text{lt}^1 \delta}{\text{lt}^1 \delta} \delta$ is again a binomial, as the leading terms in this subtraction cancel. On the other hand, if no $\text{lt}^1 \delta \in \text{NF}^1 \delta$, then in line 9-10 we have $A = \text{lt}^1 \delta = 0$ and $\delta = \delta - \text{lt}^1 \delta = \delta - \text{lt}^1 \delta$. From that point on δ is a monomial and the previous discussion applies (with the additional constant factor 1) and the result is a binomial.

Furthermore, if all binomials involved are actually differences of monomials, then the result will again be a pure binomial (note that $1 = 1$ in this case).

(ii) We postpone the proof for a few pages until the introduction of Buchberger's algorithm, see example 2.7.

(iii) This follows from the previous two statements, as $\text{NF}^1 \delta = \text{rem}^1 \delta; \alpha$, where α is the reduced Gröbner basis of δ .

We now turn to the case of pure binomial ideals and draw a connection to congruence relations on monomials, that is, equivalence relations compatible with multiplication (Definition A.4). We define \sim if and only if $\alpha - \beta \in I$. This makes sense for all ideals I , but for pure difference ideals we obtain a description of the normal form map, Gröbner basis and initial ideal in terms of equivalence classes.

Theorem 1.34 (Kopenhagen & Mayr 1999 [27]). Let I be a pure difference ideal with reduced Gröbner basis G .

- (i) For $\alpha \in \text{Mon}_k$, $\text{NF}(\alpha)$ is the minimal monomial in the equivalence class $[\alpha]$ (w.r.t. \prec).
- (ii) If $\alpha - \beta \in I$, $\alpha \succ \beta$, then β is the minimal monomial in $[\alpha]$.
- (iii) For any $\alpha \in \text{Mon}_k$ there is a $\beta \in G$ such that $\alpha - \beta \in I$.
- (iv) $\text{Mon}_k \setminus I$ consists of the monomials which are not the minimal element in $[\alpha]$.

Proof. (i) By the previous Lemma, $\text{NF}(\alpha)$ is a monomial which is by definition in $[\alpha]$. We also know that the normal form is a polynomial of minimal multidegree with $\text{lt}(\text{NF}(\alpha)) = \alpha$ (Lemma 1.23), so $\text{NF}(\alpha)$ is the unique minimal monomial in the class of α .

(ii) This is a direct consequence of Theorem 1.32 and statement (i).

(iii) Let $G = \{g_1, \dots, g_r\}$ be the reduced Gröbner basis of I , consisting of differences of monomials by the previous lemma. As $\alpha \in \text{Mon}_k$, there is a $g_j = \beta_j - \gamma_j$ with $\text{lt}(\beta_j) = \alpha$. Let $\beta_j = \alpha + \delta_j$; then $\alpha - \delta_j = \gamma_j \in I$ has leading term α .

(iv) Let $\alpha \in \text{Mon}_k$, then (iii) yields a $\beta \in G$ with $\alpha - \beta \in I$ and $\beta \prec \alpha$. Conversely, if α is not the minimal element of $[\alpha]$, then by (i) $\text{NF}(\alpha) \prec \alpha$, so $\alpha - \text{NF}(\alpha) \in I$ has leading monomial α .

1.7 Representing polynomials

In order to perform algorithmic manipulation on polynomials we need to fix a way to represent polynomials and their coefficients over a (finite) fixed alphabet. Let $\text{enc}: \mathbb{N}^n \rightarrow \mathbb{N}^m$ be an encoding. In order to do arithmetic calculations in the field of coefficients, we would like to be able to perform the usual field operations $+$, $-$, \cdot at low computational cost. More precisely, for $0 \leq i \leq m$, one can calculate $\text{enc}^{-1}(\text{enc}(a) + \text{enc}(b))$ in polynomial time with

$$\begin{aligned} \text{enc}^{-1}(\text{enc}(a) + \text{enc}(b)) &= \text{enc}^{-1}(\text{enc}(a) + \text{enc}(b)) \\ \text{enc}^{-1}(\text{enc}(a) - \text{enc}(b)) &= \text{enc}^{-1}(\text{enc}(a) - \text{enc}(b)) \\ \text{enc}^{-1}(\text{enc}(a) \cdot \text{enc}(b)) &= \text{enc}^{-1}(\text{enc}(a) \cdot \text{enc}(b)) \\ \text{enc}^{-1}(\text{enc}(a)^i) &= \text{enc}^{-1}(\text{enc}(a)^i) \text{ if } \text{enc}(a) < 0 \end{aligned}$$

Furthermore, equality of elements $\text{enc}^0 = \text{enc}^1$ must also be decidable in polynomial time.

This will be our standing assumption for the rest of the thesis. For example, if \mathcal{K} is a finite field, then we can calculate any of the arithmetic operations in constant time with a (large but constant size) lookup table. In finite fields pose a more interesting challenge.

Example 1.35. If $\mathcal{K} = \mathbb{F}_2$ then we can use the following encoding scheme: We encode $\sum_{i=0}^n a_i x^i$ with $\sum_{i=0}^n a_i 2^i$, as $\text{bin}^0 / \text{bin}^1$. We can then use integer arithmetic to calculate

$$\frac{0}{1} + \frac{2}{3} = \frac{03, 12}{13} \quad \frac{0}{1} = \frac{0}{1} \quad \dots$$

and can test for equality using $\frac{0}{1} = \frac{2}{3}$ if and only if $03 = 21$. Notice that the denominators will swell pretty quickly, so it might be well-advised to simplify the fraction if desired. y

Remark. Strictly speaking, this is not efficient enough for good upper bounds. Instead one should require addition and multiplication to be in AC^0 and NC^1 respectively, in order to obtain a well-endowed ring [43, Definition 3.14]. This is necessary in order to enable fast matrix operations as in section 2.5. But we will only consider the integers and rational numbers, which are in fact well-endowed, so we do not elaborate this further.

Suppose now that we have fixed a suitable encoding scheme for \mathcal{K} . Then there are two important choices to be made in order to encode polynomials from $\mathcal{K}[x_1, \dots, x_n]$

- (i) Are the exponents of the monomials encoded in binary or is a monomial represented by a sequence of variables? The former is called binary exponent representation, the latter unary representation.
- (ii) Are all coefficients written down (up to the leading term), or only those in the support of f ? The first case is a dense encoding, the second case is sparse encoding.

We will use sparse polynomial encoding with binary exponent representation, although it is remarkable that the lower bounds also hold true with unary exponent notation.

We now explain how to represent and calculate a monomial order. Robbiano showed that any monomial order \prec on $\text{Mon}_{\mathbb{Z}^n}$ can be represented by a finite set of weight vectors $\{w_1, \dots, w_m\}$, in the following sense: Let $\mathcal{F} = \{f_1, \dots, f_m\}$, the weight vectors can be interpreted as linear functions

$$w_i : \mathbb{Z}^n \rightarrow \mathbb{R} \quad w_i = \sum_{j=1}^n w_{ij} x_j \quad \text{with } w_{ij} \in \mathbb{R}$$

Then, \prec induces a monomial order with $f \prec g$ if and only if there is a $\lambda \in \mathbb{R}^m$ with

$$\sum_{i=1}^m \lambda_i w_i \cdot f > \sum_{i=1}^m \lambda_i w_i \cdot g \quad \text{and for all } \lambda \geq 0, \sum_{i=1}^m \lambda_i = 1$$

This is very similar to the definition of the lexicographic order \prec_{lex} , and in a sense all monomial orders can be understood as lexicographic orders with weights:

Theorem 1.36 (Robbiano 1985 [44]). For any monomial order there is a weight matrix $W \in \mathbb{R}^{n \times n}$ with $W_{ij} = w_j$.

Example 1.37. In the case of \prec_{lex} the weights have the simple form $w_j = \delta_{j1}$, so, W is the identity matrix. The graded lexicographic order can be represented by

$$W_{ij} = \begin{cases} 1 & \text{if } j=1 \\ 2^{-i} & \text{if } j=2, \dots, n \end{cases}$$

Similarly, for \prec_{grevlex} the following weight functions may be used

$$W_{ij} = \begin{cases} 1 & \text{if } j=1 \\ 2^{-i} & \text{if } j=2, \dots, n \end{cases}$$

Dubé, Mishra & Yap [13] gave a constructive proof of this theorem and also showed that the entries of W may be taken to be non-negative. In the previous example \prec_{grevlex} can be represented by $W_{ij} = \delta_{j1} + 2^{-i} \delta_{j2, \dots, n}$.

In order to represent an ordering in a finite number of bits, we restrict ourselves to the case where the weights are non-negative rational numbers $w_j \in \mathbb{Q}$. This is not a harsh restriction, as for any $W \in \mathbb{R}^{n \times n}$ there is a rational matrix W_i such that W_i coincides with W on monomials of degree $\leq i$.

Remark. The representation of monomial orders as weight matrices is mainly useful for theoretical considerations (for example in Chapter 2). In actual computer algebra systems it is usually much faster to directly implement the monomial orders of interest.

Algorithms and upper bounds

In this chapter we describe two fundamentally different approaches to the task of computing Gröbner bases and solving the ideal membership problem. The first is Buchberger's Algorithm, which uses so-called S-polynomials to enlarge a given set of generators to a Gröbner basis. The second approach is based on degree bounds for the polynomials in an ideal membership certificate or a reduced Gröbner basis, and uses linear algebra techniques to obtain exponential space algorithms. We also compare complexity-theoretic upper bounds results for different classes of polynomials.

The material on Buchberger's algorithm is standard to computational commutative algebra texts, we follow [24, Chapter 9]. The content of the later sections is inspired by survey articles of Mayr [32] and Mayr & Toman [35] together with the original literature.

2.1 S-Polynomials

We start with proving a criterion for a set $\{f_1, \dots, f_n\}$ to constitute a Gröbner basis of $\langle f_i \rangle$. The greatest common divisor and least common multiple for monomials x^α is defined similarly to the integers as

$$\gcd(x^\alpha, x^\beta) = x^{\min(\alpha, \beta)} \quad \text{lcm}(x^\alpha, x^\beta) = x^{\max(\alpha, \beta)}.$$

Definition 2.1 (S-Polynomial). Let $0 < \alpha < \beta$ be two polynomials. The S-polynomial is defined as

$$\text{Spoly}(f, g) = \frac{\text{lt}(g)}{C} f - \frac{\text{lt}(f)}{C} g \quad \in \langle \gcd(\text{lm}(f), \text{lm}(g)) \rangle$$

Equivalently, using $\gcd(x^\alpha, x^\beta) = x^\alpha$, we can write

$$\text{Spoly}(f, g) = \frac{\text{lc}(g)}{\text{lm}(f)} f - \frac{\text{lc}(f)}{\text{lm}(g)} g \quad \in \langle \text{lcm}(\text{lm}(f), \text{lm}(g)) \rangle$$

Example 2.2 The S-polynomial of two monomials is always zero. If f, g are differences of monomials or more generally binomials, then their S-polynomial is also a difference of monomials

resp. a binomial. For example, if $f_5 = x^1 - y^1$, $f_6 = x^2 - y^2$ with $\delta_8 = \delta_8$, then

$$S_{\text{poly}}(f_5 - f_6) = \frac{x^2 - y^2}{C} - \frac{x^1 - y^1}{C} = \frac{x^2 - x^1 - y^2 + y^1}{C} = \frac{x^1(x - y) - y^1(y - x)}{C} = \frac{(x - y)(x + y - y)}{C} = \frac{(x - y)x}{C} \in \text{gcd}(f_5, f_6) \cdot y$$

The key property of the S-polynomial is that the leading terms of $\frac{\text{lt}(f_6)}{C} f_5$ and $\frac{\text{lt}(f_5)}{C} f_6$ cancel, as both equal $x^2 y^0$. With this notion we can formulate and prove Buchberger's criterion.

Theorem 2.3 (Buchberger's criterion). Let $B = \{f_1, \dots, f_n\}$ be a finite list of polynomials. The following are equivalent:

- (a) B is a Gröbner basis of $\langle f_i \rangle$;
- (b) For all $f \in \langle f_i \rangle$ we have $\text{NF}(S_{\text{poly}}(f - B)) = \emptyset$;
- (b') For all $f \in \langle f_i \rangle$ we have $\text{rem}(S_{\text{poly}}(f - B)) = 0$.

Proof. We follow the proof given by Kemper [24, Theorem 9.12].

(a) \implies (b'): All S-polynomials of elements $f \in \langle f_i \rangle$ are linear combinations of elements of B and hence lie in $\langle f_i \rangle$. By characterization 1.18(c) we have $\text{rem}(S_{\text{poly}}(f - B)) = 0$, and thus clearly $\text{NF}(S_{\text{poly}}(f - B)) = \emptyset$.

(b) \implies (a): Assume (b) but also that B is not a Gröbner basis. We will arrive at a contradiction picking a minimal counterexample (with respect to the well-order \prec) and then construct an even smaller counterexample; thus showing that no such counterexample can exist.

Step 1: Construct a minimal expression of a counterexample.

By 1.18(a) there is a $f \in \langle f_i \rangle$ with $\text{lm}(f) \notin \text{HLM}(B)$, since B is not a Gröbner basis.

$$f = \sum_{i=1}^n c_i f_i + g, \quad \text{with } g \in \langle f_i \rangle, \quad \text{and } \text{lm}(g) \prec \text{lm}(f)$$

is not empty. Consider the map $\mu: \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ which assigns $\sum_{i=1}^n c_i f_i$ the maximum multidegree $\max_{i=1, \dots, n} \text{mdeg}_i(c_i f_i)$ with respect to \prec . As \prec is a well-order, this map takes its minimal value for some $\sum_{i=1}^n c_i f_i$; let $C = \sum_{i=1}^n c_i f_i$. Since

$$f = \sum_{i=1}^n c_i f_i + g \tag{2.1}$$

$\text{lm}(f)$ occurs in some $\text{supp}(c_i f_i)$, but not as its leading monomial (as $\text{lm}(f) \notin \text{HLM}(B)$), so $\text{mdeg}_i(c_i f_i) < \text{mdeg}_i(f)$. In particular, C does not occur in $\text{supp}(f)$, and so comparing coefficients of C in (2.1) and using $\text{mdeg}_i(c_i f_i) < \text{mdeg}_i(f)$ yields

$$0 = \sum_{i=1}^n c_i \text{lc}(f_i) - \sum_{i=1}^n c_i \text{lc}(f_i) \quad \text{if } \text{lm}(f) = C \\ \text{otherwise.} \tag{2.2}$$

to obtain a new representation $f_1^{(0)} - \dots - f_n^{(0)}$:

$$5 = 5 \cdot 6, \quad 6 = \sum_{s=1}^{\infty} \left| \begin{matrix} 2s \\ \{z\} \\ C \end{matrix} \right| \cdot \begin{matrix} 1 \\ s^0 \\ 0 \end{matrix} \cdot i_s \cdot 6^s$$

It remains to show that $\max_s mdeg^1 f_s^{(0)} = 0$. If $2s = 0$, then $mdeg^1 f_s^{(0)} = 0$ and hence

$$mdeg^1 f_s^{(0)} = mdeg^1 f_s, \quad i_s \cdot 6^s = \max_{f \in B} \{ 2s - i_s \cdot 6^s \} \cdot 6^s$$

On the other hand if $2s < 0$, then $mdeg^1 f_s = 2s \cdot \ln^1 f_s^{(0)} = mdeg^1 f_s - \ln^1 f_s^{(0)} = mdeg^1 f_s^{(0)}$ and

$$mdeg^1 f_s^{(0)} = \max \{ mdeg^1 f_s - 2s \cdot \ln^1 f_s^{(0)}, mdeg^1 f_s^{(0)} \} \cdot 6^s$$

Corollary 2.4. Given a set of polynomials $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$, the question whether B is a Gröbner basis of I is decidable.

Proof. By Buchberger's criterion it suffices to verify $\text{rem}^1 \text{Spoly}^1 f_i - f_j = 0$ for all i, j .

2.2 Buchberger's algorithm

In this section we present Buchberger's algorithm, historically the first algorithm calculating the Gröbner basis of an ideal, introduced by Buchberger in his PhD thesis [8].

Algorithm 4 Buchberger's algorithm

```

Require:  $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$ 
Ensure:  $B$  is a Gröbner basis of  $I = \langle f_1, \dots, f_n \rangle$ 
1:  $B := \{f_1, \dots, f_n\}$ 
2:  $\% B := \{f_j \mid 1 \leq j \leq n\}$ 
3: while  $\% <$  ; do
4:   Pick  $i \in \{1, \dots, n\}$ 
5:    $\% \quad \%n f_i - B$ 
6:    $B := \text{Spoly}^1 f_i - B$ 
7:    $B := \text{rem}^1 B - 0$ 
8:   if  $B < 0$  then
9:      $\% \quad \%[ \quad 1B - 0 \quad 6 \quad 2$ 
10:     $\quad [f \quad Bg$ 
11:   end if
12: end while
    
```

Theorem 2.5 (Correctness of Buchberger's algorithm). Algorithm 4 terminates after a finite number of steps and calculates a Gröbner basis of the ideal generated by the input f_1, \dots, f_n .

Proof. Termination: We first show that the branch in line 8-10 for $B < 0$ is only taken a finite number of times. Indeed, if $B < 0$, then in particular $\text{lm}^1 B^0 \notin \text{Hm}^1 \mathcal{G}$ and $\text{Hm}^1 \mathcal{G} \cap (\text{Hm}^1 [f, B] \cap \mathcal{G}) \neq \emptyset$. So each pass of line 10 strictly increases the ideal $\text{Hm}^1 \mathcal{G}$ and by the Noether property of R any ascending chain of ideals must eventually become stationary (see A.1). From this point on each pass through the loop decreases the size of \mathcal{G} in line 5, so the algorithm terminates with $\mathcal{G} = \emptyset$.

Correctness: Let \mathcal{G} be the final result of the algorithm and \mathcal{G}_0 the set at any point in the algorithm. We have the following invariants:

- $\text{Hm}^1 \mathcal{G}_0 = \text{Hm}^1 \mathcal{G}$ (as $\mathcal{G}_0 \supseteq \mathcal{G}$, line 1).
- For $f \in \mathcal{G}_0$, $B = \text{Spoly}^1 f - \mathcal{G}$ either $0 \in \text{NF}_{\mathcal{G}_0} B$ or \mathcal{G}_0 contains a normal form $\text{NF}_{\mathcal{G}_0} B$ (line 10).

In particular this applies to $f_0 = 0$. If \mathcal{G}_0 contains a normal form A of $B = \text{Spoly}^1 f_0 - \mathcal{G}$ then $0 = A - A$ is also a normal form of B with respect to \mathcal{G}_0 . Hence by Buchberger's criterion 2.3 the set \mathcal{G}_0 is a Gröbner basis of \mathcal{G} .

Example 2.6 We take the polynomials $f_1 = x^2 - 1$, $f_2 = x^2 - 1$ from example 1.16 with lex . We have $B_1 = \text{Spoly}^1 f_1 - \mathcal{G}^0 = x^2 - 1$ and $B_2 = \text{rem}^1 B_1; f_1 - \mathcal{G}^0 = B_1$. Hence we add B_1 to \mathcal{G} and consider the new pairs $B_1 - \mathcal{G}^0$ and $B_2 - \mathcal{G}^0$. We have

$$B_2 = \text{Spoly}^1 B_1 - \mathcal{G}^0 = x^2 - 1 - (x^2 - 1) = 0 \quad B_3 = \text{Spoly}^1 B_2 - \mathcal{G}^0 = 0$$

Now $B_2 = \text{rem}^1 B_2; f_1 - \mathcal{G}^0 = 0$ and $B_3 = \text{rem}^1 B_3; f_1 - \mathcal{G}^0 = 0$, hence the algorithm terminates and we obtain the Gröbner basis $\{x^2 - 1\}$.

Remark. Consider a set of polynomials $f_1, \dots, f_n \in R$ containing $x^2 - 1$. These polynomials enforce that any solution to this system takes values in $\{0, 1\}$. In this way Boolean formulae and equations can be expressed using polynomial systems, and one can use techniques from commutative algebra to reason about such statements. For an interesting example see the Gröbner proof system by Clegg, Edmonds & Impagliazzo [10], who use Gröbner bases and Buchberger's algorithm to produce proof certificates for tautologies.

If one is interested in a reduced Gröbner basis, then algorithm 5 can be applied after producing an arbitrary Gröbner basis \mathcal{G} :

The correctness of this algorithm follows from the results and proofs of Lemma 1.25 and Theorem 1.28. For example, the Gröbner basis from the previous example can be reduced to $\{x^2 - 1\}$. As a first application, we fill the gap in the proof of lemma 1.33 as promised.

Example 2.7 (The reduced Gröbner basis of a binomial ideal). Let $\mathcal{G} = \{f_1, \dots, f_n\}$ be a set of binomials, then any S-polynomial B formed from this set is also a binomial, and so is $B \text{ rem } \mathcal{G}$ by Lemma 1.33(i). Hence Buchberger's algorithm adds only binomials to \mathcal{G} and thus produces some Gröbner basis consisting of differences of monomials. Similarly, the algorithm reducing

Algorithm 5 Reduction of a Gröbner basis

Require: G a Gröbner basis of I

Ensure: G^0 is the unique reduced Gröbner basis of I

```

1:  $G^0 \leftarrow G$ ;
2: for all  $g \in G$  do
3:   if  $lc(g) < 0$  and  $lm(g) \neq lm(g')$  for all  $g' \in G^0$  then
4:      $g \leftarrow -g$ 
5:   end if
6: end for
7:  $G^0 \leftarrow G$ ;
8: for all  $g = \sum_{i=1}^n c_i x_i^{a_i} \in G$  do
9:    $r \leftarrow \text{rem}(g, G^0)$ 
10:   $G^0 \leftarrow G^0 \cup \{r\}$ 
11: end for
```

› Interreduction
 › Normalization

 › $M^0 = \langle g_1, \dots, g_r \rangle$
 › Reduction

this Gröbner basis will only delete or normalize elements from G and then introduce some remainders which are again binomials. Hence the reduced Gröbner basis consists of binomials. The same argument works for pure binomials and for homogeneous polynomials. \square

We also note that the combination of Buchberger's algorithm and the normal form algorithm yield:

Theorem 2.8. The ideal membership problem and (reduced) Gröbner basis algorithms are decidable (as long as the field operations are computable).

The run-time of Buchberger's algorithm depends heavily on the number of Polynomials B which have to be added to G . Also, the majority of the computation is spent calculating the remainder of the B with respect to increasingly complicated sets G . A good implementation uses various techniques to reduce the number of unnecessary normal form calculations, for example [19, Exercise 1.7.2]:

Lemma 2.9 (Product criterion). If $f = \sum_{i=1}^n c_i x_i^{a_i}$ with $\gcd(lm(f), lm(g)) = 1$, then

$$0 \leq \text{NF}_{f, G}(f) \leq \sum_{g \in G} \text{Spoly}(f, g)$$

and hence $\text{Spoly}(f, g)$ may be skipped in Buchberger's algorithm.

Remark. One of the most widely used improvements of Buchberger's algorithm are the algorithms \mathcal{G}_4 and \mathcal{G}_5 by Faugère [16]. For some bounds on the complexity of \mathcal{G}_5 see for example the work of Bardet, Faugère & Salvy [2].

2.3 Degree bounds

In this section we gather some upper bounds on the degrees of polynomials appearing in the problems of our interest, following Mayr [32] and Mayr & Toman [35]. We start with the

ideal membership problem IM , let $S = \{f_1, \dots, f_B\} \subset \mathbb{C}[x_1, \dots, x_g]$ then we are interested in bounds depending on the following factors:

- B the number of generators f_1, \dots, f_B
- g , the number of variables in $\mathbb{C}[x_1, \dots, x_g]$.
- $d_i = \deg f_i$, $d = \max_i d_i$, the degrees. Without loss of generality we may assume $d_1 \geq d_2 \geq \dots \geq d_B$ and $d = d_1$.

In order to decide whether $f \in \langle S \rangle$ one could try to systematically search the space of polynomials $\mathbb{C}[x_1, \dots, x_g]$ in order to find a solution to

$$f = \sum_{i=1}^B h_i f_i \tag{2.3}$$

A first step in order to make this feasible is to bound the degree of the h_i , historically the first result is due to Hermann, see Mayr & Meyer for a short proof [33, Appendix].

Theorem 2.10 (Hermann 1926 [20]). If the equation (2.3) admits a solution, then there is a solution with

$$\deg h_i \leq 3^{B-1} d^{B-1}$$

In the next section we will see how this and the bounds below may be used to turn ideal membership, normal form and Gröbner basis calculation into problems from linear algebra.

A natural question is to ask whether this degree can be improved, since a better bound yields a system of linear equations with fewer variables and equations. In this generality, the double-exponential nature of the Hermann bound is unavoidable in the following sense: For any $\epsilon > 0$ there exist polynomials f_1, \dots, f_B where $B = 10/\epsilon$, $O(1/\epsilon)$, the number of variables is $g = 10/\epsilon$, $O(1/\epsilon)$ and the degree is $O(1/\epsilon^3)$, such that any solution to (2.3) has at least one h_i with

$$\deg h_i \geq \frac{1}{2} \cdot 3^{B-1} d^{B-1}$$

This result is due to Mayr & Meyer [33], we will prove a variant of this in chapter 3. On the other hand, if the f_i satisfy additional properties, then better bounds can be proved. The case of homogeneous polynomials has already been mentioned in Lemma 1.7, there the degrees of the h_i are simply bounded by d .

Another important special case is the case $f = 1$, i.e. the Nullstellensatz case for HNST. Here a single exponential bound was proven by Brownawell for $f = f_1$, which was improved and extended to arbitrary fields by Kollár.

Theorem 2.11 (Kollár 1988 [26]). If $1 \in \langle f_1, \dots, f_B \rangle$ then there exist h_1, \dots, h_B with $1 = \sum_{i=1}^B h_i f_i$ such that

$$\deg h_i \leq \deg f_i + \sum_{j=1}^B \max\{0, \deg f_j - \deg f_i\} \tag{2.4}$$

This result is sometimes called the effective Nullstellensatz as it yields explicit bounds on the degrees occurring in Hilbert's Nullstellensatz.

Finally, we give an example on how the dimension of the ideal influences the degree bound, for more on dimension see for example [19, Chapter 5].

Definition 2.12 (Dimension of an ideal). The dimension $\dim^1 \mathfrak{a}$ of an ideal $\mathfrak{a} \subseteq \mathbb{K}[x_1, \dots, x_n]$ is the largest integer $d \leq n$ such that there exist variables $x_1, \dots, x_d \in \mathbb{K}[x_1, \dots, x_n]$ with

$$\mathfrak{a} \cap \mathbb{K}[x_1, \dots, x_d] \neq \{0\} \tag{2.10}$$

Theorem 2.13 (Dickstein et al. 1991 [12]). Assume (2.3) admits a solution and the ideal \mathfrak{a} is of dimension zero. Then there is a solution with

$$\deg(x_i) \leq 3^{2n-1} \cdot 3^{n-1} \cdot 3, \quad \deg(x_n) \leq 5^n \tag{2.11}$$

We now turn to degree bounds of Gröbner bases, let \prec be a monomial order on Mon_n . We can reduce to the homogeneous case as follows: Let $f = f_0 + \dots + f_d$ and add a new variable x_{n+1} .

Definition 2.14 ((De)homogenization). Let $f \in \mathbb{K}[x_1, \dots, x_n]$ of degree d , then its homogenization is

$$h_f = \sum_{j=0}^d f_j x_{n+1}^{d-j} \tag{2.12}$$

If $f \in \mathbb{K}[x_1, \dots, x_n]$ is homogeneous, then its dehomogenization is

$$a_f = f(x_1, \dots, x_n) \tag{2.13}$$

We define an ordering on $\text{Mon}_n^f = \mathbb{K}[x_1, \dots, x_n, x_{n+1}]$ via $h \prec g$ if and only if

$$\deg(h) < \deg(g) \quad \text{or} \quad \deg(h) = \deg(g) \quad \text{and} \quad h \prec g \tag{2.14}$$

Lemma 2.15. Let $\mathfrak{a} = \mathfrak{a}_d \subseteq \mathbb{K}[x_1, \dots, x_n]$ be an ideal and $\mathfrak{h} = \mathfrak{h}_d \subseteq \mathbb{K}[x_1, \dots, x_n, x_{n+1}]$ a homogeneous Gröbner basis with respect to h , then $\mathfrak{a} \cup \mathfrak{h}$ is a Gröbner basis of \mathfrak{a} .

This is not a difficult result, but it requires additional concepts from commutative algebra, see for example [37, Lemma 2.5] or [34, Lemma 7]. This shows that upper bound on the degree of Gröbner bases elements of homogeneous ideals (in $n+1$ variables) automatically yields bounds on the degree of Gröbner bases of arbitrary ideals (in n variables). Some conditional results in this direction were obtained by Möller & Mora [37], but the most influential result

is the unconditional degree bound by Dubé:

Theorem 2.16 (Dubé 1990 [14]). Let $\mathcal{I} = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ be an ideal and $\mathcal{B} = \max\{\deg f_i\}$. Then the reduced Gröbner basis consists of polynomials of degree

$$\deg \mathcal{G} \leq 2 \frac{3^2}{2} \cdot 3^{2^r - 1}.$$

If the f_i are homogeneous, then the exponent can be improved to

The proof uses the Hilbert function of a homogeneous ideal and cone decompositions, for an overview see the paper by Mayr & Ritscher [34], who also prove dimension-dependent upper bounds.

Theorem 2.17 (Mayr & Ritscher 2013 [34]). Let \mathcal{I} be an ideal. Let $\mathcal{I} = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ be an ideal of dimension A generated by homogeneous f_i of degrees d_1, \dots, d_r . Then the reduced Gröbner basis consists of polynomials of degree

$$\deg \mathcal{G} \leq 2 \frac{1}{2} d_1 \cdot 3_{=A} \cdot 3_1^{2^A - 1}$$

If the polynomials are not necessarily homogeneous, then a similar bound with exponent 2^A can be achieved. The degree bound by Dubé will enable us to prove an exponential space upper bound on the complexity of computing Gröbner bases.

2.4 From polynomials to linear algebra

We continue to use notation from the previous section with $\mathcal{I} = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ of degrees d_1, \dots, d_r in n variables. Furthermore, let \prec be a monomial order, given by a weight matrix $W \in \mathbb{R}^{n \times n}$ as in section 1.7. We will now describe how to translate the following problems into problems of linear algebra:

- (i) Decide whether $\mathcal{I} = \langle f_1, \dots, f_r \rangle = \langle 0 \rangle$ for suitable $\mathcal{B} \subseteq \mathbb{C}[x_1, \dots, x_n]$
- (ii) Calculate $\text{NF}(\mathcal{I})$, where $\mathcal{I} = \langle f_1, \dots, f_r \rangle$ with respect to \prec .

In order to obtain concrete upper bounds on the space required by a Turing machine to solve these problems, we work over the field of rational numbers \mathbb{Q} from here on until the end of this chapter. The input to these algorithms consists of the sequence of polynomials f_1, \dots, f_r and in second case the weight matrix W . The rational numbers and the exponents of the monomials are encoded in binary (or fractions of binary numbers). Let n be the length of the input, then we have the following estimates

$$3^{n-3} \cdot 2^{n-2} = n \cdot \quad (2.4)$$

We first consider the case of ideal membership. Let δ be a estimate of the degree of a set of solution $\deg \delta$, for example the Hermann bound $\delta = 3^0, 1 B 3^{2^}$. We use the notation b_j to indicate the coefficient of x^j in f . Then the solution of (i) depends on the finitely many coefficients in

$$f = \sum_{j=0}^{\delta} b_j x^j = \sum_{j=0}^{\delta} b_j x^{2j} \cdot x^j$$

A standard counting argument shows that the number of monomials of degree $\leq \delta$ in n variables is $\sum_{j=0}^{\delta} \binom{n+j-1}{j} = \binom{n+\delta}{\delta}$. Finding a solution to (i) is then equivalent to solving the following enormous system of linear equations:

- ^ Variables: $\{b_j\}_{j=0}^{\delta}$ unknowns b_j , indexed by f_1, \dots, f_g $\sum_{j=0}^{\delta} b_j x^j = g$.
- ^ Equations: $\sum_{j=0}^{\delta} b_j x^j = 0$ equations where $\delta = 3, \dots$, corresponding to the coefficient of x^j in (i)

$$f = \sum_{j=0}^{\delta} b_j x^j = \sum_{j=0}^{\delta} b_j x^{2j} \cdot x^j = 0$$

By construction the ideal membership problem is equivalent to solvability of this system of linear equations. In order to represent this as a matrix, we choose an ordering of the sets $\{x^j\}_{j=0}^{\delta}$ of monomials of degree $\leq \delta$ and $\{x^{2j}\}_{j=0}^{\delta}$ respectively, for example lexicographically. Then it makes sense to talk about the δ -th monomial in each set, and the system of equations can be written as

$$A \cdot b = B \cdot c \quad A \in \text{Mat}(A, \mathbb{C}^{\delta}, \mathbb{C}^{\delta}) \quad B \in \mathbb{C}^{2^g \times \delta}$$

In this presentation we have:

- ^ b_j is the coefficient of the j -th monomial in f (which is zero if $j > \delta$).
- ^ Write $c = \{c_j\}_{j=0}^{\delta}$, $c_0 = 1, c_j = 0$ for $j > \delta$, then c_j is the coefficient of the j -th monomial in g .
- ^ $A_{j,g}$ consists of the coefficients of the f_j as follows: Let x^j be the j -th monomial in $\{x^j\}_{j=0}^{\delta}$ (as in the previous case), then $A_{j,g} = \sum_{k=0}^{\delta} b_k x^{2k} \cdot x^j$.

In the language of linear algebra, the equation $A \cdot b = B \cdot c$ has a solution if and only if $B \cdot c$ is in the linear span of the columns of A , or equivalently if the matrix $[A \ B]$ has the same rank as A . This reduces the ideal membership to the task of computing a rank of a matrix. The size of this matrix can be estimated in the input length as follows:

- ^ The entries of A and A^0 are coefficients of f_1, \dots, f_g and hence of size $\leq \delta$.
- ^ The degree δ is bounded by

$$\delta = 3^0, 1 B 3^{2^} \stackrel{(2.4)}{\leq} 1 + 2 \cdot 0^2 + 2^{2^3}$$

using the generous estimate 2^5 .

^ The number of equations A is bounded by

$$A = \sum_{i=0}^5 \binom{5}{i} 2^{2^i} \cdot$$

^ Similarly, the number of variables B is bounded by

$$B = \sum_{i=0}^5 \binom{5}{i} 2^{2^i} \cdot$$

Thus we have proven

Theorem 2.18. The ideal membership problem can be reduced to the rank computation of two matrices of size $2^{2^5} \times 2^{2^5}$ whose entries are coefficients of the input. Furthermore, the polynomials can be obtained as solutions to a system of linear equations of the same characteristics.

We now turn to the calculation of the normal form. Here a similar approach may be used, namely we have the polynomial equation

$$0 = \sum_{j=1}^B \tilde{B}_j x^j \tag{2.5}$$

and we are looking for a solution with $\text{supp}(f) = \{j \mid \tilde{B}_j \neq 0\}$ minimal (Lemma 1.23). In order to do this we need an estimate on $\deg \sum_{j=1}^B \tilde{B}_j x^j$. Let

$$g = \max_{j \in \text{supp}(f)} \tilde{B}_j x^j$$

be the largest natural number occurring in the weight matrix \tilde{B} , and let g be a bound on the degree of the reduced Gröbner basis of \tilde{B} . Kühnle & Mayr [30, Section 2], expanding on [13], proved the following upper bound:

Theorem 2.19. For any $5 \leq g$ we have

$$\deg \sum_{j=1}^B \tilde{B}_j x^j \leq \deg \sum_{j=1}^B \tilde{B}_j x^j + g \cdot \# \tilde{B}$$

Remark. If a specific monomial order is considered, then better bounds are available. For example, if \tilde{B} is degree-dominated, i.e. $\deg \tilde{B}_j \leq \deg \tilde{B}_k$ implies $\tilde{B}_j \leq \tilde{B}_k$, then of course $\deg \sum_{j=1}^B \tilde{B}_j x^j \leq \deg \tilde{B}_5$ implies $\deg \sum_{j=1}^B \tilde{B}_j x^j \leq \deg \tilde{B}_5$.

We applying the Hermann bound to $\sum_{j=1}^B \tilde{B}_j x^j = \sum_{j=1}^B \tilde{B}_j x^j$ to obtain

$$\deg \sum_{j=1}^B \tilde{B}_j x^j \leq \deg \sum_{j=1}^B \tilde{B}_j x^j + g \cdot \# \sum_{j=1}^B \tilde{B}_j x^j$$

We use a strategy similar to the ideal membership case to turn (2.5) into a system of linear

equations, for additional details see [43, Chapter 6]. We introduce an extra factor $\delta_0 = 1$ to recreate the shape of the ideal membership equation

$$\delta_0 \delta_1 \dots \delta_B = \sum_{\alpha} A_{\alpha} x^{\alpha} = B \bullet$$

This time δ_0 contains the coefficients of $x_1 \dots x_B$, δ_1 contains the coefficients of x_0 , A contains the coefficients of $x_1 \dots x_B$, δ_B contains 0's and 1's for the coefficients of δ_0 and B contains the coefficients of δ_0 .

We now sketch how this system can be used to find the normal form $\delta_0 = NF(\delta_0)$. We know that there is some solution (for example $\delta_0 = \delta_0$) when all monomials in δ_0 are allowed. The normal form is characterized as the unique polynomial $\delta_0 \in \mathbb{F}_p[x_0, \dots, x_B]$ with minimal support $\text{supp}(\delta_0)$ with respect to \prec (see Lemma 1.23). The key idea is to systematically remove monomials from δ_0 together with the corresponding row from A and see whether the system still has a solution. We order the columns of A so that the columns in δ_0 are in ascending order with respect to the monomials in δ_0 , i.e. the lowest monomials come first. Then we have a maximal regular minor (an invertible square sub-matrix of maximal size) corresponding to the minimal solution δ_0 . One can decide whether a given column indexed by i is contained in this minor (i.e. if the corresponding monomial x^{α_i} is in $\text{supp}(\delta_0)$) by comparing the rank of the minor of the first i rows/columns to the rank of the first $i-1$ rows/columns: If the rank is different, then x^{α_i} is indispensable, otherwise it is not in the support.

The maximal degree of a monomial in (2.5) is bounded by $\max\{i, 3g - i, 3\}$, so the number of equations is bounded by $\sum_{i=0}^3 \binom{B}{i} p^{3g-i}$. Using similar estimates as before, we obtain the following result.

Theorem 2.20. The computation of (elements of) the support $\text{supp}(NF_{\mathbb{F}_p[x_0, \dots, x_B]}(\delta_0))$ can be reduced to rank computations of matrices of size $2^{2^{O(1)}} \times 2^{2^{O(1)}}$ whose entries are coefficients of the input (or 1). Furthermore, the normal form itself can be obtained as solutions to a system of linear equations of the same characteristics.

We note here that this is true even if the degree estimate for $\delta_0 = \deg \delta_0$ is not 2 but rather $2^{2^{O(1)}}$, this will become important when enumerating a Gröbner basis in algorithm 6.

2.5 Fast linear algebra on PRAMs

In this section we briefly introduce the PRAM model for parallel computation, for details and a modern treatment see for example the book by Parhami [40]. Since we will only use abstract results about the complexity on PRAMs, only an overview of the model is given.

A PRAM (parallel random access machine) consists of

- ^ a set of global registers, containing arbitrary integers,
- ^ a number of processors $p \geq 1$ (depending on the input size), each with their own local registers,
- ^ a finite program consisting of arithmetic operations, branching and read/write access to local or global memory.

Each processor runs on the same program with the knowledge of its id $i \in \{0, \dots, p-1\}$ and the number n . The input is contained in the global register, for example if the input is a matrix $A \in \mathbb{R}^{n \times n}$, then the global registers contain the n^2 coefficients. The execution is performed synchronously, and read/write conflicts are handled properly.

The efficiency of an algorithm is expressed both in the number p of processors used, as well as the number of steps T taken until each processor halts. A central result relating the PRAM model to (deterministic) Turing machines is the Parallel Computation Thesis

Theorem 2.21 (Fortune & Wyllie 1978 [17]). Let $T = O(\log^k n)$.

- (i) If $L \in \text{SPACE}(n^k)$, then L is accepted by a PRAM in parallel time $O(T)$.
- (ii) If L is accepted by a PRAM in parallel time $O(T)$, then $L \in \text{SPACE}(n^{O(T)})$.

In particular, parallel time complexity is polynomially related to sequential space complexity.

Thus, in order to obtain space-efficient algorithms for problems such as rank computation, we can employ efficient parallel algorithms. Of particular relevance are the following results due to Csanky.

Theorem 2.22 (Csanky 1976 [11]). Given an integer $n \times n$ matrix, the tasks of

- (i) matrix inversion
- (ii) solving a system of linear equations
- (iii) computing the determinant
- (iv) computing the coefficients of the characteristic polynomial

can be solved in parallel time $O(\log^2 n)$ using $O(n^2)$ processors.

Ibarra, Moran & Rosier extended this list to include matrix rank calculation.

Theorem 2.23 (Ibarra, Moran & Rosier 1980 [22]). The problem of calculating the rank of an $n \times n$ matrix can be solved in parallel time $O(\log^2 n)$ using $O(n^2)$ processors.

Remark. The papers cited here use the arithmetic machine model, i. e. directly manipulating integers (or rational numbers). Some care has to be taken in order to translate these results to the bit model, Pan describes some appropriate methods [39].

2.6 Upper bounds on ideal membership

We finally apply the space-efficient linear algorithms from the previous section to the ideal membership and normal form problems.

Theorem 2.24 (Mayr 1989 [31], $\text{IM} \in \text{EXPSPACE}$). There exists a deterministic algorithm which on input $\langle \mathcal{I}, \mathbf{f} \rangle$ decides whether there exist \mathbf{g} with $\mathbf{f} = \sum_{i=1}^B g_i \mathbf{f}_i$, using no more than exponential working space.

Proof sketch. Using polynomial space we can clear denominators of the input polynomials \mathbf{f}_i and hence may assume that all polynomials have integer coefficients. We first describe a parallel algorithm for this task.

Theorem 2.23 describes an algorithm for matrix rank calculation in parallel time $O^1 \log n$, where n is the size of the matrix. The matrices A, A^0 from **Theorem 2.18** have size $2^{O(n)}$ and hence there is a parallel algorithm calculating the rank of A in time $2^{O(n)}$ using $2^{2^{O(n)}}$ processors. Notice that we cannot write down these matrices explicitly (in exponential space), so instead each time this parallel algorithm requests an entry of A (by indexing it), we calculate it on the fly from the input polynomials. The time required to do this is negligible, since the entries are coefficients of the \mathbf{f}_i which can be indexed efficiently.

Now apply the parallel computation hypothesis (**Theorem 2.21**) to turn this exponential parallel time algorithm into an exponential space algorithm.

With some additional care one can extend this algorithm to output the solution in the same space bounds, for details see **Theorem 4** in the work of Mayr [31].

Theorem 2.25. With notation as in the previous theorem, if a solution exists, then the algorithm can write it to an output tape in exponential work space.

Notice however that the size of the \mathbf{g}_i themselves may be double-exponential by the Hermann bound and the results of **chapter 3**, hence it is important to distinguish the work tape from the output tape. A similar argument proves the analogous statement for the normal form, see also [43, **Theorem 6.2**].

Theorem 2.26. There is an exponential space algorithm which on input $\langle \mathcal{I}, \mathbf{f} \rangle$ computes the normal form $\text{NF}_{\mathcal{I}}(\mathbf{f})$.

Again, the size of the normal form may exceed exponential space, so care has to be taken if this algorithm is used as a subroutine.

If the polynomials are of a specific type, then we can use the other bounds from **section 2.3** to give better estimates on the degrees of the \mathbf{g}_i . This leads to matrices of single exponential space, and we conclude:

Theorem 2.27 ($\text{IM}_{h, \perp} \in \text{PSPACE}$). In the situation of **Theorem 2.24**, if

- (i) the polynomials \mathbf{f}_i are homogeneous or

(ii) $5 = 1$ (the Nullstellensatz case),

then the corresponding problem can be solved in polynomial space.

While the homogeneous ideal membership problem $\text{IM}_{h^{\perp}}$ is indeed hard for PSPACE (and hence complete), for the problem HNST^{\perp} much better results are available:

Theorem 2.28 (Koiran 1996 [25]). Under the assumption of the Generalized Riemann Hypothesis (GRH) we have $\text{HNST}^{\perp} \in \text{RP}^{\text{NP}}$. In fact, $\text{HNST}^{\perp} \in \text{AM} = \text{BP} = \text{NP}$.

For the definition of the Arthur-Merlin class see for example [1, Section 8.2]. Since HNST^{\perp} is NP-hard, this implies the surprising result that (under the GRH assumption) $\text{P} < \text{NP}$ if and only if $\text{HNST}^{\perp} \in \text{P}$. For details and improvements (weakening the GRH assumption) see the work of Rojas [45]. An overview over known complexity bounds for several variants of ideal membership is presented by Mayr & Toman [35, Table 1].

2.7 Computing a Gröbner basis in EXPSPACE

We finally present an algorithm computing the reduced Gröbner basis of an ideal $I = \langle f_1, \dots, f_n \rangle$ in exponential space. It is important to distinguish the work tape from the output tape, since the output may consist of double-exponentially many polynomials, each of which might contain double-exponentially many terms. The key to algorithm 6 is to enumerate the possible leading monomials one by one, and then comparing them to their normal forms in a sufficiently space-efficient way.

Algorithm 6 Enumerating the reduced Gröbner basis

Require: $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$, a weight matrix for

Ensure: Yields all elements of the reduced Gröbner basis of $I = \langle f_1, \dots, f_n \rangle$

```

1:  $m \leftarrow \max\{\deg f_1, \dots, \deg f_n\}$ 
2:  $z \leftarrow \frac{3^2}{2}, \gamma \leftarrow 3^{2^m-1}$  › The Dubé bound 2.16
3: for all  $Z = \sum_{j=1}^n z_j$  do
4:    $\langle \cdot \rangle \leftarrow \cdot$ 
5:   if  $\langle \cdot \rangle = \text{NF}_{h_{f_1, \dots, f_n}}^1 < 0$  then
6:     continue in line 3 ›  $m$  is not reducible
7:   end if
8:   for  $g \in \{f_1, \dots, f_n\}$  do
9:      $\langle \cdot \rangle \leftarrow \langle \cdot \rangle - \frac{1}{z_j} \langle \cdot \rangle - \frac{g}{z_j} \langle \cdot \rangle = \cdot$ 
10:    if  $\langle \cdot \rangle < \text{NF}_{h_{f_1, \dots, f_n}}^1 < 0$  then
11:      continue in line 3 ›  $m$  is not minimally reducible
12:    end if
13:   end for
14:   yield  $\langle \cdot \rangle = \text{NF}_{h_{f_1, \dots, f_n}}^1 < 0$  ›  $m$  is minimally reducible
15: end for
```

Theorem 2.29. Algorithm 6 enumerates the reduced Gröbner basis of $\mathcal{S} = \{f_1, \dots, f_n\}$ in exponential work space and double-exponential time.

Proof. Correctness: By Theorem 1.32, the reduced Gröbner basis consists of polynomials of the form $\langle \text{NF}_{\mathcal{S}}(f_j) \rangle$ where \langle is a monomial which is minimally reducible. The Dubé bound gives an upper bound on the degree of the elements of \mathcal{S} (Theorem 2.16), i. e. of \langle . The algorithm iterates through all possible leading terms \langle (line 3) and checks if \langle is reducible (line 5-8) and if any divisor $\langle^0 j \langle$ is irreducible (line 11-14). It succeeds to check this for \langle^0 with $\deg \langle^0 = \deg \langle - 1$, so in line 16 the algorithm has verified that \langle is minimally reducible and it yields the corresponding element.

Space requirement: Let n be the input size, then $n = B$ and $3 \leq B$. With this we have $2^{2^{O(n)}}$, which fits into the working memory of exponential size.

We can enumerate the monomials \langle of degree n in any order we like. In order to do this in exponential space, use binary counters $\langle_1, \dots, \langle_n$ from 0 to B and then take $\langle = \langle_1^{e_1} \dots \langle_n^{e_n}$. This requires $O(n \log B)$ space.

We use the normal form algorithm from the previous section on input $\langle \text{NF}_{\mathcal{S}}(f_j) \rangle$; this requires exponential space in \mathcal{S} (!) by the remark after Theorem 2.20. We cannot afford to write down the resulting polynomial in its entirety, but we can check (term by term) whether it coincides with \langle . This technique is applied in line 5 and 10, while in line 14 we can write the result (with an additional minus sign) to the output tape.

Time requirement: The number of configurations of an algorithm working in space $2^{O(n)}$ is bounded by $2^{2^{O(n)}}$, and hence its time requirement is at most double-exponential.

Corollary 2.30 (GROEBM \in EXPSPACE). There is an exponential space algorithm deciding whether \mathcal{S} is contained in the reduced Gröbner basis of \mathcal{S} .

Proof. Indeed, modify algorithm 6 as follows:

- ^ In line 15, instead of writing $\langle \text{NF}_{\mathcal{S}}(f_j) \rangle$ to the output, compare it to \langle , if they coincide then accept.
- ^ After line 17, reject.

This algorithm has essentially the same space requirements and decides GROEBM.

Remark. This algorithm is worst-case optimal in the sense that GROEBM is EXPSPACE hard and there exist inputs \mathcal{S} such that the corresponding reduced Gröbner basis indeed has double-exponentially many elements. On the other hand, this algorithm is uniformly impractical in the sense that even if \mathcal{S} consists of few elements, then algorithm 6 still requires exponential space (as \mathcal{S} is extremely large, and the normal form algorithm also uses exponential space on all inputs).

Ritscher improved this approach using S-polynomials and by increasing \mathcal{S} only as far as necessary to obtain a more space efficient algorithm [43]. For the class of pure binomial

ideals Koppenhagen & Mayr [27] devised an algorithm using combinatorial tools. While this algorithm requires exponential space (this is necessary, see chapter 3), it does not make use of the parallel computation hypothesis.

For low-dimensional ideals better bounds are known.

Theorem 2.31 (Krick & Logar 1991 [29]). If $I = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ is an ideal of dimension 1, then a Gröbner basis can be calculated in $2^{O(n)}$ assuming unit cost arithmetic of \mathbb{C} .

Lower bounds

In this chapter we prove an exponential space lower bound for the ideal membership problem and the reduced Gröbner basis membership problem. For this we introduce the notion of Thue systems, which are essentially presentations of semigroups. The key result is that there is a family of commutative Thue systems which can produce words of double exponential length in the size of the presentation. The chain of reductions from a generic EXPSPACE problem to Gröbner bases is displayed in Figure 3.1. We also introduce the concept of Church-Rosser systems, which are a string-replacement analogue of Gröbner bases. These notions will lead to examples of ideals with Gröbner bases of double-exponential length and degree.

The primary source for most of the chapter is the original work by Mayr & Meyer [33] and Huynh [21].

Figure 3.1: The chain of complexity-theoretic reductions.

Remark. In the literature, for example [33] and [32], the type of reduction is not polynomial time many-one reductions. Instead, more restrictive log-lin reductions are used: The reduction function f may use logarithmic space and $|f(x)| \leq |x|^{c_1}$. With this notion, the problems considered here are not complete for $\text{EXPSPACE} = \text{SPACE}^{2^{O(n)}}$, but rather $\text{SPACEB} = \text{SPACE}^{2^{O(\log n)}}$. This has the advantage that if \mathcal{L} is a SPACEB -hard problem with respect to log-lin reductions, then there is a $c > 0$ such that $\mathcal{L} \in \text{SPACE}^{2^{cn}}$, proving exponential resource lower bounds [33, Section 2] (this is essentially an application of the space hierarchy theorem [1, Theorem 4.8]).

In this thesis we only consider polynomial time reductions for simplicity, although the interested reader will have no difficulty in verifying that the reductions $\text{EBC} \leq \text{CSG} \leq \text{IM} \leq \text{GROEBM}$ are actually log-lin reductions.

3.1 Thue systems

We start by introducing a decision problem which is closely related to ideal membership: The word problem for finitely presented commutative semigroups (CSG). We present it in the general context of string rewriting systems (SRS), a concept closely related to formal grammars.

Definition 3.1 (String rewriting system, Thue system). A string rewriting system or semi-Thue system consists of an alphabet Σ together with a finite set of production rules $P \subseteq \Sigma^+ \times \Sigma^+$, written as

$$P = \{ \alpha_1 \rightarrow \beta_1, \dots, \alpha_n \rightarrow \beta_n \}$$

A Thue system is a semi-Thue system such that if P includes the rule $\alpha \rightarrow \beta$, then P also includes the reverse rule $\beta \rightarrow \alpha$. A production $\alpha \rightarrow \beta \in P$ can be applied to two strings $G = H\alpha$ if there is a decomposition

$$G = H_1 \alpha H_2 = H_1 \beta H_2$$

in symbols $G = H\alpha$. Let \equiv_P be the reflexive and transitive hull of \rightarrow_P , i.e. $G \equiv_P H$ if and only if G can be rewritten into H using a finite sequence of rules from P . Two Thue systems $\langle \Sigma, P \rangle, \langle \Sigma, P_0 \rangle$ are equivalent iff \equiv_P and \equiv_{P_0} coincide.

If P is a Thue system, then this is an equivalence relation, and even a congruence relation (see Definition A.4, in essence this means that the set of equivalence classes again form a monoid). Hence we get a monoid Σ^0 / \equiv_P generated by Σ where two strings coincide if and only if they can be derived from each other. The equivalence class of G is denoted as $\langle G \rangle_P$.

Example 3.2 In order to indicate how expressive SRS are, we sketch how to simulate any Turing machine using string rewriting rules, for details see the original paper by Post [42]. Consider a 1-tape Turing machine M with states $Q = \{q_0, \dots, q_n\}$ over $\Sigma = \{0, 1, \dots, g\}$. We can encode a configuration of the machine as a string over $\Sigma \cup \{ \$, \# \}$ as

$$q_0 \$; 0 ; \dots ; 0_1 | 0_0 0_1 \dots 0_n \#$$

where q_i is the current state, the head is on tape symbol 0_0 and $\$$ is the first tape cell which has not been visited yet in each direction. If $q_i \xrightarrow{a,b,c} q_j$, then this transition can be described by the four production rules

$$q_i 0_0 \rightarrow q_j 0_0, \quad q_i 0_0 \rightarrow q_i 0_0, \quad q_i 0_0 \rightarrow q_i 0_0, \quad q_i 0_0 \rightarrow q_i 0_0$$

and similarly for a move to the right. In this way one can construct a string rewriting system which mimics the behavior of M in a precise way when starting with the string $\$ q_0 G \#$. This easily implies that the statement $\langle G \rangle_P = H$ for given $\langle P \rangle = G \rightarrow H$ is undecidable; even for fixed P if a universal Turing machine M is used. It turns out that if M is deterministic, then this

translation still works if the reverse rules are included, so string equivalence with respect to a Thue system is also undecidable (in fact RE-complete).

In this sense Thue systems are too powerful to be useful as a complexity-theoretic lower bound, since Gröbner bases and ideal membership are computable (even in EXPSPACE). But if we move from strings (with non-commuting letters) to commutative strings, then the corresponding Thue systems do become decidable.

Definition 3.3 (Commutative Thue system). Let Σ be a finite alphabet, then (Σ^*, P) is the free commutative monoid over

$$\Sigma^* / \sim_P \quad \bullet \quad - \quad D \quad E \text{ if and only if } |D|_G = |E|_G \quad \bullet$$

A commutative Thue system is a Thue system (Σ^*, P) defined over commutative strings.

Convention: From now on only commutative Thue systems will be considered. When specifying P as a list of rules of the form

$$u \rightarrow v \quad ! \quad (\sim)$$

we implicitly always add the converse rules, too. We write $u \rightarrow_P v$ for a forward application of the rule and $v \rightarrow_P u$ for an application of the reverse rule, but we stress that \rightarrow_P is a symmetric relation. If the concrete derivation is not important, then we simply write $u \sim_P v$. If the Thue system is understood from the context, then we omit the subscript.

Remark. In the literature commutative Thue systems are defined as ordinary Thue systems containing the rules $GH \rightarrow HG$ for all $G, H \in \Sigma^*$, which is of course equivalent to our definition.

Commutative Thue systems can be understood as monomial replacement systems; this insight is a key ingredient in the reduction to the ideal membership problem. They also coincide with finite presentations of commutative semigroups in the following sense:

Example 3.4 (Commutative Thue systems are finite commutative monoid presentations). If (Σ^*, P) is a commutative Thue system over Σ , then $(\Sigma^* / \sim_P, \cdot)$ is a monoid generated by the classes of elements of Σ , and commutativity of the strings ensures that Σ^* / \sim_P is commutative. This commutative monoid coincides with the finitely presented monoid $\langle \Sigma \mid P \rangle$, since the relation \sim_P is the congruence relation generated by P (Lemma A.6).

Conversely, if $\langle \Sigma \mid R \rangle$ is a finitely presented monoid, then by adding the reverse rules we get a commutative Thue system P such that $\langle \Sigma \mid P \rangle \cong \langle \Sigma \mid R \rangle$.

We finally define the word problem for finitely presented commutative semigroups.

Definition 3.5 (Word problem for commutative semigroups, CSG).

Input: $\langle \Sigma \mid R \rangle$, where Σ is a finite set of symbols, R a list of generating congruences $f^1 \cdot g^{-1} \cdot h^2 \cdot i^{-1}$ and $g^2 \cdot h^{-1}$.

Output: Decide whether $g \sim_R h$ in the commutative semigroup $\langle \Sigma \mid R \rangle$.

derive G as desired:

$$I_a ?_g B_1 \dots B_n) I_a ?_1 B_1 \dots B_n) I_a ?_1 B_{-1} \dots B_{-n})) I_a ?_1 B_{-1} \dots B_{-n} = G$$

Conversely, assume $G) P_{n=}$ G and consider a repetition-free derivation

$$G = (0) (1)) < = G$$

As G contains I_a , there is a minimal $<_0 \geq 0$ such that $<_0$ contains I_a .

Claim: In this derivation $(0) P_{n=}$ $<_0$ only (forward) rules from M are applied.

Indeed, rules from (iii) and their converse are not applicable by minimality of $<_0$. Assume that a converse rule from M is used in some $(i+1) P_{n=}$ and choose i maximal with this property. $(i) < <_0$, as I_a does not occur on any left hand side in M (I_a is a final state), so $(i) P_{n=}$ applies a forward rule from M by maximality of i . We are in the following situation:

$$(i+1) (M : using I_a^{00} B_{0-8} I_a ?_g B_{0-8}) M :_{i+1} using I_a ?_g B_{0-8} I_a^{00} B_{0-8}$$

For any configuration there is (at most) a single applicable rule from M corresponding to the deterministic transition $\rightarrow \rightarrow \emptyset$. In this situation the rule is determined by (i) as both share I_a , $?_g$ and therefore B_{0-8} so the same production is applied and the reverse and forward application cancel each other. Thus $(i+1) = (i)$, but the derivation was assumed to be repetition-free, so no reverse rule could have been applied in the first place, proving the claim.

We have established that $G = (0) P_{n=}$ $<_0$ consists of forward rules from M corresponding to the behavior of \rightarrow on G . Since $<_0$ contains the accepting state, we see that $G \in L^*$ and the proof is complete.

If the function f is bounded by a polynomial, then this yields a polynomial-time reduction from L^* to the word problem for commutative semigroups.

Theorem 3.7 (CSG_n is PSPACE-hard). If $\in PSPACE$ then $\in P_m$ CSG_n, in particular CSG and CSG_n are PSPACE-hard.

Proof. Let $\in PSPACE$ be a language over $\{0,1\}$ and let \rightarrow be a deterministic 1-tape Turing machine deciding \in in space bounded by $f(n) = 2^n$. Let $(i) P_{n=}$ be the commutative presentation from the previous lemma (i.e. containing the rules (i) (iii)) for $\# = f(n) = 2^n$. Notice that by construction, all rules are homogeneous. The map

$$f(n) B^{-1} \rightarrow_j G^{-1} P_{n=} \rightarrow_j G^{-1} G^0$$

can be computed in deterministic polynomial time and reduces \in to CSG_n by Lemma 3.6.

It turns out that CSG is not in $PSPACE$, in contrast to CSG_n , but rather $EXPSPACE$ hard. Our approach here does not generalize to this case, as we need a variable for each tape cell and such an alphabet cannot be written down by a polynomial-time algorithm. On the other hand, non-homogeneous rules allow the derivation strings of superpolynomial length (compared to the input string and the set of rules), see section 3.4. Thus our next step is to find a model of computation whose configurations can be encoded with long strings from Σ^* for small n .

3.2 Counter machines

It turns out that a convenient model of computation to be simulated by commutative semi-group presentations are Counter machines. A classical reference is Minsky's book [36, Chapter 11 and 14], where these machines are called program machines (and use a slightly different instruction set). Informally, these are finite automata together with a fixed number of counters. The counters can be INCREASED, DECREASED or used to BRANCH the program flow on a ZERO. More formally:

Definition 3.8 (Counter machine). A counter machine with $k \geq 1$ counters is a tuple $(Q, \Sigma, \delta, q_0, q_f)$ where

- Q is a finite set of states
- δ is a transition function

$$\delta : Q \times \Sigma^k \rightarrow Q \times \Sigma^k \cup \{f, b, z\} \times \Sigma^k \cup \{f, b, z\} \times \Sigma^k \times \{0, 1\}$$

- $q_0 \in Q$ is the initial state and $q_f \in Q$ is the final/accepting state.

A configuration of M is described by the current state and the content of the k counters, i. e. a tuple in $Q \times \mathbb{N}^k$. The transition function is used to define the (unique) successive configuration as follows: Let $(q, (c_1, \dots, c_k))$ be the current configuration, $(q', (c'_1, \dots, c'_k))$.

- (i) If $(q, (c_1, \dots, c_k)) \in \delta^{-1}(op, (c'_1, \dots, c'_k))$ then the next configuration is

$$(q, (c_1, \dots, c_k)) \xrightarrow{op} (q', (c'_1, \dots, c'_k)) \quad \begin{cases} c'_9 = c_9 + 1 & \text{if } 8 = 9 \text{ and } op = INC \\ c'_9 = c_9 - 1 & \text{if } 8 = 9 \text{ and } op = DEC \\ c'_8 = c_8 & \text{if } 8 < 9 \end{cases}$$

- (ii) If $(q, (c_1, \dots, c_k)) \in \delta^{-1}(z, (c'_1, \dots, c'_k))$, the next configuration is

$$(q, (c_1, \dots, c_k)) \xrightarrow{z} (q', (c'_1, \dots, c'_k)) \quad \begin{cases} c'_9 = c_9 & \text{if } c_9 = 0 \\ c'_9 = c_9 - 1 & \text{if } c_9 > 0 \end{cases}$$

As usual, we denote the transitive and reflexive closure of the transition relation as \rightarrow^* .

Example 3.9 (Multiplication and division by 2). In this example we assume that counter 1 holds a non-negative integer and counter 2 is empty.

(i) We can move the content of counter 1 to counter 2 (emptying the former) and transition from state q_0 to q_1 with the following instructions:

$$q_0! \text{ BZ}_1 - q_1 - 0 \quad q_1! \text{ INC}_2 - 1 \quad q_1! \text{ DEQ} - q_2$$

This has the effect of $1q_0 - \#0^0 \rightarrow^* 1q_1 - 0 - \#0$.

(ii) We can similarly double the content of counter 1 if we increase twice instead of once:

$$q_2! \text{ BZ}_1 - q_3 - 2 \quad q_3! \text{ INC}_2 - 3 \quad q_3! \text{ INC}_2 - 4 \quad q_3! \text{ DEQ} - q_4$$

This has the effect of $1q_1 - \#0^0 \rightarrow^* 1q_3 - 0 - 2\#^0$. Using the copy instructions from (i) we can then move the result back to counter 1.

(iii) Using the same trick we can also halve the first counter and branch into q_{even} or q_{odd} depending on the remainder:

$$q_4! \text{ BZ}_1 - q_{\text{even}} - 5 \quad q_4! \text{ DEQ} - q_5 - 6 \quad q_5! \text{ BZ}_1 - q_{\text{odd}} - 0 \quad q_5! \text{ DEQ} - q_6 - 8 \quad q_6! \text{ INC}_2 - q_7$$

This has the effect of $1q_3 - 0 - \#0^0 \rightarrow^* 1q_{\text{even}} - 0 - \#0$ and $1q_3 - 0 - \#0^0 \rightarrow^* 1q_{\text{odd}} - 0 - \#0$ and we can again move the result back if desired. y

We say that the counter machine M accepts an input $\# = 2^k$ if and only if

$$1q_0 - \# - 0 - \dots - 0^0 \rightarrow^* 1q_1 - 0 - \dots - 0^0$$

Lemma 3.10 (Counter machines are Turing complete). For any Turing machine T on the input alphabet $\Sigma = \{0, 1\}$ there exists a 3-counter machine such that T halts on $G \Sigma^*$ if and only if M accepts the binary number $\# = 1G$.

A leading 1 is necessary to discriminate different strings that would otherwise describe the same binary number, for example 0 vs 00. The proof uses stack machines as an intermediary machine model, for our purposes, this is a finite state machine together with (in our case) two stacks (Σ_1, Σ_2) . Depending on the current state and the top symbols of the stacks (including observing an empty stack $\#$), the machine transitions into a unique successor state and can push and pop¹ single elements from both stacks:

$$(\sigma : \& \Sigma_1 \cup \{0, 1, \#\} \rightarrow \Sigma_1 \cup \{0, 1, \#\} \cup \{0, 1, \#\} \cup \{0, 1, \#\}) \& \Sigma_2 \cup \{0, 1, \#\} \rightarrow \Sigma_2 \cup \{0, 1, \#\} \cup \{0, 1, \#\} \cup \{0, 1, \#\}$$

¹A pop operation on an empty stack has no effect.

the input is encoded in a very specific way [36, Theorem 14.1-1].

The computation of φ on input $\# 2^j$ is said to be bounded by 2^j if the counters of all intermediate configurations $10\#0\cdots0$, $110\cdots0$ are in the range $0 \leq c_i \leq 2^j$. Notice that the construction in the previous lemma has the following property: If φ is operating in space $5^i = 0$, then the constructed counter machine will have its counters bounded by $2^{5^i + 1}$, as this is a bound on the number 1, where φ is the (binary) number spelled out on the tape.

Theorem 3.11 (EBC is EXPSPACE-complete). The language of exponentially bounded counter machines EBC is EXPSPACE-complete:

- Input: $\langle \varphi, n \rangle$, a 3-counter-machine
- Output: Decide whether φ accepts n and has computation bounded by 2^{2^j}

Proof. Step 1: EBC is in EXPSPACE

A Turing machine can easily simulate the configuration transitions. Each counter and the current state is stored as a binary number on a separate tape and the instructions INC-DEG can be executed using only the cells belonging to the counters. If the computation of φ is bounded by 2^{2^j} , then the space resources of this Turing machine are bounded by $3 \cdot 2^{2^j}$, which is exponential in the input length of $\langle \varphi, n \rangle$.

Step 2: $\text{EBC} \stackrel{P}{m}$ hard for all $2 \in \text{EXPSPACE}$

Let φ be a 1-tape machine deciding φ which visiting at most 2^{2^G} cells on the working tape on input G for some fixed $2 \leq G \in \mathbb{N}$. In order to show $\text{EBC} \stackrel{P}{m}$ we use the 3-counter machine constructed in the previous lemma. For $G \geq 1$ let φ_G be the following 3-counter machine:

- (i) Starting from φ use $\$ 1jG^0$ instructions to count 2_1 to the value $1G$ using the binary representation and the doubling algorithm from example 3.9.
- (ii) Then add the instructions from Lemma 3.10 to simulate the behavior of φ .
- (iii) Artificially enlarge the set of states φ & (if necessary) in order to ensure $2^{2^j} \leq 2^{2^G}$.

Then the computation of φ_G is bounded by $2^{2^{2^G} + 1} \leq 2^{2^{2^G}}$ and φ_G accepts 0 if and only if $G \in \varphi$. Step (ii) only depends on φ and not on G so the map $G \mapsto \varphi_G$ can be computed in polynomial time.

Remark. It may seem kind of arbitrary to consider the computation bounded by $2^{2^{2^j}}$. Indeed, if we require φ to have its computation bounded by 2^{2^j} instead, then this problem becomes PSPACE-complete.

3.3 Simulating counter machines with CSG

We now describe how to encode the behavior of a counter machine using commutative Thue systems. Let M be a counter machine whose computation is bounded by the number e , then a configuration of M is encoded over $\Sigma^0 = \{f_1, \dots, f_{2^e-2}, f_{2^e-1}, g\}$ as

$$\text{rep}^1 @_{-1} 2^e - 2^0 B @_{1}^{2^1} @_{2}^{e-2^1} @_{3}^{2^2} @_{3}^{e-2^2} @_{3}^{2^3} @_{3}^{e-2^3} 2^0 \bullet \tag{3.2}$$

This is essentially a unary representation of the counter values. The initial configuration is $B @_{1}^{e} @_{2}^{e} @_{3}^{e}$ and the terminal configuration is $B @_{1}^{e} @_{2}^{e} @_{3}^{e}$. We translate the function into congruence rules P^0 as follows:

(INC) If $1 @ = 1 \text{INC}_8 @$, then add the rule $@_8! @_8$.

(DEC) If $1 @ = 1 \text{INC}_8 @$, then add the rule $@_8! @_8$.

The 8 th counter is zero if and only if the configuration string contains 4_8 and nonzero if and only if it contains $_8$. Thus we can define

(BZ) If $1 @ = 1 \text{BZ}_8 @ @$, then add the rules $@_8^e! @_8^e$ and $@_8! @_8^0$.

Notice that the application of any rule to strings of the form (3.2) yields again a string of this form.

Lemma 3.12. Let $\Sigma^0 - P^0 - \Sigma$ be as above, then accepts^0 and has computation bounded by e and only if Σ^0 in the commutative semigroup $\Sigma^0 \cup \{P^0\}$.

Proof. Assume first that Σ has its computation bounded by 4 . If $1 @_{-1} 2^e - 2^0 \sim 1 @_{-1} 2^e - 2^0$, then $\text{rep}^1 @_{-1} 2^e - 2^0 \in P^0 \text{rep}^1 @_{-1} 2^e - 2^0$, hence by induction we obtain that $1 @_{-1} 2^e - 2^0 \sim 1 @_{-1} 2^e - 2^0$ implies $\Sigma \in P^0$.

Conversely assume $\Sigma \in P^0$ and consider a repetition-free derivation

$$= 0) P^0 (1) P^0 \dots) P^0 < = \bullet$$

The same argument as in the proof of Lemma 3.6 shows that this derivation only uses forward rules for (INC), (DEC), (BZ). This sequence of derivations hence describes the configuration transitions of M and witnesses that M accepts 0 with computation bounded by e .

Unfortunately, this does not immediately allow us to obtain a polynomial-time reduction $\text{EBC} \stackrel{P}{\sim} \text{CSG}$ since Σ and P^0 would have to contain the expression 2^{2^e} where $e = B \cup \{j\}$. We use the following result which will be proved in the next section:

Theorem 3.13 (Mayr & Meyer, 1982 [33]). For given n there exists a commutative semigroup presentation $\langle \Sigma \cup \{P\} \mid \dots \rangle$ of length $O(n^2)$ with the following properties:

Lemma 3.14. We have the following equivalences:

(i) $\mathcal{Q}_0 \stackrel{P}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} = \text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$ and $\mathcal{Q}_0 \stackrel{P}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} = \text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$.

(ii) If $\text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{P^0}{\sim} \text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$, then $\text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{P}{\sim} \text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$.

Proof. (i) This is a consequence of (0_0) (0_3) and Theorem 3.13:

$$\begin{aligned} \mathcal{Q}_0 \binom{0_0}{1} &\stackrel{(3.13)}{\sim} \mathcal{Q}_1 \binom{e_1}{1} \binom{0_1}{1} \stackrel{(3.13)}{\sim} \mathcal{Q}_2 \binom{e_1}{2} \binom{e_2}{1} \binom{0_2}{2} \stackrel{(3.13)}{\sim} \mathcal{Q}_3 \binom{e_1}{3} \binom{e_2}{2} \binom{e_3}{1} \\ &\stackrel{(0_2)}{\sim} \mathcal{Q}_3 \binom{e_1}{2} \binom{e_2}{1} \binom{e_3}{2} \stackrel{(3.13)}{\sim} \mathcal{Q}_3 \binom{e_1}{3} \binom{e_2}{2} \binom{e_3}{1} \stackrel{(0_3)}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \end{aligned}$$

The second derivation is completely analogous with (a_0) (a_3) instead.

(ii) P inherits all rules from P except for $\mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \rightarrow \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$. If this rule is applied in a derivation (say with $\delta = 1$) to $\text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{P^0}{\sim} \text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$, then we have

$$\begin{aligned} \text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} &= \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{(\&)}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{(3.13)}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{(\times)}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \\ &\stackrel{(3.13)}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{(\%) }{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} = \text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \end{aligned}$$

The difficult part is to prove that the inverse is also true: An equivalence of configurations by P implies the equivalence by P^0 . Consider the set of all possible configurations

$$\mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{P}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{P^0}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$$

Lemma 3.15. (i) Any derivation $\mathcal{Q}_0 \stackrel{P}{\sim} \mathcal{Q}_0$ contains $\text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$ and $\text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$.

(ii) For all $F \stackrel{P^0}{\sim} F'$, we have $F \stackrel{P}{\sim} F'$ if and only if $F \stackrel{P^0}{\sim} F'$.

With this result we can finally prove the promised hardness result for CSG

Theorem 3.16 (CSG is EXPSPACE-hard). The map $\mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \rightarrow \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$ defines a polynomial-time many-one reduction $\text{EBC} \stackrel{P}{\sim} \text{CSG}$. In particular, CSG is EXPSPACE-hard.

Proof. The map can clearly be computed in polynomial time (provided this is true for P , which we will see in the next section). If $\mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{P^0}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$, then $\text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{P^0}{\sim} \text{rep}^1 \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$ by Lemma 3.12 and consequently $\mathcal{Q}_0 \stackrel{P}{\sim} \mathcal{Q}_0$ by Lemma 3.14. Conversely, if $\mathcal{Q}_0 \stackrel{P}{\sim} \mathcal{Q}_0$, then by Lemma 3.15 and again Lemma 3.12 $\mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3} \stackrel{P^0}{\sim} \mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$.

Proof of Lemma 3.15. (i) Any derivation $\mathcal{Q}_0 \stackrel{P}{\sim} \mathcal{Q}_0$ must replace \mathcal{Q}_0 , the only rule allowing for this is (0_0) , introducing $\mathcal{Q}_1 \binom{e_1}{1}$. Only the rules (0_0) (0_3) and P are applicable until the first word containing some $\mathcal{Q} \binom{e_1}{1} \binom{e_2}{2} \binom{e_3}{3}$ is produced (which will be \mathcal{Q} by (0_3)).

In order to apply (O₁) the previous rules from P₌ must create a string containing $\alpha_1^{e_1}$, by 3.13 the only possibility being $\alpha_1^{e_1}$. If the derivation is repetition-free, then the only applicable rule now is (O₁), so the derivation has the form

$$\alpha_0^{(0_0)} \alpha_1^{e_1} \alpha_2^{e_2} \alpha_3^{e_3} \dots \alpha_n^{e_n}$$

Repeating this argument two more times shows that the word $\alpha_1^{e_1} \alpha_2^{e_2} \alpha_3^{e_3}$ must occur in the derivation $\alpha_0^{(0_0)} \alpha_1^{e_1}$. Essentially the same reasoning starting from $\alpha_0^{(0_0)}$ and using (a₀) (a₃) shows that $\alpha_1^{e_1} \alpha_2^{e_2} \alpha_3^{e_3}$ is contained in the derivation, too.

(ii) The backward implication was proven in Lemma 3.15, so assume $\alpha = \text{rep}^1 \alpha_1 \alpha_2 \alpha_3 \dots \alpha_n$. We proceed by induction on the length of a derivation, the case of length 0 being trivial. Consider a shortest (necessarily repetition-free) derivation

$$\alpha = \alpha_0^{(0_0)} \alpha_1^{e_1} \alpha_2^{e_2} \alpha_3^{e_3} \dots \alpha_n^{e_n}$$

and let $\alpha_0^{(0_0)} \alpha_1^{e_1}$ be the first step using one of the new rules (&), ..., (a₃). Then all previous steps in the derivation $\alpha_0^{(0_0)} \dots \alpha_1^{e_1}$ consists of rules from P⁰ (the rules from P₌ cannot be applied in the absence of $\alpha_1^{e_1}$), so $\alpha_0^{(0_0)} \alpha_1^{e_1} \in P^0$.

The only rules possibly applicable to $\alpha_0^{(0_0)} \alpha_1^{e_1}$ are (&), (%), (O₃), (a₃), as all other rules require the presence of symbols not in $\alpha_0^{(0_0)} \alpha_1^{e_1}$.

(O₃) Then $\alpha_0^{(0_0)} \alpha_1^{e_1}$ contains state α_0 which is replaced by α_3 , and hence the only rules applicable to $\alpha_0^{(0_0)} \alpha_1^{e_1}$ containing α_3 are rules from P₌. Theorem 3.13 tells us that P₌ can only be used to produce $\alpha_3^{e_3}$, furthermore, the maximum number e_3 of α_3 's are removed in this process (and so the string contains neither α_3 's nor α_3 's). Then the only applicable rule is (O₂) and we can repeat this argument twice to arrive at $\alpha_0^{(0_0)} \alpha_1^{e_1}$. Now the only applicable rule replaces this with $\alpha_0^{(0_0)}$ at which point no rule can be applied.

(a₃) The same line of reasoning prohibits the occurrence of this rule in a repetition-free derivation.

(&) Again only rules from P₌ can be applied to $\alpha_0^{(0_0)} \alpha_1^{e_1}$ and by applying Theorem 3.13 twice we must have

$$\alpha_0^{(0_0)} \alpha_1^{e_1} = \alpha_0^{(0_0)} \alpha_1^{e_1} \alpha_2^{e_2} \alpha_3^{e_3} \dots \alpha_n^{e_n}$$

where $\alpha_0^{(0_0)}$ is determined by $\alpha_0^{(0_0)}$ and F determined by $\alpha_1^{e_1}$. Hence $\alpha_0^{(0_0)} \alpha_1^{e_1} \in P^0$.

(%) The same argument yields $\alpha_0^{(0_0)} \alpha_1^{e_1} \alpha_2^{e_2} \alpha_3^{e_3} \dots \alpha_n^{e_n} \in P^0$.

By induction $\alpha_0^{(0_0)} \alpha_1^{e_1} \alpha_2^{e_2} \alpha_3^{e_3} \dots \alpha_n^{e_n} \in P^0$.

3.4 Producing words of double-exponential length

In this section we prove Theorem 3.13, we follow the exposition by Bayer & Stillman [4]. Let $e = B^{2^2}$. The alphabet Σ consists of $10^e = 10^{10^4}$ characters

$$\Sigma = \{ \emptyset, B, A^{-1}, A, B^{-1}, B, A^{-1}A^{-1}, A^{-1}A^{-2}, A^{-1}A^{-3}, A^{-1}A^{-4}, A^{-2}A^{-1}, A^{-2}A^{-2}, A^{-2}A^{-3}, A^{-2}A^{-4} \}$$

Definition 3.17 (Level of a word, box). The symbols in Σ_A are defined to be of level A . A word $F \in \Sigma^*$ is said to be of level A if all symbols in F are of level A and

$$|F|_{B_A}, |F|_{A^{-1}} = 1 - \sum_{g=1}^{\infty} |F|_{2_A^{-g}} = 1 - |F|_{B_g} = |F|_{A_g} = 0 \text{ for } g \geq A.$$

The set of level A words is Lvl^A / Lvl^{A-1} . If $F \in Lvl^A$, then denote by $box^A(F)$ the (unique) combination of B and A in G .

Notice that not all words are assigned a level. In order to ease notation, when writing A we use $(-)_g$ to denote the symbols of level A and B^{-1}_g for level $A-1$ respectively. The defining relations in $P =$ are defined inductively as follows: P_0 contains the four rules

$$B_{2_0^{-1}}! \quad B_{2_0^{-2}}! \quad B_{2_0^{-3}}! \quad B_{2_0^{-4}}! \quad (O_g)$$

For $A \geq 1$ define P_A to contain P_{A-1} and the ten rules

- (A) $(-)_A! \quad B_{2_A}!$
- (B) $B_{2_A}! \quad B_{2_A}!$
- (C_g) $B_{2_A}! \quad B_{2_A}! \quad B_{2_A}! \quad B_{2_A}! \quad B_{2_A}! \quad B_{2_A}! \quad B_{2_A}! \quad B_{2_A}! \quad B_{2_A}! \quad B_{2_A}!$
- (D) $B_{2_A}! \quad B_{2_A}!$
- (E) $B_{2_A}! \quad B_{2_A}!$
- (F) $B_{2_A}! \quad B_{2_A}!$
- (G) $B_{2_A}!$

The rules move words (of a given level) around in the boxes, this can be visualized as in figure 3.3. We first verify that the string $B_{2_A}^{e_A}$ (from level $A =$) can actually be derived from $(-)_g$ in the commutative Thue system defined by $P =$ over $\Sigma =$.

Lemma 3.18. For $A = 0, \dots, \infty$ and $B = 1, \dots, 4$ we have

$$B_{2_{B-A}}! \in P = B_{2_{B-A}}^{e_A} \quad (V)$$

	2_1	2_2	2_3	2_4
B	$10-0^0$	$14-0^0$	$14-0^0$	$10-0^0$
5	$14-0^0$	$14-0^0$	$14-0^0$	$14-0^0$

Table 3.1: Values of ϕ on the boxes, $4 \leq B \leq e_{A-1}$.

Lemma 3.21. Let $F \in \text{Lvl } A^0$ and assume Theorem 3.20(iii) is true in the case $A-1$. If there is a single $G_0 \in \text{Lvl } A-1^0 \setminus F$ such that the value $\phi(G_0)$ is according to ϕ in table 3.1, then this is true for all $G \in \text{Lvl } A-1^0 \setminus F$. The same is true for $G \in Q_{A^0}$.

Proof. Consider a simple path in $G^1 P_{A^0}$ from G_0 to $G \in \text{Lvl } A-1^0$. This path is an alternating sequence of segments of rules $P_A \cap P_{A-1}$ and of segments contained in $G^1 P_{A-1^0}$.

- ^ Rules (A) or (G) do not appear on the path, as this would result in a word without 2_{9-8} for $9 \leq A-1$, and no rule of P_A can be applied (except for (A) or (G) again but the path is simple).
- ^ Rules (B) (F) preserve being of level $A-1$ and also preserve correctness of table 3.1.
- ^ Segments in $G^1 P_{A-1^0}$ preserve being of level $A-1$ by Theorem 3.20(i) and must end in a word of level $A-1$. Theorem 3.20(iii) then shows that the start and end of this segment also respect the values in Table 3.1.

Thus, since the statement is true for G_0 and is preserved along the path, it holds true for G . The proof for $G \in Q_{A^0}$ is essentially the same, as rule (C) also respects the table.

Proof of Theorem 3.20 We proceed by induction on A starting with $A=0$. The arguments for $G \in Q_{A^0}$ only depend on the induction hypothesis for $G^1 P_{A^0}$, hence the start only needs to consider P_0 .

If F contains 2_{0-8} and B_0 or 5_0 , then there is at most one applicable rule, namely (O_8) in one direction. This rule clearly preserves the property of being of level 0. Since there is at most one applicable rule, we immediately get that the component of F is either a single word or a pair of words separated by one application of (O_8) , this proves both (ii) and (iii).

Now let $A \geq 1$ and assume that the Theorem is proven for the case $A-1$.

(i) Depending on whether F contains $($ or $)$, the rule (A) or (G) is the only applicable rule and yields a neighbor G_0 of level $A-1$. This word has $\phi(G_0) \in \{B_2-5_2\}$ and no 1_8 's, hence Lemma 3.21 holds true.

Let G be any word of level $A-1$ in the component of F . Any rule from P_{A-1} applied to G leads to words of level $A-1$ by induction hypothesis (i). Any rule from $P_{A-1} \cap P_A$ or (C) either leads to

- ^ a word F^0 of level $A-1$ (in the case of (B) (F), (C)) or

- ^ a word F^0 containing (or and no symbols of level $A - 1$ except possibly $1_1 \dots 1_{-1}$ (in the case of (A) or (G)). In this case we must have $\text{box}^1 G^0 \in \{B_2, 5_2\}$ and Lemma 3.21 tells us that G contains no 1_8 , so F^0 is of level A . Furthermore, in this case G is the only neighbor of F^0 .

Thus the words on any simple path in $G^1 P_A^0$ or $G^1 Q_A^0$ from F

$$F \rightarrow G_0 \rightarrow G \rightarrow F^0$$

are all of level $A - 1$ except possibly the last one being of level A (G is the only neighbor of F^0 , hence such a word cannot appear inside simple path). This proves (i) for $G^1 P_A^0$, in $G^1 Q_A^0$ we start at $F = ($, then F^0 must be a single (or as no rule of Q_A introduces other symbols of level A .

- (ii) Consider a simple cycle C in a component of (in $G^1 Q_A^0$, i. e.

$$G_0 \rightarrow_{P_A} G_1 \rightarrow_{P_A} \dots \rightarrow_{P_A} G_k = G_0 \quad \leftarrow \quad 2 \rightarrow G < G_9 \text{ for } 0 \leq 9 < 1.$$

Step 1: Translate into a statement purely about words of level $A - 1$.

The cycle C does not contain (or (having only a single neighbor), hence by (i) all G_i are in Lvl^{A-1} . At least one of the G_i must be of level $A - 1$, since otherwise no edges stemming from $Q_A \cap P_{A-1}$ are used and C is a cycle on a component of a level $A - 1$ word inside $G^1 P_{A-1}^0$, contradicting the induction hypothesis (ii) for $G^1 P_{A-1}^0$.

Let $H_0 = H_1 \dots H_k = H_0 \in \text{Lvl}^{A-1}$ be all words in C of level $A - 1$ (in order of appearance). As in the proof of Lemma 3.21 we see that H_i is joined to H_{i+1} by either a rule (B), (C), (D) (F) from $Q_A \cap P_{A-1}$ or $B_2 \rightarrow_{P_{A-1}} 5_2 \xrightarrow{e_A} 1_8$ (V) by hypothesis (iii).

Step 2: Put the H_i into boxes and observe the transitions.

Hence no H_i is in box B_2 or B_4 , as words in these boxes have only one outgoing edge (case (V)). By extension, no H_i is in box 5_2 or 5_4 , since otherwise one of H_{i+1} would necessarily be in box B_2 or B_4 . Hence all H_i lie in boxes $\{B_2, 5_2, 5_4, B_4\}$. We must have a sort of circular traversal of the boxes for the following reason:

- ^ If $\text{box}^1 H_0 \in \{B_2, B_4, 5_2\}$, then by inspection of (B) (F), (V)

$$\text{box}^1 H_{i+1} - \text{box}^1 H_i = \begin{cases} \in \{B_2, 5_2\} & \text{if } \text{box}^1 H_i \in \{B_2, 5_2\} \\ \in \{B_2, 5_2\} & \text{if } \text{box}^1 H_i = B_4 \end{cases}$$

- ^ If $\text{box}^1 H_0 = 5_2$, then by Lemma 3.21 $j H_{i+1} \rightarrow_j H_{i+2} = e_{A-1}$. The only applicable rule within the box is (C), trading 1_2 for 1_3 . The other rules are (D) (to box 5_2) and case (V) (to box B_2 , only applicable if $j H_{i+2} = e_{A-1}$). If (D) leads to, say, H_{i+1} , then the vertical rule (V) is

only applicable if $jH_{j-1}j_{13} = e_{A-1}$, hence H_j must be part of a sequence

$$H_1 \xrightarrow{(V)} H_{j-1} \xrightarrow{(C_\partial)} \dots \xrightarrow{(C_\partial)} H_j \xrightarrow{(C_\partial)} \dots \xrightarrow{(C_\partial)} H_{A-2} \xrightarrow{(D)} H_{A-1} \xrightarrow{(V)} H_A \bullet$$

e_{A-1} applications of (C_∂)

Step 3: Derive a contradiction from these observations.

These considerations show that the sequence of H_j 's must loop around the four boxes in a fixed direction, say $B_2 \{ 5_2 \{ 5_2 \{ B_2 \{ B_2$. Along such a loop, rule (D) is the only rule affecting 1_4 and it strictly increases the number $jH_{j-1}j_{14}$. But this is clearly impossible in a closed cycle, hence the component of $($ in $G^1Q_A^0$ contains no cycle.

Assume there is a simple cycle C in $G^1P_A^0$, then the homomorphism φ_A maps this to a cycle $\varphi_A^1C^0$ in $G^1Q_A^0$. $\varphi_A^1C^0$ is in the component of $\varphi_A^1F^0 \neq f(-g$, but this is the same component (Lemma 3.19). As any rule in P_A involves symbols not deleted by φ_A , $\varphi_A^1C^0$ is a non-trivial cycle in $G^1Q_A^0$, a contradiction.

(iii) The existence of a path $()_{Q_A}$ is Lemma 3.19, uniqueness is immediate from (ii), as distinct simple paths can be patched together to form a non-trivial cycle.

Let $G = H_2 L_{V_1} A^0$ be distinct with $G)_{P_A} H_1$, the uniqueness of such a path is again a consequence of (ii). Since there is a rule from P_A applicable to G we must have $G_2 L_{V_1} A^0$, the same is true for H . We must have $\varphi_A^1G < \varphi_A^1H$, since otherwise the path from G to H is mapped to a non-trivial cycle in $G^1Q_A^0$, contradicting (ii). Without loss of generality, let $\varphi_A^1G = (, \varphi_A^1H =)$.

Let $\text{box}^1G = (\&_8$, then $\text{box}^1H = \&_8$ as all rules of P_A preserve the level A symbol $\&_8$. The image of the path in $G^1Q_A^0$ is a path from $($ to $)$, hence the unique sequence of derivations from Lemma 3.19. This information together with the presence of $\&_8$ (and no other $\&_9$) allows us to conclude that the path from G to H uses the sequence of derivations from Lemma 3.18. In particular, if $G = (\&_8$, then $H = \&_8 \overset{e_8}{\&_8}$.

Theorem 3.13 is now an easy consequence:

Proof of theorem 3.13 The presentation $h = j P_{=} i$ is of length $\$ 1^=0$ with $10^1 = , 1^0$ variables and $10 = , 4$ relations of length 9 (the longest being (C_∂)).

If $(\&_8)_{P_{=}} F$ such that F contains $)$, then F is of level $=$ and Theorem 3.20(iii) says that

$$(\&_8 = (\&_8 - F = \&_8 \overset{e_8}{\&_8} = \&_8 \overset{e_8}{\&_8} \bullet$$

The proof of the second claim in Theorem 3.13 is analogous.

Remark. While we mostly care about $P_{=}$ and the derivation $(\&_8)_{P_A} \&_8 \overset{e_8}{\&_8}$, the structure of $G^1Q_A^0$ is used crucially in the final step of the argument. This is one explanation to why we

took the extra mile to introduce Q_A and prove statements for both graphs. Another reason is that Q_A is useful for proving degree lower bounds on the ideal membership, see below.

We also remark that this construction has been dramatically improved by Yap from 10^8 , O^{11^0} variables down to only 2^8 , O^{11^0} [47]. Furthermore, if rule (O_g) contains 1_{0-8}^3 instead of 1_{0-8}^2 then the same construction yields a commutative Thue system which can count to 3^{2^8} [4].

3.5 Hardness of the ideal membership problem

We now reduce CSG to the ideal membership problem (over an arbitrary field \mathbb{K}). Let (P, \mathcal{G}) be a tuple as in Definition 3.5, $\mathcal{G} = \{G_1, \dots, G_m\}$, $P = \{p_1, \dots, p_n\}$. To a word $\alpha = i_1 \dots i_m$ we associate the monomial $B^\alpha = \prod_{j=1}^m B_j^{i_j}$. The corresponding input to IM_K is the set of polynomials $\{B^\alpha - p_\alpha\}$ with

$$B^\alpha - p_\alpha = \sum_{j=1}^m B_j^{i_j} - p_\alpha = 1 - \dots - B^\bullet$$

As these polynomials have coefficients in \mathbb{F}_2 , these polynomials are defined over any field (or ring).

Theorem 3.22. With the preceding notation, the following statements are equivalent:

- (a) $P \in \langle \mathcal{G} \rangle$;
- (b) $\exists \mathbb{K} \ni B^\alpha - p_\alpha \in \langle \mathcal{G} \rangle_{\mathbb{K}}$;
- (c) $\exists \mathbb{K} \ni B^\alpha - p_\alpha \in \langle \mathcal{G} \rangle_{\mathbb{K}}$ for any field \mathbb{K} .

Proof. (a) (b): Consider a derivation of length $\#$

$$= (0) P_1) P_2) \dots P_{\#} = \bullet$$

Each step corresponds to an application of a rule G_i from \mathcal{G} such that

$$: 1 = \$: G_i - : = \$: G_i - \$: 2 - : = 1 - \dots - \# \bullet$$

Thus we get a telescoping sum

$$- \dots - = \sum_{i=1}^{\#} \{ Z_i - Z_{i+1} \} = Z_{\#} - Z_1 = \bullet$$

- (b) (c): Any \mathbb{K} -linear combination is valid over an arbitrary field \mathbb{K} .
- (c) (a): This is the most difficult implication. Our strategy is to consider the fields \mathbb{F}_2 and \mathbb{F}_3 (prime) first, and then generalize to arbitrary fields.

Step 1. $\langle = \prime$. Consider a linear combination

$$5 = \begin{matrix} \tilde{O} \\ 6: 5_3 - \\ 6: 2' \gg \frac{1}{4} \\ \vdots \end{matrix} \tag{3.3}$$

Let $3 \cdot 2 \cdot \tilde{Z}_{70}$ be a common denominator of all coefficients of all $6:$, then $36: 2 \cdot \tilde{s} \gg \frac{1}{4}$. By artificially increasing the number of summands in (3.3), we may assume that all $36:$ are monomials with coefficient 1, for example

$$36: = 3- \cdot 2 \cdot 2, 2 \{ - \cdot, - \cdot, - \cdot \cdot^2 \cdot^2, 1, 1 \bullet$$

Thus we obtain a (potentially much larger) sum

$$3- \cdot 3- = \begin{matrix} \tilde{G} \\ 1 \cdot 1^0 : - \$: 1- \cdot 9 - \cdot 9 \bullet \\ \vdots = 1 \end{matrix} \tag{3.4}$$

We claim that there is a derivation $\langle \rangle_P$ of length at most $\#$. Indeed, since the term $-$ occurs on the left side of (3.4), this monomial must occur in one of the summands, i. e. $- \cdot \$ < 1- \cdot 9 - \cdot 9 \bullet = - \cdot 1 -$. Removing this summand yields

$$3- \cdot 1 \cdot 3 \cdot 1^0- \cdot - \cdot 1 = \begin{matrix} \tilde{G} \\ 1 \cdot 1^0 : - \$: 1- \cdot 9 - \cdot 9 \bullet \\ \vdots = 1- \cdot < < \end{matrix} \tag{3.5}$$

such that $\langle \rangle_P \cdot 1$ by application of the rule $9 \cdot 9$. If $1 =$ then we are done, otherwise apply the same reasoning to the monomial $- \cdot 1$ to inductively obtain $2- \cdot 3- \bullet \bullet \bullet$. This process ends after at most $\#_0 \cdot \#$ steps with $\#_0 =$, since each step removes a summand from (3.4).

Step 2. $\langle = \dagger ?$. Here nearly the same proof applies: Take a linear combination as in (3.3), this time over $\dagger ? \gg \frac{1}{4}$ then we can interpret the $6:$ as some polynomials with integer coefficients (being unique modulo $?$). We can again rewrite this sum as in (3.4), this time with $3 = 1$ (no need to kill denominators). Then the same replacement scheme yields a sequence $\langle \rangle_P \cdot 1 \rangle_P \cdot 2 \bullet \bullet \bullet$. The left hand side always reads $- \cdot - \cdot 9$ at each step, so no cancellation can happen (even mod $?$) unless $9 =$ after at most $\#$ steps and we obtain a derivation $\langle \rangle_P \cdot$.

Step 3. \langle arbitrary. Any field contains either \prime or some $\dagger ?$, its so-called prime field. All polynomials considered are defined over the prime field, so Lemma A.2 shows that $5 \cdot 2 \cdot \langle$ already implies \prime or $\dagger ?$ respectively, so by the previous two cases $\langle \rangle_P \cdot$.

This shows that the equivalence relation $\langle \rangle_P$ is basically the relation $\langle \rangle$ from Lemma 1.34 on monomials. In this way we get a reduction from commutative semigroups to polynomial ideals.

Theorem 3.23 (CSG reduces to IM_{\leq}). We have $CSG \stackrel{P}{m} IM_{\leq}$ for any field \mathcal{K} (and even for $\mathcal{K} = \mathbb{Z}$). This is also true for the homogeneous variants, $CSG_h \stackrel{P}{m} IM_{h \leq}$.

Proof. Indeed, the previous theorem shows

$$IM_{\leq} \stackrel{P}{m} CSG \text{ if and only if } IM_{h \leq} \stackrel{P}{m} CSG_h.$$

Moreover the reduction mapping is computationally trivial, regardless of the encoding of coefficients (the only coefficients required are two constants ± 1) or monomials (the total degree is bounded).

For the second statement it suffices to notice that the $\mathbb{Z}[x_1, \dots, x_n]$ are homogeneous if P consists of homogeneous congruence rules.

Together with the previous hardness results and the upper bounds from section 2.6 we see:

Corollary 3.24. The problem IM_{\leq} is EXPSPACE-hard and $CSG \stackrel{P}{m} IM_{\leq}$ are EXPSPACE-complete. The homogeneous variant $IM_{h \leq}$ is PSPACE-hard and $CSG_h \stackrel{P}{m} IM_{h \leq}$ are PSPACE-complete.

It is interesting to consider the analogous problem in the context of algebraic complexity theory. Bürgisser has adapted these techniques to prove analogous results for algebraic circuits.

Theorem 3.25 (Bürgisser 1998 [9]). For any infinite field \mathcal{K} there is a constant c such that any sequence of algebraic circuits $\{C_n\}_{n \geq 0}$ deciding IM_{\leq} has $\text{depth}(C_n) \leq c \cdot 2^n$ for $n \geq 0$.

Remark. Recall the Hermann bound which states that if $f = \sum_{\alpha \in \mathbb{N}^n} a_{\alpha} x^{\alpha}$, then the a_{α} may be chosen of degree $\deg f + \sum_{i=1}^n \deg x_i^{\alpha_i}$. The results from the previous section show that this bound is asymptotically tight as follows: We have seen that there is a unique derivation $(\partial_{\alpha})_{\alpha \in \mathbb{N}^n}$ which contains words of length $\leq n$. This corresponds to a polynomial equation $(\partial_{\alpha} f)_{\alpha \in \mathbb{N}^n} = 0$ and the proof of 3.22 shows that the degree of any term $\partial_{\alpha} f$ gives an upper bound on the length of words in the derivation. Thus, any such $\partial_{\alpha} f$ must have degree double-exponential in n , for details see the paper by Bayer & Stillman [4, Theorem 2.4].

3.6 Church-Rosser systems

We return to the topic of Gröbner bases. The previous section gave a connection between commutative semigroup presentations and binomial ideals. We now extend this connection and define a notion analogous to Gröbner bases, following the paper by Huynh [21]. Fix a monomial order \prec on Mon_{Σ} and consider a commutative Thue system P .

Definition 3.26 ((Ir)reducible words). Let $P = \{l_i \rightarrow r_i\}_{i \in I}$; A, g . A word $G \in \text{Mon}_{\Sigma}$ is reducible with respect to P if $G = H l_i$ for some $H \in \text{Mon}_{\Sigma}$, and irreducible otherwise. The transformation $G \rightarrow H r_i$ is called a reduction step. y

Notice that if $G \equiv_P H$, then by the defining property of a monomial order, $G \equiv_H A s$ is a well-order, any sequence of reduction steps must be of finite length and hence every word is equivalent to an irreducible word with respect to P . Of course, such an irreducible word is generally not unique, similarly to how normal forms of polynomials are not unique. But we have seen that this does not happen for Gröbner bases (Theorem 1.18(b)), so we use this to define an analogous notion for commutative Thue systems.

Definition 3.27 (Church-Rosser system, reduced). A commutative Thue-system $\langle \Sigma, P \rangle$ is a Church-Rosser system if for any two words $D \equiv_P E$, both irreducible with respect to P , we have $D = E$.

A Church-Rosser system is reduced if for all $u, v \in \Sigma^*$ both u, v are irreducible with respect to P and $u \equiv v$ implies $u = v$.

We use the notation from the previous section to translate commutative Thue systems into ideal generators.

Theorem 3.28. Let P be a commutative Thue system and

$$I = \langle \sum_{i=1}^n a_i x_i - b_i \mid a_i, b_i \in \Sigma^* \rangle$$

Then P is a Church-Rosser system if and only if I is a Gröbner basis of $B(\Sigma)$. Furthermore, P is reduced if and only if I is reduced.

Proof. Assume first that I is a Gröbner basis. Let $D \equiv_P E$, D, E both irreducible with respect to P . Then D and E are in normal form with respect to I (compare Definition 1.14), and hence $NF_{I, \prec} D = D$, $NF_{I, \prec} E = E$, as I is a Gröbner basis. Theorem 1.34 tells us that both D and E are the unique minimal element of their equivalence classes with respect to I . But by assumption $D \equiv_P E$, by Theorem 3.22 we have $D \equiv E$, and so they must coincide.

Now assume that P is a Church-Rosser system. Let $D \equiv E$ and assume D were irreducible with respect to P . Theorem 1.34 yields a $u \in \Sigma^*$ such that $D \equiv u$. Theorem 3.22 implies that $u \equiv_P E$, and after applying a finite number of reduction steps we obtain $u \equiv_P E$ with E irreducible, too. So $D \equiv_P E$ and both are irreducible, by the Church-Rosser property we have $D = E$, which contradicts $D \equiv E$. Hence there is a $u, v \in \Sigma^*$ with $u \equiv v$ and $u \equiv_P v$, and I is a Gröbner basis by characterization 1.18(a).

It is immediate from the definitions that I is reduced if and only if P is reduced.

Corollary 3.29. For every congruence relation \equiv there exists a unique Church-Rosser system P with $\equiv_P = \equiv$.

Proof. There exists some commutative semigroup presentation P_0 with $\Sigma = \Sigma_{P_0}$ by Rédei's theorem A.7. Let $I = \langle \sum_{i=1}^n a_i x_i - b_i \mid a_i, b_i \in \Sigma_{P_0} \rangle$ and let I be the reduced Gröbner basis of

. Then $P = \{f^1; \dots; f^k\}$ is a Church-Rosser system equivalent to P_0 . Uniqueness follows immediately from the uniqueness of reduced Gröbner bases.

We now translate some notation and results from the polynomial world to the land of Thue systems. Fix a commutative Thue system P .

Definition 3.30. For a word $D \in \Sigma^*$ let $NF_P^{-1}(D)$ be the minimal word in Σ^* with respect to \sim_P . We define the sets

$$\text{Min}_P = \{D \in \Sigma^* \mid NF_P^{-1}(D) = D\} \quad \text{and} \quad \text{Red}_P = \Sigma^* \setminus \text{Min}_P.$$

We denote the minimal elements of a set S with respect to string containment by $\min S$.

Lemma 3.31. Let P be a reduced Church-Rosser system.

- (i) Red_P is the set of elements reducible with respect to P .
- (ii) $\text{Min}_P = \{f^1; \dots; f^k\}$.

Proof. As P is a Church-Rosser system, a string $D \in \Sigma^*$ is irreducible with respect to P if and only if it is minimal in its congruence class Σ^*/\sim_P , i. e. in Min_P . This proves the first statement, the second statement is a direct translation of Theorem 1.32.

3.7 The size of a reduced Gröbner basis

In this section we restrict ourselves to a degree-dominating monomial order with the property

$$|D| \geq |E| \Rightarrow D \succ E.$$

For example grlex and grevlex have this property, but lex does not.

Theorem 3.32 (Huynh 1986 [21]). For each n there exists an ideal I_n generated by $O(n^2)$ differences of monomials of total degree $O(n)$ with the following properties:

Any Gröbner basis of I_n has at least 2^{2^n} elements and the maximal total degree of its elements is at least 2^{2^n} .

By Corollary 1.29 the equivalence of reduced Church-Rosser systems and reduced Gröbner bases of pure difference ideals, it suffices to prove the analogous statement for Church-Rosser systems:

Theorem 3.33. For each n there exists a commutative Thue system P_n generated by $O(n^2)$ rules of length $O(n)$ with the following properties:

The reduced Church-Rosser system generating the same congruence has at least 2^{2^n} elements and the maximal length of one side of the rules is 2^{2^n} .

To prove this, we follow the strategy of Huynh [21], but we simplify the construction of a system R_{\neq} with the following property:

Lemma 3.34. Let $D = A(\ 3\ 4\ 5\ 2\)$ with $4, 5 = e_{\neq}$. Then D is not minimal in $\gg D \gg_{R_{\neq}}$ with respect to \neq , but any proper substring $D^0 j$ D is the minimal element of $\gg D^0 j \gg_{R_{\neq}}$.

We first show that this property implies the theorem.

Proof of Theorem 3.33. Consider the $e_{\neq}, 1$ distinct words $D, B = A(\ 3\ 1\ 2\)^{e_{\neq}}$, $\neq = 0 \dots e_{\neq}$, each of length $e_{\neq}, 2$. By Lemma 3.34 each $D, 2 \gg_{R_{\neq}}$ is a minimal element of this set, and hence by Lemma 3.31 we have

$$f D_0 \dots e_{\neq} D g \quad f ; j 1 ; - A 2 P g$$

where P is the reduced Church-Rosser system equivalent to R_{\neq} . Hence $|P| \geq e_{\neq}$ and P contains rules of length $\geq e_{\neq}$.

We now construct R_{\neq} : Recall the construction of $\neq = P_{\neq}^0$ from section 3.4, then the alphabet is $\neq = \{A, A^0, A^0 c_1, c_2\}$ and R_{\neq} consists of P_{\neq} and the additional rules

$$\begin{aligned} A\ 3\ 1\ !\ A\ 3\ c_1\ 4\ & \quad A\ 3\ 2\ !\ A\ 3\ c_2\ 4\ & (R) \\ A\ 3\ !\ A^0\ 1\ & (R_1^0) \\ A^0\ c_1\ !\ A^0\ 3\ & (R_2^0) \\ A\ 3\ !\ A^{00}\ 4\ & (R_1^{00}) \\ A^0\ c_2\ !\ A^0\ c_1\ \bullet & (R_2^{00}) \end{aligned}$$

The rules and their intended behavior is visualized in Figure 3.4. The proof of Lemma 3.34 makes use of the properties of P_{\neq} from Theorem 3.13, and the additional fact that in the derivation $\neq V g^0(\ 3\) \neq \neq$ any intermediate expression has length ≥ 3 .

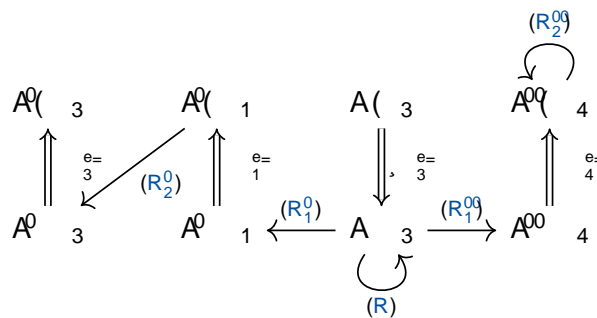


Figure 3.4: A visualization of the rules in R_{\neq} .

Proof of Lemma 3.34 Let $D = A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix})$ and assume first that $4, 5 = e_3$, then

$$D \stackrel{(V_3^0)}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(R)}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(R_1^{00})}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(V_4^0)}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(R_2^{00})}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(R)}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix})$$

This shows that all such D are equivalent to $A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix})$. We then have

$$A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(R_1^0)}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(V_1^0)}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(R_2^0)}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix}) \stackrel{(V_3^0)}{=} A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix})$$

and since $|D| = 7$, we have $D \notin \mathcal{M}$, so D is not minimal in its equivalence class.

Now consider any proper substring D^0 of D . If D^0 does not contain A , then only rules from P_3 , leading to strictly longer words. If D^0 does not contain $(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix})$, then no rule is applicable at all and $\text{rank}(D^0) = \text{rank}(D)$, so D^0 is trivially minimal. Hence we may assume $D^0 = A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix})$. In order to prove minimality it suffices to show that for any $E < D^0$ with $E \in \mathcal{M}$ we have $|E| > |D^0|$, as this implies $E \notin \mathcal{M}$.

Consider a repetition-free derivation from D^0 to E , the prefix of E is the substring of E of the form $A^j A^i A^k A^l A^m A^n A^p A^q A^r A^s A^t A^u A^v A^w A^x A^y A^z A^{\dots}$ (the structure of \mathcal{M} easily implies that A contains at most one such word). Then P_3 (in the form of Theorem 3.13) and (R) (R_2^{00}) imply that the only possible transitions between words of different prefixes behave as displayed in Figure 3.4.

First assume that the derivation uses (parts of) (V_1) or (V_4) , and let E^0 be word in the derivation prior to the first such step. The rules $(R), (R_1^0), (R_1^{00})$ and the transformation (V_3) leave the numbers

$$\#_E = |E|_1, |E|_2, |E|_3, |E|_4 - \#_E = |E|_1, |E|_2, |E|_3, |E|_4$$

invariant, so $\#_{E^0} = \#_D = 4, 5 = e_3, \#_{E^0} = 0$. In particular $|E^0|_1 - |E^0|_4 = 5 = e_3$, so neither (V_1) nor (V_4) can ever be completely applied.

The derivation $D^0 \rightarrow E$ necessarily starts by following the unique derivation in P_3 from $A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix})$ to $D^{00} B A(\begin{smallmatrix} 3 & 4 & 5 \\ 1 & 2 & 3 \end{smallmatrix})$. Any intermediate word is strictly longer than D^0 . We have $|D^{00}| = |D^0| + e_3$, and it is not hard to see that $(R), (R_1^0), (R_1^{00})$ and parts of the derivations $(V_1), (V_4)$ only lead to words of length $> |D^{00}| + e_3 = |D^0| + 2e_3$. We conclude that $E = D^0$ or $|E| > |D^0|$ and hence D^0 is minimal in its equivalence class.

In chapter 2 we have seen that upper bounds on the degree of Gröbner bases of homogeneous ideals lead to upper bounds on the degree of arbitrary ideals (Lemma 2.15). Conversely, lower bounds for arbitrary ideals also apply to homogeneous ideals, in particular Theorem 3.32 also holds for homogeneous ideals. Mayr & Ritscher also gave some lower bounds depending on the dimension of the ideal.

Theorem 3.35. There are a monomial ordering and a family of ideals $\langle \dots \rangle$ of dimension

By Theorem 3.32, for all $n \in \mathbb{N}$, there exist polynomials of degrees bounded by n such that each Gröbner basis has a maximal degree of at least 2^{2^n} for any $n \geq 0$ and sufficiently large n .

This shows that the upper bound from Theorem 2.17 is somewhat tight, in particular the degree of Gröbner bases may be loosely described as 2^{2^n} .

3.8 Hardness results of Gröbner bases

We will now prove some results on the complexity of Gröbner bases. Fix a monomial order which is degree-dominating.

Theorem 3.36. Any algorithm which on input $\langle n, f_1, \dots, f_m \rangle$ computes the reduced Gröbner basis of $\langle f_i \rangle$ with respect to grlex uses in the worst case at least space 2^{2^n} and time $2^{2^{2^n}}$ in the length of n . This is independent of the base of the encoding of field elements or whether binary or unary exponent representation of the monomials is used. This also holds true when restricting homogeneous ideals.

Proof. Indeed, the polynomials from Theorem 3.32 are differences of monomials and hence use coefficients $\in \{0, -1\}$. Furthermore, the terms have bounded degree $\leq n$, so dense or sparse encoding of the monomials does not change the input length up to a constant factor.

The output consists of $2^{2^n} = e_n$ different polynomials, so the algorithm requires at least e_n steps and passes through at least e_n different configurations of the work tape. This implies that at least 2^n work tape cells have to be visited in order to represent e_n different configurations.

This lower bound matches the space and time requirements of Theorem 2.29 (for $\langle = \rangle$).

Remark. We have seen that the size of the output of the Turing machine dictates a lower bound on the resources used by said machine. This is however not enough to prove that the individual elements of the output are hard to describe. For example, consider the function

$$f_n = 10^{-1} - 2^{-2} - \dots - 2^{-2^n} - 10^{-1}$$

where numbers are encoded in binary. Then the length $|f_n|$ is exponential in n and hence double-exponential in $\lfloor \log |f_n| \rfloor$, but on the other hand it is computationally trivial to decide whether $\langle 2^{-j} \rangle$ is part of the list $f_n = 0$. This is not true in the case of the reduced Gröbner basis, as shown next.

Theorem 3.37 (GROEBM is EXPSPACE-hard). The problem to decide whether a given polynomial f is a member of the reduced Gröbner basis of $\langle f_1, \dots, f_m \rangle$ is hard for EXPSPACE regardless of the specified monomial order.

Proof. The reduction $EBC \stackrel{P}{m} CSG \stackrel{P}{m} IM_k$ shows that IM_k is EXPSPACE-hard even when restricting to the following subset \mathcal{S} :

- The polynomials f_1, \dots, f_m are differences of monomials of positive degree.
- The polynomial h whose membership has to be decided is of the form $h = G - H$, $G \in \mathcal{S}$.

After renumbering the variables we may assume that $G < H$ for all $G \in \mathcal{S}$, i.e. H is the smallest variable with respect to $<$. This implies that H is also the smallest monomial different from 1: Any monomial $<$ contains some variable G , and hence $< G < H$. Moreover $1 \leq < < 1$ for any monomial $< < 1$, since the f_i have positive degree (in Thue system language: No rule is applicable to the empty string).

Let $\mathcal{I} = \langle f_1, \dots, f_m \rangle$ be an ideal generated by pure differences and \mathcal{S} the reduced Gröbner basis of \mathcal{I} . With this notation we claim

$$G \in \mathcal{S} \iff G \in \mathcal{I} \text{ if and only if } G \in \mathcal{S}.$$

If $G \in \mathcal{S}$, then surely $G \in \mathcal{I}$, as $G \in \mathcal{S}$. Conversely, assume $G \in \mathcal{I}$, then Theorem 1.34 shows that $NF_{\mathcal{I}}(G) = H$ and H is the smallest monomial in $\text{Mon}_{\mathbb{Z}} \setminus \{1\}$. The monomial G is minimally reducible with respect to $<$ (Definition 1.31), as it is reducible ($NF_{\mathcal{I}}(G) = H < G$), but its only proper divisor 1 is irreducible. Then Theorem 1.32 shows that $G \in \mathcal{S}$.

This proves $\stackrel{P}{m} \text{GROEBM}$, where the reduction function is the identity map, so GROEBM is EXPSPACE-hard, too.

Combining this with the exponential space algorithm for reduced Gröbner basis membership from chapter 2 yields the following completeness result:

Corollary 3.38. The problem GROEBM is EXPSPACE-complete.

Remark. The hardness result of GROEBM is implicitly contained in the literature, although not mentioned explicitly (to the knowledge of the author). The phrase “Gröbner bases are EXPSPACE-complete” mostly refers to the results of Theorem 2.29 and 3.36.

We close our discussion on the complexity of Gröbner bases with a recent result due to Rolnick & Spencer which shows that Gröbner bases are hard to approximate. Let $\epsilon \in (0, 1)$ be a constant and define the ϵ -Fractional Gröbner problem as follows:

- Input: $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ polynomials
- Output: (α, β) , where $\alpha \in [0, 1]$ with $\beta \in \mathbb{Z}$ and β is a Gröbner basis of $\langle f_i \rangle$

Theorem 3.39 (Rolnick & Spencer 2018 [46]). For infinite fields \mathbb{K} , the ϵ -Fractional Gröbner problem is NP-hard for every fixed $\epsilon \in (0, 1)$. This is true for any monomial order and even when the polynomials are of degree 3.

The authors remark that this holds true even if polynomial time is measured not only in the size of the input, but also on the output [46, Theorem 3]. This is remarkable, since we know that Gröbner bases may become exceedingly large even for small inputs.

Conclusion

In this thesis we discussed the polynomial ideal membership and its connection to Gröbner bases. We have seen how Gröbner bases can be constructed using Buchberger's algorithm and how the multivariate division algorithm calculates normal forms which can be used to ideal membership. Although this approach is successful in many cases, especially with improved algorithms such as Faugère's F_5 algorithm, the worst-case complexity points to the limitations of Gröbner bases.

We have seen that both the ideal membership problem IM as well as the reduced Gröbner basis membership problem $GROEBM$ are $EXPSPACE$ complete, in particular both problems are computationally very involved in their full generality. While it is intuitively clear that Gröbner bases must be at least as complex as the problem they are trying to solve (in an appropriate sense), the other results surveyed here suggest that they are sub-optimal in many important cases. Namely, the ideal membership problem for homogeneous polynomials $IM_{h,d}$ is $PSPACE$ complete, but Gröbner basis computation for homogeneous ideals still requires exponential space in the worst case. Even worse, the number and degree of elements in a Gröbner basis of a homogeneous ideal may be double-exponential in the number of variables and generators of the ideal. Still, in many practical cases Gröbner bases are a good first choice for problems in computer algebra.

There are many other interesting topics related to the ideas presented here, we would like to point to three particular ones.

- ^ When presented with a problem involving Gröbner basis computation, it is often difficult to estimate whether the computation will be a matter of minutes or months. Hence an important question is: What properties of an ideal make their Gröbner basis complicated? This is particularly important for applications in computational algebraic geometry, where many problems can be reduced to a Gröbner basis computation of some sort. We have seen that the number of variables and the dimension play a role both for the complexity of the ideal membership as well as the size of the reduced Gröbner basis. An important piece of the puzzle is the regularity of the ideal, a notion which is explored in the paper by Bayer & Mumford [3].
- ^ Gröbner bases provide an approach to calculate normal forms of polynomials with respect to an ideal. If the system of polynomials has a finite number of solutions and is sufficiently general, then the set of solutions is closely connected to the quotient ring

$f \gg \frac{1}{4} \cdot 5 - \dots - 5$ for example its dimension over f is the number of solutions. Normal forms provide a way to compute effectively in this ring, see for example the truncated normal form by Telen [38]. For an analysis of the performance of several normal form algorithms see the work of Parkinson et. al [41].

- ^ While symbolic computations on systems of polynomial equations are important, for many applications approximations to solutions are sufficient, especially for large systems. One of the most successful techniques is homotopy continuation, where a system of equations with known solutions is continuously transformed into the target system, and the solution paths are tracked. A particular implementation, which allows for certifying zeros (i. e. providing a certificate that a given approximate zero corresponds to an actual solution in $f^=$) is [HomotopyContinuation.jl](#) [6].

A

Appendix

A.1 Commutative Algebra

All rings in this thesis are assumed to be commutative and with unity. An ideal of a ring is an additive subgroup closed under multiplication with elements from R , i.e. $0 \in I$ for $0 \in R$. If S is a subset, then the ideal generated by S is

$$\langle S \rangle = \{ \sum_{i=1}^n r_i s_i \mid r_i \in R, s_i \in S \}$$

this is the smallest ideal containing S and S is a generating set. If $I = \langle s \rangle$ then we write $I = (s)$. An ideal of the form (s) is a principal ideal.

A ring R is Noetherian if one of the following equivalent conditions is satisfied [24, Thm. 2.9]

- (i) Any generating set of an ideal contains a finite generating set.
- (i') Every ideal of R admits a finite generating set.
- (ii) R satisfies the ascending chain condition on ideals: Any chain of ideals $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ eventually becomes stationary: $I_n = I_{n+1} = \dots$ for all $n \geq n_0$.
- (iii) Any nonempty set of ideals in R has a maximal element with respect to inclusion.

The most important ring for our purposes is the ring of polynomials in a set of indeterminates over a field K . A classical result asserts that this is a Noetherian ring.

Theorem A.1 (Hilbert basis theorem). If R is a Noetherian ring, then so is $R[x_1, \dots, x_n]$. In particular $K[x_1, \dots, x_n]$ is a Noetherian ring.

Proof. See for example [24, Thm. 2.11] or [19, Thm. 1.3.5]

If R and S are rings and $I \subseteq R$, then in general $\langle I \rangle_S \neq \langle I \rangle$, but we have equality in the following special case:

Lemma A.2. Let $R \subseteq S$ be two fields, $I \subseteq R$ then we have

$$\langle I \rangle_S = \langle I \rangle$$

Proof. \mathcal{C} is a vector space over \mathbb{C} , we can choose¹ a basis $\{1_{g_i}\}_{i \in \mathbb{Z}}$ containing $1_{g_0} = 1 \in \mathcal{C}$. This then also constitutes a basis of the free module $\mathcal{C}\langle \mathbb{Z} \rangle$ over \mathbb{C} . Now consider an expression

$$5 = \sum_{i=1}^{\infty} 6_i 5^{-i} - \sum_{i=2}^{\infty} 6_i 2 \mathbb{C}\langle \mathbb{Z} \rangle$$

We can write $6_i = \sum_{j \in \mathbb{Z}} 6_{i,j} 1_{g_j}$ with finitely many nonzero $6_{i,j} \in \mathbb{C}$, then the former equation becomes

$$5 \cdot 1_{g_0} = 5 = \sum_{i=1}^{\infty} \sum_{j \in \mathbb{Z}} 6_{i,j} 1_{g_j} 5^{-i} = \sum_{j \in \mathbb{Z}} \sum_{i=1}^{\infty} 6_{i,j} 5^{-i} 1_{g_j}$$

Comparing the coefficient of the basis element $1_{g_0} = 1$ in this equation yields

$$5 = \sum_{i=1}^{\infty} 6_{i,0} 5^{-i} - \sum_{i=2}^{\infty} 6_{i,0} 2 \mathbb{C}\langle \mathbb{Z} \rangle$$

A.2 Commutative semigroups

A semigroup is a set together with an associative binary operation \cdot , as usual we will omit the operation, i. e. write 01 instead of $0 \cdot 1$. A monoid is a semigroup with a neutral element 1 ; one can always adjoin a neutral element to a semigroup if desired and since we will only consider monoids, we use these notions interchangeably. Our binary operation will be commutative in most interesting cases, hence we are really studying commutative monoids.

Example A.3 (Free (commutative) monoids) The most well-known semigroup in computer science is the free monoid over a finite alphabet Σ , consisting of strings of letters from Σ with string concatenation as the composition.

Similarly, the free commutative monoid over the alphabet $\Sigma = \{G_1, \dots, G_n\}$ is the set of (commuting) monomials

$$\text{Mon}^{\Sigma} = \{G_1^{a_1} G_2^{a_2} \dots G_n^{a_n} \mid a_i \in \mathbb{N}\}$$

This semigroup is isomorphic to the commutative monoid of integer vectors \mathbb{N}^n .

A homomorphism of semigroups is a map of sets $f: S \rightarrow T$ with $f(0) = 0$ and $f(0^1 0^2) = f(0^1) f(0^2)$ for $0^1, 0^2 \in S$, in the case of monoids we also require that $f(1) = 1$.

Remark. Notice that the concept of kernel of a homomorphism from group theory is not well-behaved in this general situation. For once, the kernel of $f: S \rightarrow T$ is usually defined as $f^{-1}(1)$, and needn't have a neutral element. And even if both S and T have neutral elements, then we may have $f^{-1}(1) = \emptyset$ even though f is not injective! Consider for

¹This can be easily done for finite extension of \mathbb{C} , and is always possible assuming the axiom of choice.

example

$$\phi: \mathbb{Z}^2 \rightarrow \mathbb{Z} \times \mathbb{Z} \quad \phi(a, b) = (a, a + b)$$

then $\phi^{-1}(0) = \{(0, 0)\}$, but in general $\phi^{-1}(a, b)$ has precisely $\gcd(a, b)$ preimages

$$\phi^{-1}(a, b) = \{(a - kb, a) \mid k \in \mathbb{Z}\}$$

The previous example shows that the naive definition of a kernel fails to measure the number of preimages in any meaningful way. But we can still define the following:

Definition A.4 (Congruence relation). A congruence relation on a semigroup S is an equivalence relation (i. e. reflexive, symmetric and transitive) such that for $a, b, c \in S$

$$a \sim b \text{ and } c \in S \Rightarrow ac \sim bc$$

If $\phi: S \rightarrow T$ is a homomorphism of semigroups, then

$$a \sim b \Rightarrow \phi(a) = \phi(b)$$

defines a congruence relation on T . Conversely, if \sim is a congruence relation on T , then the set of equivalence classes T/\sim forms a semigroup (with $(a\sim) \cdot (b\sim) = (ab)\sim$) and the surjective homomorphism

$$\phi: S \rightarrow T/\sim \quad \phi(a) = (a)\sim$$

defines the same equivalence relation $a \sim b \Leftrightarrow \phi(a) = \phi(b)$.

Definition A.5 (Commutative semigroup presentation). A semigroup presentation is a pair $\langle S, R \rangle$, where S is a set of generators and R is a set of relations. The congruence relation \sim_R generated by R is the smallest congruence relation on S^* containing R . The commutative semigroup $\langle S \mid R \rangle$ is the quotient of S^* / \sim_R .

The presentation is finite if both S and R are finite. A commutative semigroup is finitely presented if it is isomorphic to $\langle S \mid R \rangle$ for some finite presentation.

Lemma A.6. If R is a set of relations, then $\langle S \mid R \rangle$ is free if and only if there is a (possibly empty) sequence $G = G_0, G_1, \dots, G_n$ such that

$$G_{i+1} = g_i g_j^{-1} \quad G_i = g_i g_i^{-1}$$

for suitable $g_i \in S^*$ and $g_i^{-1} = g_i^{-1}$ or $g_i^{-1} = g_i^{-1}$ in R .

Proof. $\langle S \mid R \rangle$ contains R , by symmetry all $g_i^{-1} = g_i^{-1}$ for $g_i^{-1} = g_i^{-1} \in R$ and by reflexivity all $g_i^{-1} = g_i^{-1}$, $g_i^{-1} = g_i^{-1}$. Since it is a congruence relation, it contains all pairs $(g_i^{-1} g_j^{-1}, g_i^{-1} g_j^{-1} g_i^{-1} g_j^{-1})$ and hence by transitivity also $(g_i^{-1} g_j^{-1}, g_i^{-1} g_j^{-1})$ as in the lemma.

Conversely, it is easy to see that the relation

$G \sim^0$ If there exists a sequence as above

is already a congruence relation, so the two relations coincide.

It turns out that every finitely generated commutative monoid is in fact finitely presented!
 Theorem A.7 (Rédei). If M is finitely generated, i. e. we have a surjective homomorphism
 $\phi: \mathbb{Z}^n \rightarrow M$ for a finite set S , then M is generated by finitely many relations.

We can sketch a elegant and short proof due to Freyd [18]. If M is a monoid, then its
 monoid ring $R = \mathbb{Z}\langle M \rangle$ is the \mathbb{Z} -algebra whose underlying vector space has $\{x^a\}$ as a basis and
 the multiplication is defined by $x^a x^b = x^{a+b}$ on this basis and extended by bilinearity. For example,
 $R = \mathbb{Z}\langle \mathbb{N} \rangle \cong \mathbb{Z}[x]$ is just the polynomial ring in n variables.

Proof (sketch) Let $M = \langle S \rangle$. Assume that M is not finitely presented, then there exists an
 infinitely ascending sequence $R_1 \subset R_2 \subset \dots$ contained in R such that $R_{i+1} \subset R_i$ for all i . Let
 $\phi_i: R \rightarrow R_i$ be the natural surjection, then this gives rise to a chain of surjective but non-injective homomorphisms

$$R \xrightarrow{\phi_1} R_1 \xrightarrow{\phi_2} R_2 \xrightarrow{\phi_3} \dots$$

These maps yield surjective ring homomorphisms $R \xrightarrow{\phi_1} R_1 \xrightarrow{\phi_2} R_2 \xrightarrow{\phi_3} \dots$ let \mathfrak{a}_i be the kernel. By
 construction $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$ is a strictly increasing chain of ideals in $R \cong \mathbb{Z}\langle S \rangle$ but this contradicts the Noetherian property of polynomial rings (Hilbert's basis theorem
 A.1)!

Index

- Fractional Gröbner problem, 68
- Church-Rosser system
 - reduced, 63
- church-rosser system, 63
- Counter machine
 - computation bounded by $=$, 49
- counter machine, 46
- degree-dominating, 64
- dehomogenization, 30
- dimension
 - of an ideal, 30
- exponentially bounded counter machines,
49
- free commutative monoid, 43
- generating set, 73
- Gröbner basis, 13
 - membership problem, 17
- graded lexicographic ordering, 9
- graded reverse lexicographic order, 9
- Gröbner basis
 - interreduced, 15
 - reduced, 16
- homogenization, 30
- Ideal membership problem, 6
- initial ideal, 13
- leading coefficient, 10
- leading monomial, 10
- leading term, 8, 10
- level
 - of a symbol, 54
 - of a word, 54
- lexicographic ordering, 9
- monomial, 5
 - minimally reducible, 17
- monomial ideal, 6
- monomial ordering, 9
- multidegree, 10
- noetherian, 73
- normal forms, 12
- normalized, 15
- Nullstellensatz, 7
- parallel computation thesis, 35
- polynomial, 5
 - degree, 5
 - reducible w.r.t. an ideal, 17
- principal ideal, 73
- pure binomials, 7
- reducible
 - word, 62
- s-polynomial, 23
- semigroup, 74
- stack machine, 47
- string rewriting system, 42
- support
 - of a polynomial, 5
- Thue system

commutative, [43](#)
equivalent, [42](#)
thue system, [42](#)

Word problem for commutative semi-
groups, [43](#)

List of Symbols

$\dagger @$	the finite field of order $@$ (unique up to isomorphism)
$\mathbb{Z}, \mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	the natural numbers (with 0), the integers, the rational numbers, the real numbers and the complex numbers
\underline{f}	a set of variables f_1, \dots, f_g
Mon_k^n	the set of monomials in n variables and in k
$\text{supp}(f)$	the monomials occurring in a polynomial f
IM_k	the ideal membership problem over the field k
HNST_k	the decision problem to Hilbert's Nullstellensatz
\prec, \prec_P	a monomial order and the induced order on finite sets
$\text{lex}, \text{grlex}, \text{grevlex}$	the lexicographic, graded lexicographic and graded reverse lexicographic order
$\text{lt}(f), \text{lm}(f), \text{lc}(f)$	the leading term, leading monomial and leading coefficient of a polynomial f
$\text{mdeg}(f)$	the multidegree of a polynomial f
$\text{rem}(f, \mathfrak{B}), \text{in}^1(\mathfrak{B})$	the remainder of f with respect to \mathfrak{B} and the initial ideal generated by leading terms of \mathfrak{B}
$\text{NF}(f), \text{NF}^1(\mathfrak{B})$	the set of normal forms of f with respect to a set \mathfrak{B} or an ideal
GROEBM	the membership problem for reduced Gröbner bases of polynomials over k
$\sim_{\mathfrak{B}}$	the congruence relation defined by the ideal \mathfrak{B} and the equivalence class of f
W, \prec_W	a weight matrix and the associated monomial order
$\text{gcd}(f, g), \text{lcm}(f, g)$	the greatest common divisor and least common multiple of two monomials
$\text{Spoly}(f, g)$	the S-polynomial of $f - g$
h_5, d_6	the homogenization of f and dehomogenization of g
$P \rightarrow P - P$	a Thue system and the derivation relations
$\cdot, \dot{\cdot}$	the set of commutative words over Σ
$\sim, \dot{\sim}$	the configuration transition relation for a (counter) machine M and its transitive reflexive closure

$\text{rep}^1 @ \neg_1 z \bar{z} - \bar{z}^0$	the string representation of a con guration of a counter machine
$^1 = -P =^0$	the commutative Thue system by Mayr & Meyer counting to $2^{2^=}$
$\text{Lvl } ^1 A^0$	the set of words in $=$ of level A
$\text{box}^1 G^0$	the box of Gof the form $^1(j \ ^0 1 - \bullet \bullet \bullet - 4^0$
$G^1 P^0$	the graph associated to a commutative Thue system P
$* P - P$	the set of irreducible and reducible words with respect to a commutative Thue system P

List of Definitions and Theorems

1.3	Definition (Polynomial)	5
1.4	Definition (Ideal membership problem, $IM_{\mathbb{K}}$)	6
1.8	Theorem (Hilbert's Nullstellensatz)	7
1.9	Definition (Nullstellensatz, $HNST_{\mathbb{K}}$)	7
1.10	Definition (Monomial ordering)	9
1.14	Definition (Normal form, NF)	12
1.18	Theorem (Characterizations of Gröbner bases)	13
1.19	Definition (Gröbner basis)	13
1.22	Theorem (The normal form map NF)	14
1.24	Definition (Interreduced Gröbner basis)	15
1.27	Definition (Reduced Gröbner basis)	16
1.30	Definition (Reduced Gröbner basis membership problem, $GROEBM$)	17
1.31	Definition ((Ir)reducible, minimally reducible)	17
1.34	Theorem (Kopenhagen & Mayr 1999 [27])	19
1.36	Theorem (Robbiano 1985 [44])	21
2.1	Definition (S-Polynomial)	23
2.3	Theorem (Buchberger's criterion)	24
2.5	Theorem (Correctness of Buchberger's algorithm)	26
2.10	Theorem (Hermann 1926 [20])	29
2.11	Theorem (Kóllar 1988 [26])	29
2.12	Definition (Dimension of an ideal)	30
2.13	Theorem (Dickenstein et al. 1991 [12])	30
2.14	Definition ((De)homogenization)	30
2.16	Theorem (Dubé 1990 [14])	31
2.17	Theorem (Mayr & Ritscher 2013 [34])	31
2.21	Theorem (Fortune & Wyllie 1978 [17])	35
2.22	Theorem (Csanky 1976 [11])	35
2.23	Theorem (Ibarra, Moran & Rosier 1980 [22])	35
2.24	Theorem (Mayr 1989 [31], $IM_{\mathbb{K}} \in 2 \text{ EXPSPACE}$)	36
2.27	Theorem ($IM_{\mathbb{K}} \in \text{HNST} \in 2 \text{ PSPACE}$)	36
2.28	Theorem (Koiran 1996 [25])	37
2.31	Theorem (Krick & Logar 1991 [29])	39

3.1	De nition (String rewriting system, Thue system)	42
3.3	De nition (, Commutative Thue system)	43
3.5	De nition (Word problem for commutative semigroups, CSG)	43
3.7	Theorem (CSG_n is PSPACEhard)	45
3.8	De nition (Counter machine)	46
3.11	Theorem (EBC is EXPSPACEcomplete)	49
3.13	Theorem (Mayr & Meyer, 1982 [33])	50
3.16	Theorem (CSG is EXPSPACEhard)	52
3.17	De nition (Level of a word, box)	54
3.20	Theorem (Bayer & Stillman [4])	56
3.23	Theorem (CSG reduces to IM_k)	61
3.25	Theorem (Bürgisser 1998 [9])	62
3.26	De nition ((Ir)reducible words)	62
3.27	De nition (Church-Rosser system, reduced)	63
3.32	Theorem (Huynh 1986 [21])	64
3.37	Theorem (GROEBM is EXPSPACEhard)	67
3.39	Theorem (Rolnick & Spencer 2018 [46])	68
A.1	Theorem (Hilbert basis theorem)	73
A.4	De nition (Congruence relation)	75
A.5	De nition (Commutative semigroup presentation)	75
A.7	Theorem (Rédei)	76

List of Figures

1.1	The perpendicular bisectors of a triangle intersecting in the circumcenter "	4
3.1	The chain of complexity-theoretic reductions.	41
3.2	How to represent the tape of a Turing machine with two stacks.	48
3.3	Rules (A) (G),(V) in the context of boxes.	55
3.4	A visualization of the rules in $R_{=}$.	65

Bibliography

- [1] Sanjeev Arora and Boaz Barak. Computational Complexity: A Modern Approach. Cambridge: Cambridge University Press, 2009. isbn: 9780521424264. doi: [10.1017/CBO9780511804090](https://doi.org/10.1017/CBO9780511804090) (cit. on pp. [37](#), [41](#)).
- [2] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of the F5 Gröbner basis algorithm . In: Journal of Symbolic Computation **70** (2015), pp. 49 70. issn: 0747-7171. doi: <https://doi.org/10.1016/j.jsc.2014.09.025> (cit. on p. [28](#)).
- [3] Dave Bayer and David Mumford. What can be computed in algebraic geometry. **1993**. doi: [10.48550/ARXIV.ALG-GEOM/9304003](https://doi.org/10.48550/ARXIV.ALG-GEOM/9304003) (cit. on p. [71](#)).
- [4] David Bayer and Michael Stillman. On the complexity of computing syzygies . In: Journal of Symbolic Computation **6.2** (1988), pp. 135 147. issn: 0747-7171. doi: [https://doi.org/10.1016/S0747-7171\(88\)80039-7](https://doi.org/10.1016/S0747-7171(88)80039-7) (cit. on pp. [54](#), [56](#), [60](#), [62](#)).
- [5] Lenore Blum et al. Complexity and Real Computation. Springer New York, Oct. 2012. 472 pp. isbn: 1461268737. doi: [10.1007/978-1-4612-0701-6](https://doi.org/10.1007/978-1-4612-0701-6) (cit. on p. [7](#)).
- [6] Paul Breiding and Sascha Timme. HomotopyContinuation.jl: A Package for Homotopy Continuation in Julia . In: Mathematical Software ICMS 2018. Ed. by James H. Davenport et al. Cham: Springer International Publishing, 2018, pp. 458 465. isbn: 978-3-319-96418-8 (cit. on p. [72](#)).
- [7] Paul Breiding et al. Nonlinear Algebra and Applications. **2021**. doi: [10.48550/ARXIV.2103.16300](https://doi.org/10.48550/ARXIV.2103.16300) (cit. on p. [4](#)).
- [8] Bruno Buchberger. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal . In: Journal of Symbolic Computation **41.3** (2006). Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday), pp. 475 511. issn: 0747-7171. doi: <https://doi.org/10.1016/j.jsc.2005.09.007> (cit. on p. [26](#)).
- [9] Peter Bürgisser. On the Parallel Complexity of the Polynomial Ideal Membership Problem . In: Journal of Complexity **14.2** (1998), pp. 176 189. issn: 0885-064X. doi: <https://doi.org/10.1006/jcom.1998.0472> (cit. on p. [62](#)).
- [10] Matthew Clegg, Je Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability . In: Proceedings of STOC'00 (Mar. 2000). doi: [10.1145/237814.237860](https://doi.org/10.1145/237814.237860) (cit. on p. [27](#)).

- [11] Laszlo Csanky. Fast Parallel Matrix Inversion Algorithms . In: SIAM Journal on Computing 5.4 (1976), pp. 618 623doi: [10.1137/0205040](https://doi.org/10.1137/0205040) (cit. on p. 35).
- [12] Alicia Dickenstein et al. The membership problem for unmixed polynomial ideals is solvable in single exponential time . In: Discrete Applied Mathematics 33.1 (1991), pp. 73 94. issn: 0166-218Xdoi: [https://doi.org/10.1016/0166-218X\(91\)90109-A](https://doi.org/10.1016/0166-218X(91)90109-A) (cit. on p. 30).
- [13] Thomas Dubé, B. Mishra, and Chee-Keng Yap. Admissible Orderings and Bounds for Gröbner Basis Normal Form Algorithms . In: (1986) (cit. on pp. 21, 33).
- [14] Thomas W. Dubé. The Structure of Polynomial Ideals and Gröbner Bases . In: SIAM Journal on Computing 9.4 (Aug. 1990), pp. 750 773doi: [10.1137/0219053](https://doi.org/10.1137/0219053) (cit. on p. 31).
- [15] David Eisenbud and Bernd Sturmfels. Binomial Ideals . In: Duke Math. J 84 (Feb. 1994). doi: [10.1215/S0012-7094-96-08401-X](https://doi.org/10.1215/S0012-7094-96-08401-X) (cit. on p. 18).
- [16] Jean Charles Faugère. A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5) . In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC '02. Lille, France: Association for Computing Machinery, 2002, pp. 75 83.isbn: 1581134843doi: [10.1145/780506.780516](https://doi.org/10.1145/780506.780516) (cit. on p. 28).
- [17] Steven Fortune and James Wyllie. Parallelism in Random Access Machines . In: Proceedings of the Tenth Annual ACM Symposium on Theory of Computation STOC '78. San Diego, California, USA: Association for Computing Machinery, 1978, pp. 114 118. isbn: 9781450374378doi: [10.1145/800133.804339](https://doi.org/10.1145/800133.804339) (cit. on p. 35).
- [18] Peter J. Freyd. Rédei's finiteness theorem for commutative semigroups . In: 1968. doi: [10.1090/S0002-9939-1968-0227290-4](https://doi.org/10.1090/S0002-9939-1968-0227290-4) (cit. on p. 76).
- [19] Gert-Martin Greuel and Gerhard Pfister. A Singular Introduction to Commutative Algebra Springer Berlin Heidelberg, Nov. 2007. 712 pp. isbn: 3540735410doi: [10.1007/978-3-540-73542-7](https://doi.org/10.1007/978-3-540-73542-7) (cit. on pp. 3, 7, 13, 28, 30, 73).
- [20] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale . In: Mathematische Annalen 85 (1926), pp. 736 788 (cit. on p. 29).
- [21] Dung T. Huynh. A Superexponential Lower Bound for Gröbner Bases and Church-Rosser Commutative Thue Systems . In: Inf. Control. 68 (1986), pp. 196 206 (cit. on pp. 41, 62, 64, 65).
- [22] Oscar H. Ibarra, Shlomo Moran, and Louis E. Rosier. A note on the parallel complexity of computing the rank of order n matrices . In: Information Processing Letters 14,5 (1980) (cit. on p. 35).
- [23] Jürgen Gerhard Joachim von zur Gathen. Modern Computer Algebra Cambridge University Press, Mar. 2017. 812 pp isbn: 1107039037doi: [10.1017/CBO9781139856065](https://doi.org/10.1017/CBO9781139856065) (cit. on pp. 3, 4, 9).

- [24] Gregor Kemper. A course in commutative algebra. Springer, 2011, p. 246. isbn: 9783642035456 (cit. on pp. [1](#), [3](#), [7](#), [13](#), [23](#), [24](#), [73](#)).
- [25] Pascal Koiran. Hilbert's Nullstellensatz Is in the Polynomial Hierarchy . In: Journal of Complexity 12.4 (1996), pp. 273 286. issn: 0885-064X. doi: <https://doi.org/10.1006/jcom.1996.0019> (cit. on p. [37](#)).
- [26] Janos Kollar. Sharp Effective Nullstellensatz . In: Journal of the American Mathematical Society 1.4 (1988), pp. 963 975. issn: 08940347, 10886834. url : <http://www.jstor.org/stable/1990996> (cit. on p. [29](#)).
- [27] Ulla Koppenhagen and Ernst W. Mayr. An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals . In: Journal of Symbolic Computation 28.3 (1999), pp. 317 338. issn: 0747-7171. doi: <https://doi.org/10.1006/jsco.1999.0285> (cit. on pp. [18](#), [19](#), [39](#)).
- [28] Martin Kreuzer and Lorenzo Robbiano. Computational Commutative Algebra. Springer Berlin Heidelberg, 2000. doi: [10.1007/978-3-540-70628-1](https://doi.org/10.1007/978-3-540-70628-1) (cit. on pp. [3](#), [14](#)).
- [29] Teresa Krick and Alessandro Logar. Membership problem, Representation problem and the Computation of the Radical for one-dimensional Ideals . In: Effective Methods in Algebraic Geometry. Ed. by Teo Mora and Carlo Traverso. Boston, MA: Birkhäuser Boston, 1991, pp. 203 216. isbn: 978-1-4612-0441-1. doi: [10.1007/978-1-4612-0441-1_13](https://doi.org/10.1007/978-1-4612-0441-1_13) (cit. on p. [39](#)).
- [30] Klaus Kühnle and Ernst W. Mayr. Exponential Space Computation of Gröbner Bases . In: Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation ISSAC '96. Zurich, Switzerland: Association for Computing Machinery, 1996, pp. 63 71. isbn: 0897917960. doi: [10.1145/236869.236900](https://doi.org/10.1145/236869.236900) (cit. on pp. [17](#), [33](#)).
- [31] Ernst W. Mayr. Membership in polynomial ideals over \mathbb{Q} is exponential space complete . In: STACS 89. Ed. by B. Monien and R. Cori. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989, pp. 400 406. isbn: 978-3-540-46098-5 (cit. on p. [36](#)).
- [32] Ernst W. Mayr. Some Complexity Results for Polynomial Ideals . In: Journal of Complexity 13.3 (1997), pp. 303 325. issn: 0885-064X. doi: [10.1006/jcom.1997.0447](https://doi.org/10.1006/jcom.1997.0447) (cit. on pp. [23](#), [28](#), [41](#), [44](#)).
- [33] Ernst W. Mayr and Albert R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals . In: Advances in Mathematics 46.3 (Dec. 1982), pp. 305 329. doi: [10.1016/0001-8708\(82\)90048-2](https://doi.org/10.1016/0001-8708(82)90048-2) (cit. on pp. [29](#), [41](#), [50](#)).
- [34] Ernst W. Mayr and Stephan Ritscher. Dimension-dependent bounds for Gröbner bases of polynomial ideals . In: Journal of Symbolic Computation 49 (2013). The International Symposium on Symbolic and Algebraic Computation, pp. 78 94. issn: 0747-7171. doi: doi.org/10.1016/j.jsc.2011.12.018 (cit. on pp. [30](#), [31](#)).

- [35] Ernst W. Mayr and Stefan Toman. “Complexity of Membership Problems of Different Types of Polynomial Ideals”. In: *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*. Ed. by Gebhard Böckle, Wolfram Decker, and Gunter Malle. Cham: Springer International Publishing, 2017, pp. 481–493. ISBN: 978-3-319-70566-8. DOI: [10.1007/978-3-319-70566-8_20](https://doi.org/10.1007/978-3-319-70566-8_20) (cit. on pp. 23, 28, 37).
- [36] Marvin L. Minsky. *Computation: Finite and Infinite Machines*. USA: Prentice-Hall, Inc., 1967. ISBN: 0131655639 (cit. on pp. 46, 49).
- [37] H. Michael Möller and Ferdinando Mora. “Upper and lower bounds for the degree of Groebner bases”. In: *EUROSAM* . Ed. by John Fitch. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984, pp. 172–183. ISBN: 978-3-540-38893-7 (cit. on p. 30).
- [38] Bernard Mourrain, Simon Telen, and Marc Van Barel. *Truncated Normal Forms for Solving Polynomial Systems: Generalized and Efficient Algorithms*. 2018. DOI: [10.48550/ARXIV.1803.07974](https://doi.org/10.48550/ARXIV.1803.07974) (cit. on p. 72).
- [39] Victor Pan. “Complexity of parallel matrix computations”. In: *Theoretical Computer Science* 54.1 (1987), pp. 65–85. ISSN: 0304-3975. DOI: [https://doi.org/10.1016/0304-3975\(87\)90019-3](https://doi.org/10.1016/0304-3975(87)90019-3) (cit. on p. 35).
- [40] Behrooz Parhami. *Introduction to Parallel Processing: Algorithms and Architectures*. Boston, MA: Springer US, 2002. ISBN: 978-0-306-46964-0. DOI: [10.1007/0-306-46964-2_5](https://doi.org/10.1007/0-306-46964-2_5) (cit. on p. 34).
- [41] Suzanna Parkinson et al. *Analysis of Normal-Form Algorithms for Solving Systems of Polynomial Equations*. 2021. DOI: [10.48550/ARXIV.2104.03526](https://doi.org/10.48550/ARXIV.2104.03526) (cit. on p. 72).
- [42] Emil L. Post. “Recursive Unsolvability of a problem of Thue”. In: *Journal of Symbolic Logic* 12.1 (1947), pp. 1–11. DOI: [10.2307/2267170](https://doi.org/10.2307/2267170) (cit. on p. 42).
- [43] Stephan Ritscher. “Degree Bounds and Complexity of Gröbner Bases of Important Classes of Polynomial Ideals”. PhD thesis. Technische Universität München, 2012 (cit. on pp. 15, 20, 34, 36, 38).
- [44] Lorenzo Robbiano. “Term orderings on the polynomial ring”. In: *EUROCAL '85* . Ed. by Bob F. Caviness. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 513–517. ISBN: 978-3-540-39685-7 (cit. on p. 21).
- [45] J. Maurice Rojas. “Dedekind Zeta Functions and the Complexity of Hilbert’s Nullstellensatz”. In: *arXiv: Number Theory* (2003) (cit. on p. 37).
- [46] David Rolnick and Gwen Spencer. “On the robust hardness of Gröbner basis computation”. In: *Journal of Pure and Applied Algebra* 223.5 (2019), pp. 2080–2100. ISSN: 0022-4049. DOI: <https://doi.org/10.1016/j.jpaa.2018.08.016> (cit. on pp. 68, 69).

-
- [47] Chee K. Yap. “A new lower bound construction for commutative thue systems with applications”. In: *Journal of Symbolic Computation* 12.1 (1991), pp. 1–27. ISSN: 0747-7171. DOI: [https://doi.org/10.1016/S0747-7171\(08\)80138-1](https://doi.org/10.1016/S0747-7171(08)80138-1) (cit. on p. 60).