Abstract

PERRY, JOHN EDWARD. Combinatorial Criteria for Gröbner Bases. (Under the direction of Hoon Hong.)

Both the computation and the detection of Gröbner bases require a criterion that decides whether a set of polynomials is a Gröbner basis. The most fundamental decision criterion is the reduction of all S-polynomials to zero. However, S-polynomial reduction is expensive in terms of time and storage, so a number of researchers have investigated the question of when we can avoid S-polynomial reduction. Certain results can be considered "combinatorial", because they are criteria on the leading terms, which are determined by integers. Our research builds on these results; this thesis presents combinatorial criteria for Gröbner bases.

The first part of this thesis reviews the relevant literature on Gröbner bases and skipping S-polynomial reduction. The second part considers criteria for skipping a fixed number of S-polynomial reductions. The first two theorems of part two show how to apply Buchberger's criteria to obtain necessary and sufficient conditions for

skipping all S-polynomial reductions, and for skipping all but one S-polynomial reductions. The third theorem considers the question of skipping all but two S-polynomial reductions; we have found that this problem requires new criteria on leading terms. We provide one new criterion that solves this problem for a set of three polynomials; for larger sets, the problem remains open.

The final part of this thesis considers Gröbner basis detection. After a brief review of a previous result that requires S-polynomial reduction, we provide a new result which takes a completely different approach, avoiding S-polynomial reduction completely.

Throughout the latter two parts, we provide some statistical analysis and experimental results.

8th April 2005

COMBINATORIAL CRITERIA FOR GRÖBNER BASES

BY
JOHN EDWARD PERRY, III

A DISSERTATION SUBMITTED TO THE GRADUATE FACULTY OF
NORTH CAROLINA STATE UNIVERSITY
IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

RALEIGH, NORTH CAROLINA
APRIL 2005

APPROVED BY:

H. HONG CHAIR OF ADVISORY COMMITTEE	E. KALTOFEN
A. SZANTO	M. SINGER

Dedication

A Nonno Felice: guardando il nipote che leggeva, vide un professore.[1]

[1]Italian: *To Nonno Felice: he looked at his grandson who was reading, and saw a professor.*

Biography

John Perry (III) was born in late 1971, in the city of Newport News, Virginia. His parents are John Perry (Jr.), originally of Hampton, Virginia, and Maria Leboffe, originally of Gaeta, Italy. Following graduation from Warwick high school, John entered Marymount University. He graduated in 1993 with his B.S. in mathematics and mathematics education. John subsequently earned an M.S. in mathematics from Northern Arizona University. It was at this time that he began to experiment with mathematics on the computer; one program that implemented the Runge-Kutta interpolation to graph differential equations is available on-line for Amiga computers: see [**Per94**].

After earning his master's degree, John returned to Virginia and taught mathematics at Franklin County High School. Two years later, he volunteered for the Catholic priesthood, but withdrew from seminary in December, 1998. He applied, and was accepted, to North Carolina State University. He entered in the fall of 1999 and spent the next six years working on his doctorate.

Acknowledgments

First, I must express my profound gratitude to the citizens of the state of North Carolina, whose system of public universities is among the finest in the world. I likewise thank the citizens of the United States, who supported my research in part with NSF grant 53344.

I could never have hoped to be a doctoral student of mathematics at North Carolina State University without both the inspiration and the instruction of past teachers and professors. There is insufficient space to name them all, but I would be remiss if I failed to name Neil Drummond, Vanessa Job, Judy Green, Adrian Riskin (or Adrien Riskin, depending on his mood), Jonathan Hargis, and Lawrence Perko.

I also thank the mathematics department at North Carolina State University, especially the computer algebra group, from whom I learned an immense amount. In particular, my committee (Hoon Hong, Erich Kaltofen, Michael Singer, and Agnes Szanto) taught excellent classes and looked at several incomplete drafts of this text.

My advisor, Hoon Hong, spent countless hours guiding my research, teaching me how to ask questions, how to answer them, and how to realize when the question might be too hard. His advice and encouragement were invaluable. His wife provided a number of delicious meals on many of the occasions that I passed the hours with her husband hunched over a sheet of paper; on one occasion she drove me to a car mechanic.

Erich Kaltofen provided a number of thoughtful conversations, not all about mathematics. One of these conversations (on how mathematicians create ideas) helped me realize that it was not yet time to abandon hope. He was always ready with advice and information.

Bruno Buchberger suggested the statistical investigations of the results that appear at the end of chapter 6. Our discussions on the results of that chapter went a long way towards deepening my understanding of them.

My officemates Chris Kuster, Alexey Ovchinnikov, Scott Pope, and George Yuhasz were especially generous with their time and made a number of helpful suggestions and contributions on papers, presentations, and this thesis.

Richard Schugart, my roommate of these past five years, has had to suffer my quirky, a-social personality. He has put up with me much better than I probably would. His mother was very generous with cookies, for which I'm not sure whether I owe her gratitude or grumbling – alas, my waistline has expanded.

My parents and my brothers have patiently endured my dissatisfaction with personal and professional imperfections for thirty-three years now, and they have never failed to challenge me to do my best. I come from a family privileged not by wealth, but by the content of its character, to say nothing of the characters in its contents. *Ardisci e spera!*[2]

Галя наградила улыбкой на семь роз. [3]

Finally: *laus tibi, lucis largitor splendide.*[4]

[2]A saying of my Italian grandfather and his brother: *Dare and hope!*
[3]Galya rewarded seven roses with a smile.
[4]Adapted from a medieval Latin hymn: *Praise to you, O gleaming giver of light.*

Table of Contents

List of Figures ix

List of Tables xi

List of Symbols xiii

Part 1. Background Material 1

Chapter 1. An introduction to Gröbner bases 2
1.1. Gröbner bases: analogy 2
1.2. Gröbner bases: definition 7
1.3. Gröbner bases: decision 22
1.4. Some properties of representations of S-polynomials 48

Chapter 2. Skipping S-polynomial reductions 54
2.1. A Bottleneck 54
2.2. Skipping S-polynomial Reductions 55
2.3. Combinatorial Criteria on Leading Terms 58
2.4. The Buchberger Criteria 59
2.5. Term Diagrams 71

Part 2. New combinatorial criteria for skipping S-polynomial reduction 77

Chapter 3. Outline of part two 78
3.1. Buchberger's criteria revisited 78
3.2. Formal statement of the problem considered in part two 80
3.3. Outline of the remainder of part two 82
3.4. An invaluable lemma 83

Chapter 4. Skipping all S-polynomial reductions 86
4.1. Problem 86
4.2. Result 87
4.3. Application of result 89

Chapter 5. Skipping all but one S-polynomial reductions 101

5.1. Problem 101
5.2. Result 102
5.3. Application of result 108

Chapter 6. Skipping all but two S-polynomial reductions (case for three polynomials) 120
6.1. Problem 120
6.2. Result 123
6.3. Application of result 148

Part 3. A New Criterion for Gröbner Basis Detection of Two Polynomials 167

Chapter 7. Gröbner basis detection: introduction 168
7.1. Introduction to the problem 168
7.2. Matrix representations of term orderings 171
7.3. Solving for admissible matrices 186

Chapter 8. Gröbner basis detection: general solution by polytopes 200
8.1. Problem 200
8.2. Polytopes, Polyhedra and Minkowski Sums 201
8.3. Result 205

Chapter 9. Gröbner basis detection of two polynomials by factoring 209
9.1. Problem 209
9.2. Result 209
9.3. Application of result 213

Conclusion 235

Bibliography 237

Index 241

List of Figures

2.1 Term diagram of $t_1, t_2, \ldots, t_6$ 72
2.2 Diagram of $t_1, t_2, \ldots, t_6$, with shading added for divisible terms. 73
2.3 Diagram of the greatest common divisor (lower left dot) and least common multiple (upper right dot) of two terms. 74
2.4 Diagram of two relatively prime terms. 74
2.5 Diagram of the divisors (in grey box) that divide $\mathrm{lcm}\,(t_4, t_6)$. 75
2.6 No other monomial lies within the region of divisors of t_1 and t_2. 76

6.1 Diagram of proof strategy for section 6.2.3. 127
6.2 Terms t_1 and t_3 have no indeterminates in common. 152
6.3 Terms t_1 and t_3 have all their indeterminates in common. 152
6.4 Terms t_1 and t_3 have one determinate in common. 153
6.5 Theorem 6.3 allows a progression from Buchberger's second criterion to Buchberger's first criterion. 155
6.6 Ordering of critical pairs excludes most occurrences of the new criterion. 161
6.7 Ordering of critical pairs excludes most occurrences of the new criterion. 162
6.8 Ordering of critical pairs excludes most occurrences of the new criterion. 162

7.1 Diagram of vectors v_1, v_2 in example 7.8. 181
7.2 How lemma 7.7 generates γ_1, γ_2 for example 7.8. 183

8.1 Newton polytope of f in example 8.2. 202
8.2 Newton polyhedron of f in example 8.2 (first quadrant view only). 202
8.3 The Minkowski sum of the Newton polytopes $N(f)$ and $N(g)$, from example 8.5 203
8.4 The Minkowski sum of the Newton polyhedra $N_{\text{aff}}(f)$ and $N_{\text{aff}}(g)$, from example 8.5 204
8.5 Normal cones of the Minkowski sum illustrated in figure 8.4. 205

9.1 Summary of the number of detections of Gröbner bases for different cases of unstructured systems. 226
9.2 Summary of the number of detections of Gröbner bases for different cases of structured systems. 230
9.3 Detection compared to computation (chart of times): fixed number of terms and fixed total degree. 231
9.4 Detection compared to computation (chart of times): 5% sparsity of terms and fixed total degree. 232
9.5 Detection compared to computation: fixed (chart of times): fixed number of terms and increasing total degree. 233

List of Tables

4.1 Number of sets of polynomials where every pair of leading terms is relatively prime, out of 100,000 sets. 95

4.2 Number of sets where every pair of leading terms is relatively prime, out of 100,000 sets. 95

4.3 Comparison of the number of Gröbner bases found by S-polynomial reduction, to the number found by applying theorem 4.1. 98

4.4 Comparison of the number of Gröbner bases found by S-polynomial reduction, to the number found by applying theorem 4.1. 99

5.1 Number of sets where we can skip all but one S-polynomial reduction, out of out of 100,000 sets. 115

5.2 Experimental results: number of sets, out of 100,000, where we can skip all S-polynomial reductions. 117

5.3 Comparison of the number of Gröbner bases found by S-polynomial reduction, to the number found by applying theorem 5.1. 118

6.1 Statistical analysis of new criterion on leading terms, assuming all S-polynomials reduce to zero. 158

6.2 Statistical analysis of new criterion on leading terms, assuming all S-polynomials reduce to zero. 158

6.3 Number of skips during the computation of a Gröbner basis for three randomly-generated polynomials; total-degree term ordering. 160

6.4 Comparison of areas of regions: Buchberger criteria vs. new criterion (total-degree ordering). 164

6.5 Comparison of areas of regions: Buchberger criteria vs. new criterion (lexicographic ordering). 164

6.6 Which $S_{i,j}$ used r polynomials to reduce to zero (system 1). 165

6.7 Which $S_{i,j}$ used r polynomials to reduce to zero (system 3). 165

6.8 Which $S_{i,j}$ used r polynomials to reduce to zero (system 6). 165

9.1 Number of times we detected a Gröbner basis for f_1, f_2 (six terms of total degree six). 224
9.2 Number of times we detected a Gröbner basis for f_1, f_2 (10% sparse, total degree 6). 225
9.3 Number of times we detected a Gröbner basis for f_1, f_2 (six terms of total degree 6×#vars). 226
9.4 Number of times we detected a Gröbner basis for gc_1, gc_2 (three terms in each of g, c_1, c_2; maximum degree per term is 10). 227
9.5 Number of times we detected a Gröbner basis for gc_1, gc_2 (number of terms in each of g, c_1, c_2 fixed at 5% sparsity, minimum two terms for c_1, c_2; maximum degree per term is 10). 228
9.6 Number of times we detected a Gröbner basis for gc_1, gc_2 (three terms in each of g, c_1, c_2; maximum degree per term is 10×#vars). 229
9.7 Detection compared to computation: fixed number of terms and fixed total degree. 231
9.8 Detection compared to computation: fixed sparsity of terms and fixed total degree. 232
9.9 Detection compared to computation: fixed number of terms and increasing total degree. 232

List of Symbols

Symbol	page	meaning
$\succ, \prec, \succeq, \preceq$	9	term ordering
$\gg$	172	lexicographic ordering of a vector
$\longrightarrow, \underset{q \cdot f}{\longrightarrow}, \nrightarrow$	17	one-step reduction
$\overset{*}{\underset{(f_1,\ldots,f_m)}{\longrightarrow}}, \overset{*}{\underset{(f_1,\ldots,f_m)}{\nrightarrow}}$	17	complete reduction
$\rightsquigarrow$	55	can skip S-polynomial reduction
$\alpha_{(i)}$	172	row i of vector α
σ_{ij}, σ_{ji}	48	monomials used to construct $S_{i,j}$
ω	187	weight vector
$\mathrm{BC1}\,(t_1, t_3)$, $\mathrm{BC2}\,(t_1, t_2, t_3)$	69	Buchberger's first combinatorial criterion
CC	80	combinatorial criterion for skipping S-polynomial reductions
$\mathbb{F}$	8	a field
$\mathbb{F}[x_1, \ldots, x_n]$		the polynomial ring in $x_1, \ldots, x_n$ over $\mathbb{F}$
$\mathrm{GB}_{\succ}\,(f_1, \ldots, f_m)$	20	$f_1, \ldots, f_m$ are a Gröbner basis with respect to $\succ$

Symbol	page	meaning
$\mathcal{I}(f_1, \ldots, f_m)$	19	$\{h_1 f_1 + \cdots + h_m f_m : \ h_k \in \mathbb{F}[x_1, \ldots, x_n]\}$ (the ideal of $f_1, \ldots, f_m$)
$\mathcal{M}_{(i)}$	172	row i of matrix $\mathcal{M}$
$\mathcal{M}_{(i,j)}$	189	row i, column j of matrix $\mathcal{M}$
$N(f)$	201	the Newton polytope of f
$N_{\text{aff}}(f)$	202	the Newton polyhedron of f
$S_{\succ}(f_i, f_j)$	23	the S-polynomial of f_i, f_j with respect to $\succ$
$S_{f_i,f_j}, S_{i,j}$	23	the S-polynomial of f_i, f_j with respect to a given $\succ$
$\mathcal{T}(x_1, \ldots, x_n)$	9	the set of terms on $x_1, \ldots, x_n$
$\text{VB1}_x(t_1, t_3)$, $\text{VB2}_x(t_1, t_2, t_3)$	123	variable-wise Buchberger criteria

Part 1

Background Material

Chapter 1

An introduction to Gröbner bases

1.1. GRÖBNER BASES: ANALOGY

This text studies certain properties of Gröbner bases. What are Gröbner bases? We introduce them as an extension of a high-school topic.

1.1.1. A "NICE FORM". Suppose we are given two polynomials f_1, f_2. We want to know the following:[1]

- Do f_1, f_2 share any *common roots*?
- If so, is the solution set *finite* or *infinite*?
- If the solution set is finite, *how many* common roots are there?
- If the solution set is infinite, *what is its dimension*?
- *Find* or *describe* these common solutions.

[1]Although we raise these questions for the purpose of motivating the study of Gröbner bases, it is beyond the scope of this text to answer them. The interested reader can find an excellent treatment of these topics in [**CLO97**].

These are natural questions: systems of polynomials appear in numerous applications of mathematics, and the common roots of polynomial systems have important real-world significance.

We would like a "nice form" that would help us answer these questions easily. *Such a "nice form" exists,* and we call it a Gröbner basis.

The precise definition of a Gröbner basis will have to wait for section 1.2.4. For now, we present an intuitive idea via two examples.

1.1.2. LINEAR POLYNOMIALS.

EXAMPLE 1.1. Consider the system

$$2x + 3y + 1 = 0$$

$$x + y = 0$$

Do the equations have common solutions?

High school students encounter this problems in Algebra I, and learn to solve them by *Gaussian elimination*. They begin by writing the variables on one side, and the constants on the opposite side:

$$2x + 3y = -1$$

$$x + y = 0$$

The goal of Gaussian elimination is to obtain a "nice form" that allows us to identify properties of the common solutions. We eliminate so-called "pivot" variables by combining two equations, yielding a new equation that lacks the pivot.

In this example, we will consider the term containing x to be the first "pivot". We multiply an appropriately-chosen constant (-2) to the second equation:

$$\left.\begin{array}{rcl} 2x+3y=-1 & \longrightarrow & 2x + 3y = -1 \\ (-2)\cdot(x+y=0) & \longrightarrow & -2x - 2y = 0 \end{array}\right\}$$

Adding the two, we obtain a new equation,

$$y = -1$$

We can replace the first equation with this new one, giving us the following system:

$$x + y = 0$$

$$y = -1$$

We say that this new system has a "nice form". *Why?* Observe that the system is "triangular": both x and y appear in the first equation, but only y appears in the second. We see immediately that any solution requires $y = -1$, and we can substitute this value into the first equation to find a unique solution at $(1, -1)$. $\_\diamond$

1.1.3. NON-LINEAR POLYNOMIALS. The situation is a little more complicated for non-linear polynomials.

EXAMPLE 1.2. Let

$$f_1 = x^2 + y^2$$

$$f_2 = xy$$

We want to know whether the system has a common root. This is equivalent to saying that we want to know whether the equations

$$x^2 + y^2 = 0$$

$$xy = 0$$

have a common solution.

Perhaps we could generalize the method of example 1.1. Do these polynomials have a "nice form"? If not, what must we do to find a similar "nice form"?[2]

To answer the first question: *no*, this system is not a nice form.

So, we need to identify "pivots". It doesn't seem unreasonable to focus our attention on the highest powers of x: so, we identify x^2 and xy as "pivots" of f_1, f_2.[3]

Now we want to eliminate the pivots. *How?* When the polynomials were linear, the pivots were like terms, so we only needed to multiply by "magic constants." In this case, the pivots are not alike, so we need to multiply by *monomials* that give

[2]We do not yet have the machinery to provide the precise definition of this "nice form"; that will come in definition 1.18 on page 19 of section 1.2.4.

[3]There is a science of choosing pivots, and we provide a treatment of this science in section 1.2.2.

the pivots' *least common multiple:* x^2y. To accomplish this, multiply y to the first equation and $-x$ to the second:

$$\left.\begin{array}{rcl} y & \cdot & (x^2+y^2=0) \\ -x & \cdot & (xy=0) \end{array}\right\} \quad \begin{array}{c} \longrightarrow \\ \longrightarrow \end{array} \quad \begin{array}{rcl} x^2y + y^3 &=& 0 \\ -x^2y &=& 0 \end{array}$$

Adding the resulting equations, we have

$$y^3 = 0$$

Let

$$f_3 = y^3$$

It turns out that f_1, f_2, f_3 together have the "nice form" we are looking for. ——◇

It is not obvious to the previously uninitiated that f_1, f_2, f_3 have a "nice form". While it is true that we eliminated x from f_3, we discarded neither f_1 nor f_2 (nor can we). Furthermore, we have increased the total degree of the system: f_3 is a cubic, whereas f_1, f_2 are quadratic in x, y.

These difficulties are unimportant for now. What matters is the illustration of the method: we identified a pivot, then eliminated it; this obtained for us a "nice form".

What is going on here?

1.2. GRÖBNER BASES: DEFINITION

In 1965 [**Buc65**] Bruno Buchberger invented an algorithm to compute such a "nice form" for systems of polynomial equations. In honor of his advisor, Wolfgang Gröbner, he named this form *Gröbner bases*; the corresponding algorithm has since become known as Buchberger's algorithm. Gröbner bases are now recognized as an important tool for describing solutions to systems of nonlinear equations. They form a part of all major computer algebra systems, and have found their place as an important application to scientific research in fields such as physics and engineering.[4]

A precise definition of a Gröbner basis appears in section 1.2.4; first, we must establish some fundamental concepts.

1.2.1. TERMS, MONOMIALS, COEFFICIENTS. Different authors give incompatible definitions to the notions of terms, monomials, and coefficients. We follow the convention of the Maple computer algebra system.

[4]An on-line conversation with a cousin drove this point home to me. When he asked me what I was researching, I told him that I was working with Gröbner bases. To my surprise, my cousin replied, "That sounds familiar... let me check." I didn't expect this, because he was a computer science major, but a few moments later, he continued, "Yes, they're in my astronomy book; they are used to compute singularities."

DEFINITION 1.3. An **indeterminate** (also called a **variable**[5]) is an unspecified value. A **term** is a product of indeterminates. A **monomial** is the product of a term and a constant from the field $\mathbb{F}$. We call this constant the **coefficient**. A **polynomial** is the sum of a finite number of monomials.

EXAMPLE 1.4. Let

$$g = 5x^2 - 3xy^2 + y^3$$

The monomials of f are

$$5x^2\ , \quad -3xy^2\ , \quad y^3$$

The terms of f are

$$x^2\ , \quad xy^2\ , \quad y^3$$

The coefficients of f are

$$5\ , \quad -3\ , \quad 1$$

◇

1.2.2. TERM ORDERINGS (THE SCIENCE OF CHOOSING PIVOTS). Recall that in example 1.2 we chose to eliminate the "pivots" x^2 and xy. Why did we choose these two monomials, rather than another pair, such as y^2 and xy? We had chosen a *term ordering* which identified x^2 and xy as the "leading terms" of f_1 and f_2, respectively.

[5]Some authors distinguish between a variable and an indeterminate. For example, [**Woo04**] indicates that a variable has a solution, while an indeterminate does not. Other authors use the terms interchangeably (for example, pg. 188 of [**BWK93**]). In any case, this distinction does not matter for our purposes.

What do we mean by "leading terms"? When polynomials are univariate, this is not a difficult task: we identify the highest power of x. Consider however the polynomial $x^2 + y^2$: which term should we identify as the leading term? It is entirely possible that in some contexts, x^2 is a better candidate; in other contexts, y^2 might be better.

This gives rise to the need for a way to pick leading terms of multivariate polynomials; we call this a *term ordering*.

DEFINITION 1.5. A **term ordering** is a relation on the set $\mathcal{T}(x_1, \ldots, x_n)$ of all terms in the indeterminates $x_1, \ldots, x_n$. We denote a term ordering by $\succ$. We say that $\succ$ is **an admissible term ordering** on $\mathcal{T}(x_1, \ldots, x_n)$ if $\forall t_1, t_2, t_3 \in \mathcal{T}(x_1, \ldots, x_n)$

- either $t_1 \succ t_2$ or $t_2 \succ t_1$
- $t_1 \succ 1$ or $t_1 = 1$
- $t_1 \succ t_2$ implies $t_1 t_3 \succ t_2 t_3$

We write $t_1 \succeq t_2$ if $t_1 \succ t_2$ or $t_1 = t_2$, and we sometimes write $t_2 \prec t_1$ instead of $t_1 \succ t_2$, and $t_2 \preceq t_1$ instead of $t_1 \succeq t_2$.

We never consider term orderings that are not admissible, so for the sake of readability we refer to admissible term orderings simply as term orderings.

Any term ordering can be applied to monomials by disregarding the coefficients. It happens that two different monomials can have equal weight in a term

ordering, but this does not present a problem in practice; normally we combine like monomials, and we will consider polynomials to be in this "simplified" form.

Let's look at some common term orderings.

EXAMPLE 1.6. Let

$$g = 5x^2 - 3xy^2 + y^3$$

One way to choose the leading terms would be by picking the higher power of x; in case of a tie, we could fall back on the higher power of y. We can write this formally as:

- lex (x, y): $t_1 \succ_{\text{lex}(x,y)} t_2$ if

  $\deg_x t_1 > \deg_x t_2$;

  in the case that $\deg_x t_1 = \deg_x t_2$, if $\deg_y t_1 > \deg_y t_2$.

Another way to chose the leading terms would be by picking the higher power of y; in case of a tie, we could fall back on the higher power of x. We can write this formally as:

- lex (y, x): we say that $t_1 \succ_{\text{lex}(y,x)} t_2$ if

  $\deg_y t_1 > \deg_y t_2$;

  in the case that $\deg_y t_1 = \deg_y t_2$, if $\deg_x t_1 > \deg_x t_2$.

We call $\succ_{\text{lex}(x,y)}$ and $\succ_{\text{lex}(y,x)}$ *lexicographic* term orderings (hence the label, lex). Consider the terms $x^2, xy^2, y^3, 1$; the former has

$$x^2 \succ_{\text{lex}(x,y)} xy^2 \succ_{\text{lex}(x,y)} y^3 \succ_{\text{lex}(x,y)} 1$$

and the latter has

$$y^3 \succ_{\text{lex}(y,x)} xy^2 \succ_{\text{lex}(y,x)} x^2 \succ_{\text{lex}(y,x)} 1$$

---◇

Of course, we need our term orderings to apply to terms in more than two indeterminates. We can generalize the two term orderings of example 1.6 as follows:

DEFINITION 1.7. The **lexicographic term ordering** $\succ = \text{lex}\,(x_1, \ldots, x_n)$ gives $t_1 \succ t_2$ if

- $\deg_{x_1} t_1 > \deg_{x_1} t_2$, or
- $\deg_{x_1} t_1 = \deg_{x_1} t_2$ and

  $\deg_{x_2} t_1 > \deg_{x_2} t_2$, or
- $\ldots$
- $\deg_{x_1} t_1 = \deg_{x_1} t_2$ and

  $\ldots$ and

  $\deg_{x_{n-1}} t_1 = \deg_{x_{n-1}} t_2$ and

  $\deg_{x_n} t_1 > \deg_{x_n} t_2$.

EXAMPLE 1.8. If $\succ = \text{lex}\,(x, y, z)$, then

$$x^2y^2 \succ x^2yz \succ xy^2z \succ y^3 \succ z^5$$

As we noted above, we need term orderings to give us a precise manner of choosing leading terms for multivariate polynomials.

DEFINITION 1.9. The **leading term** of a polynomial $f = a_1t_1 + \cdots + a_rt_r$ with respect to a term ordering $\succ$ is

$$\max_{\succ} \{t_k : k = 1, \ldots, r\}$$

that is, the term t such that $t \succ u$ for every other term u of f. We write $\mathrm{lt}_{\succ}(f) = t$. If the term ordering is understood from context, we write $\overline{f} = t$.

The **leading monomial** of a polynomial f with respect to a term ordering $\succ$ is is the monomial containing $\overline{f}$. We write $m = \mathrm{lm}_{\succ}(f)$. If the term ordering is understood from context, we write $\widehat{f} = m$. The **leading coefficient** is the coefficient of $\overline{f}$ in $\widehat{f}$, written $c = \mathrm{lc}_{\succ}(f)$.

Note that

$$\mathrm{lm}_{\succ}(f) = \mathrm{lc}_{\succ}(f) \cdot \mathrm{lt}_{\succ}(f)$$

or, if the term ordering is understood from context,

$$\widehat{f} = \mathrm{lc}_{\succ}(f) \cdot \overline{f}$$

Now let's introduce a third term ordering, a *total-degree* term ordering. Here we will pick the leading term *not* by favoring one variable over another, but by favoring terms whose exponents have the highest sum. Before defining it precisely, we'll look first at an example in two variables.

EXAMPLE 1.10. Define tdeg (x, y) over terms in x, y as follows: $t_1 \succ_{\text{tdeg}(x,y)} t_2$ if the sum of the degrees in x, y of t_1 is larger than the sum of the degrees of t_2; we will break ties by the higher degree in x.

Recall from example 1.4 the term orderings lex (x, y) and lex (y, x) as well as

$$g(x, y) = 5x^2 - 3xy^2 + y^3$$

We have

$$\text{lm}_{\succ_{\text{lex}(x,y)}}(g) = 5x^2 \qquad \text{lm}_{\succ_{\text{lex}(y,x)}}(g) = y^3 \qquad \text{lm}_{\succ_{\text{tdeg}(x,y)}}(g) = -3xy^2$$

$$\text{lt}_{\succ_{\text{lex}(x,y)}}(g) = x^2 \qquad \text{lt}_{\succ_{\text{lex}(y,x)}}(g) = y^3 \qquad \text{lt}_{\succ_{\text{tdeg}(x,y)}}(g) = xy^2$$

$$\text{lc}_{\succ_{\text{lex}(x,y)}}(g) = 5 \qquad \text{lc}_{\succ_{\text{lex}(y,x)}}(g) = 1 \qquad \text{lc}_{\succ_{\text{tdeg}(x,y)}}(g) = -3$$

◇

For terms in more than two variables, we have to decide how we should break ties if the sum of the exponents is the same for two different terms. One way would be to resort to the lexicographic technique: favoring an arbitrary variable. Another way would be to disfavor an arbitrary variable: to consider the sum of all the exponents but one. If that ties, we could exclude another variable, and so forth. This latter technique is what we will take to mean the total-degree term ordering.

DEFINITION 1.11. The **total-degree term ordering**[6] $\succ = \text{tdeg}\,(x_1, \ldots, x_n)$ gives $t_1 \succ t_2$ if

- $\deg_{x_1} t_1 + \cdots + \deg_{x_n} t_1 > \deg_{x_1} t_2 + \cdots + \deg_{x_n} t_2$, or
- $\deg_{x_1} t_1 + \cdots + \deg_{x_n} t_1 = \deg_{x_1} t_2 + \cdots + \deg_{x_n} t_2$ and

  $\deg_{x_1} t_1 + \cdots + \deg_{x_{n-1}} t_1 > \deg_{x_1} t_2 + \cdots + \deg_{x_{n-1}} t_2$, or
- $\ldots$
- $\deg_{x_1} t_1 + \cdots + \deg_{x_n} t_1 = \deg_{x_1} t_2 + \cdots + \deg_{x_n} t_2$ and

  $\deg_{x_1} t_1 + \cdots + \deg_{x_{n-1}} t_1 = \deg_{x_1} t_2 + \cdots \deg_{x_{n-1}} t_2$ and

  $\ldots$ and

  $\deg_{x_1} t_1 + \deg_{x_2} t_1 = \deg_{x_1} t_2 + \deg_{x_2} t_2$ and

  $\deg_{x_1} t_1 > \deg_{x_1} t_2$.

Let's consider one last example to clarify how the total-degree term ordering behaves with more than two indeterminates:

EXAMPLE 1.12. Let $\succ = \text{tdeg}\,(x, y, z)$. Then

$$z^5 \succ x^2y^2 \succ x^2yz \succ xy^2z \succ y^3$$

Notice that in some cases, the ordering of the terms is the same as in example 1.8: $x^2y^2 \succ x^2yz$, for example. In this case, the sum of all the exponents is 4 for both

[6] This is also called the *graded reverse lexicographic* term ordering in some texts, for example definition 6 on page 56 of [**CLO97**]: *graded* refers to the consideration of the sum of a term's exponents, while *reverse lexicographic* refers to the breaking of ties by excluding the exponent of x_n, then the exponent of x_n and x_{n-1}, etc.

terms, so we have a tie. To break it, we look at the sum of the exponents of x and y, which is 4 for x^2y^2, and only 3 for x^2yz.

On the other hand, the total degree of z^5 is larger than the total degree of x^2y^2, so $z^5 \succ x^2y^2$, which was not the case in example 1.8. ◇

In view of the large amount of polynomial arithmetic that awaits us, it is advisable to consider how leading terms behave under the operations of polynomial arithmetic. The following lemma[7] provides us with a number of useful properties.

LEMMA 1.13. *For all term orderings $\succ$ and for all polynomials f_1, f_2, we have the following:*

(A) $\overline{f_1 \pm f_2} \preceq \max_{\succ}\left(\overline{f_1}\,,\,\overline{f_2}\right)$

(B) $\overline{f_1 \cdot f_2} = \overline{f_1} \cdot \overline{f_2}$

PROOF. Let $\succ$, f_1, f_2 be arbitrary, but fixed.

(A) Let $g = f_1 \pm f_2$, and let t be an arbitrary term of g. By the definition of polynomial addition, t is a term either of f_1 or of f_2. If t is a term of f_1, then $t \preceq \overline{f_1}$; otherwise, t is a term of f_2, whence $t \preceq \overline{f_2}$. In either case, $t \preceq \max_{\succ}\left(\overline{f_1}\,,\,\overline{f_2}\right)$.

(B) Let $h = f_1 \cdot f_2$, and let t be an arbitrary term of h. Then

$$t = u_1 \cdot u_2$$

[7] Adapted from lemma 5.17 on pg. 194 of [**BWK93**].

where u_1 is a term of f_1, and u_2 is a term of f_2. Clearly $u_1 \preceq \overline{f_1}$ and $u_2 \preceq \overline{f_2}$. Thus

$$t = u_1 \cdot u_2 \preceq \overline{f_1} \cdot u_2 \preceq \overline{f_1} \cdot \overline{f_2} \qquad \square$$

COROLLARY 1.14. *For all term orderings $\succ$ and for all polynomials f_1, f_2, we have the following:*

(A) $\widehat{f_1 \pm f_2} \preceq \max_{\succ} \left(\widehat{f_1}\,,\, \widehat{f_2} \right)$

(B) $\widehat{f_1 \cdot f_2} = \widehat{f_1} \cdot \widehat{f_2}$

(B) $\mathrm{lc}_{\succ}(f_1 \cdot f_2) = \mathrm{lc}_{\succ}(f_1) \cdot \mathrm{lc}_{\succ}(f_2)$

1.2.3. REDUCTION OF A POLYNOMIAL MODULO $f_1, \ldots, f_m$. The essence of reduction is obtaining a remainder by division. This is comparable to Gaussian elimination in matrices, insofar as we reduce one row of a matrix by adding multiples of other rows to it.

DEFINITION 1.15. Given polynomials $p, f, f_1, \ldots, f_m, r$ and a term ordering $\succ$, we write:

- $p \xrightarrow[f]{} r$

  if there exists a monomial q and a monomial d of p such that $q \cdot \mathrm{lm}_{\succ}(f) = d$ and $r = p - qf$

- $p \xrightarrow[q \cdot f]{} r$

  as an explicit synonym for the above

- $p \underset{f}{\not\longrightarrow}$

  if $\neg\exists r$ such that $p \underset{f}{\longrightarrow} r$

- $p \underset{(f_1,\ldots,f_m)}{\overset{*}{\longrightarrow}} r$

  if $\exists i_1, \ldots i_\mu \in \{1, \ldots, m\}$, and there exist polynomials $p_0, \ldots, p_\mu$ such that

$$p = p_0 \underset{f_{i_1}}{\longrightarrow} p_1 \underset{f_{i_2}}{\longrightarrow} p_2 \cdots \underset{f_{i_\mu}}{\longrightarrow} p_\mu = r$$

  In this case, we say p **reduces to** r **modulo** $(f_1, \ldots, f_m)$.

EXAMPLE 1.16. Let

$$f_1 = x^2 + x + 1 \qquad f_2 = xy \qquad p = x^2y + y$$

For *every* term ordering $\succ$ we have

$$\begin{aligned} \overline{f_1} &= x^2 \\ \overline{f_2} &= xy \end{aligned}$$

Then

$$p \underset{y \cdot f_1}{\longrightarrow} xy \underset{1 \cdot f_2}{\longrightarrow} 0$$

◇

The reader should note that *a reduction path is not unique!* It frequently happens that different remainders follow from different reduction paths.[8] For instance, in

[8]For Gröbner bases, however, this phenomenon does not occur; one property of Gröbner bases is that reduction over a Gröbner basis gives the same remainder regardless of the reduction path.

example 1.16, we could have reduced

$$p \underset{x\cdot f_2}{\longrightarrow} y \overset{*}{\underset{(f_1,f_2)}{\not\rightarrow}}$$

Hence

$$p \overset{*}{\underset{(f_1,f_2)}{\longrightarrow}} 0 \qquad \text{and} \qquad p \overset{*}{\underset{(f_1,f_2)}{\longrightarrow}} y$$

1.2.4. FORMAL DEFINITION OF A GRÖBNER BASIS. We introduced Gröbner bases with an analogy from linear algebra; namely, comparing them to the "nice form" provided by Gaussian elimination. In the case of linear polynomials, this "nice form" is a basis of the vector space generated by $f_1, \ldots, f_m$. We will define Gröbner bases by drawing an analogy with a property of bases of vector spaces.

Recall from linear algebra that for polynomials $f_1, \ldots, f_m$, if $\{b_1, \ldots, b_M\}$ is a basis of the vector space

$$\mathcal{V} = \{c_1 f_1 + \cdots + c_m f_m : c_k \in \mathbb{F}\}$$

then for all $v \in \mathcal{V}$, Gaussian elimination of v over $b_1, \ldots, b_M$ compares to polynomial reduction of v by $b_1, \ldots, b_M$; indeed

$$v = v_0 \underset{(b_1,\ldots,b_M)}{\longrightarrow} v_1 \underset{(b_1,\ldots,b_M)}{\longrightarrow} \cdots \underset{(b_1,\ldots,b_M)}{\longrightarrow} v_M = 0$$

In other words, $v \overset{*}{\underset{(b_1,\ldots,b_M)}{\longrightarrow}} 0$. Note that the resulting quotients give co-ordinates of v with respect to $b_1, \ldots, b_M$. This follows from the fact that the b_k generate the vector space.

EXAMPLE 1.17. Let

$$f_1 = x + y$$

$$f_2 = y + 1$$

Note that x is a monomial of f_1, but not of f_2; hence the two polynomials are linearly independent, thus a basis for

$$\mathcal{V} = \{c_1 f_1 + c_2 f_2 : c_1, c_2 \in \mathbb{Q}\}$$

Let $g = 10f_1 - 10f_2$. Clearly $g \in \mathcal{V}$. Then

$$g = 10x - 10 \underset{10\cdot f_1}{\longrightarrow} -10y - 10 \underset{-10\cdot f_2}{\longrightarrow} 0$$

Notice that the quotients give the co-ordinates of g with respect to f_1, f_2. ———◇

Now define

$$\mathcal{I}(f_1, \ldots, f_m) = \{h_1 f_1 + \cdots + h_m f_m : h_k \in \mathbb{F}[x_1, \ldots, x_n]\}$$

We define a Gröbner basis as if it gave a non-linear generalization of the above property of the basis of a vector space.

DEFINITION 1.18. We say that $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ are **a Gröbner basis with respect to the term ordering** $\succ$ if for every $p \in \mathcal{I}$ we have $p \underset{(f_1,\cdots,f_m)}{\overset{*}{\longrightarrow}} 0$.[9]

[9]This is not the only way to define a Gröbner basis. Our definition comes from **[BWK93]** (definition 5.37 on page 207 and condition (v) of theorem 5.35 on page 206). The interested reader can find other definitions:

If $f_1, \ldots, f_m$ are a Gröbner basis, then we may write $\mathrm{GB}_{\succ}(f_1, \ldots, f_m)$ for short.

To familiarize ourselves with this definition, we reconsider the polynomials of examples 1.1 and 1.2.

EXAMPLE 1.19. Let

$$f_1 = 2x + 3y + 1$$

$$f_2 = x + y$$

Notice that f_1, f_2 are derived from 1.1 on page 3.

To work in Gröbner bases, we need a term ordering, say $\succ = \mathrm{lex}(x, y)$. Thus

$$\overline{f_1} = x \qquad \overline{f_2} = x$$

We claim that f_1, f_2 are *not* a Gröbner basis with respect to $\succ$. *Why not?*

Let

$$\begin{aligned} p &= 1 \cdot f_1 - 2 \cdot f_2 \\ &= (2x + 3y + 1) - 2(x + y) \\ &= y + 1 \end{aligned}$$

- **[CLO98]** (definition 3.1 on page 12), **[Coh03]** (definition 8.30 on page 324), and more generally **[Eis95]** define a Gröbner basis so that for every $p \in \mathcal{I}$, we have $\overline{f_i} \mid \overline{g}$ for some $i = 1, \ldots, m$;
- **[CLO97]** (Definition 5 on page 74) and **[vzGG99]** (definition 21.25 on page 579) use the definition that the ideal of the leading terms of $f_1, \ldots, f_m$ equals the ideal of the leading terms of all $p \in \mathcal{I}$.

Both these definitions also appear in **[BWK93]** (definition 5.37 on page 207 and condition (viii) of theorem 5.35 on page 206). It should come as no surprise that these definitions are equivalent; proving this fact is the point of theorem 5.35 of **[BWK93]**.

(Notice that p is the polynomial we obtained by Gaussian elimination in example 1.1.)

Certainly $p \in \mathcal{I}(f_1, f_2)$. However, neither $\overline{f_1}$ nor $\overline{f_2}$ divides any term of p. Hence

$$p \underset{(f_1,f_2)}{\not\twoheadrightarrow}$$

which implies that

$$p \underset{(f_1,f_2)}{\overset{*}{\not\twoheadrightarrow}} 0$$

Since f_1, f_2 do not satisfy definition 1.18, they are not a Gröbner basis. ——————◇

EXAMPLE 1.20. This time, let f_1, f_2 be as in example 1.2:

$$f_1 = x^2 + y^2$$

$$f_2 = xy$$

Again, let $\succ$= lex (x, y), so

$$\overline{f_1} = x^2 \quad \overline{f_2} = xy$$

We claim that f_1, f_2 are not a Gröbner basis. Let

$$\begin{aligned} p &= y \cdot f_1 - x \cdot f_2 \\ &= \left(x^2y + y^3\right) - x^2y \\ &= y^3 \end{aligned}$$

(Notice that p is the polynomial f_3 that we identified in example 1.2.)

Certainly $p \in \mathcal{I}(f_1, f_2)$. However, neither $\overline{f_1}$ nor $\overline{f_2}$ divides any term of p. Hence

$$p \underset{(f_1,f_2)}{\not\rightarrow}$$

which implies that

$$p \underset{(f_1,f_2)}{\overset{*}{\not\rightarrow}} 0$$

Since f_1, f_2 do not satisfy definition 1.18, they are not a Gröbner basis. ◇

At the end of example 1.2, we claimed that by appending f_3, we did have the "nice form." In essence, we were claiming that f_1, f_2, f_3 are a Gröbner basis with respect to $\succ$. We would like to show this, but we cannot yet sit down and verify that for all $p \in \mathcal{I}(f_1, f_2, f_3)$, $p \underset{(f_1,f_2,f_3)}{\overset{*}{\longrightarrow}} 0$.

How do we prove this claim?

1.3. GRÖBNER BASES: DECISION

Definition 1.18 does not suggest an algorithm that will decide whether the polynomials $f_1, \ldots, f_m$ are a Gröbner basis. We cannot apply the definition directly, since it is universally quantified over the p, and we would have to test infinitely many $p \in \mathcal{I}(f_1, \ldots, f_m)$.

In order to check whether some given polynomials are a Gröbner basis, we need equivalent conditions that *are not* universally quantified over $\mathcal{I}$. We present these conditions as theorem 1.30 of section 1.3.3. Before we can present theorem 1.30, however, we have two more items of background material.[10]

1.3.1. S-POLYNOMIALS. For linear polynomials, we cancel the *pivots* by multiplying appropriate *scalar* factors. For non-linear polynomials, we cancel the *leading terms* by multiplying appropriate *monomial* factors. The construction that accomplishes this is the S-polynomial:

DEFINITION 1.21. For polynomials f_1, f_2 and for a term ordering $\succ$

$$S_{\succ}(f_1, f_2) = \frac{\operatorname{lcm}(\operatorname{lt}_{\succ}(f_1), \operatorname{lt}_{\succ}(f_2))}{\operatorname{lm}_{\succ}(f_1)} \cdot f_1 - \frac{\operatorname{lcm}(\operatorname{lt}_{\succ}(f_1), \operatorname{lt}_{\succ}(f_2))}{\operatorname{lm}_{\succ}(f_2)} \cdot f_2$$

We call $S_{\succ}(f_1, f_2)$ **the S-polynomial of f_1 and f_2**; the S stands for *subtraction*.[11] When the term ordering $\succ$ is understood from the context, we will write S_{f_1,f_2} or even $S_{1,2}$.

[10]There is also the question of how to compute a Gröbner basis for $f_1, \ldots, f_m$ in the case where they are not a Gröbner basis themselves. There are several well-known algorithms for this: Bruno Buchberger's algorithm of [**Buc65**] is the most famous, and more recently there are Faugère's algorithms F_4 [**Fau99**] and F_5 [**Fau02**]. All these algorithms require a sub-algorithm that decides whether a set of polynomials is a Gröbner basis; this is the focus of our particular research A discussion of Gröbner basis computation lies beyond the scope of this thesis, and we refer the reader to the sources.

[11]Buchberger refers to the S-polynomial as a *subtraction* polynomial in his thesis [**Buc65**], although Cox, Little, and O'Shea refer to it as a *syzygy* polynomial in their text [**CLO97**]. The latter authors are trying to place S-polynomials in this very important context of syzygies.

Note that $S_{i,j} = -S_{j,i}$. As a result, we consider only the S-polynomials with $i < j$.

The polynomials p of examples 1.19 on page 20 and 1.20 on page 21 were formed by a construction very similar to that of S-polynomials. Compare their results to examples 1.22 and 1.23.

EXAMPLE 1.22. Let

$$f_1 = 2x + 3y + 1$$

$$f_2 = x + y$$

We will use $\succ = \text{lex}\,(x, y)$. Then

$$\begin{aligned} S_{1,2} &= \frac{\text{lcm}\,(x,x)}{2x} \cdot (2x + 3y + 1) - \frac{\text{lcm}\,(x,x)}{x} \cdot (x + y) \\ &= \frac{x}{2x} \cdot (2x + 3y + 1) - \frac{x}{x} \cdot (x + y) \\ &= \frac{1}{2} \cdot (2x + 3y + 1) - (x + y) \\ &= x + \frac{3}{2} \cdot y + \frac{1}{2} - x - y \\ &= \frac{1}{2} \cdot y + \frac{1}{2} \end{aligned}$$

Notice that $S_{1,2}$ is a constant multiple of p in example 1.19 on page 20, which, as we noted, is the polynomial we found by Gaussian elimination in example 1.1 on page 3. ◇

EXAMPLE 1.23. Let

$$\begin{aligned} f_1 &= x^2 + y^2 \\ f_2 &= xy \end{aligned}$$

Again, let $\succ = \text{lex}\,(x, y)$. This gives us

$$\begin{aligned} \widehat{f_1} &= x^2 \\ \widehat{f_2} &= xy \end{aligned}$$

Then

$$\begin{aligned} S_{1,2} &= \frac{\text{lcm}\,(x^2, xy)}{x^2} \cdot \left(x^2 + y^2\right) - \frac{\text{lcm}\,(x^2, xy)}{xy} \cdot xy \\ &= \frac{x^2 y}{x^2} \cdot \left(x^2 + y^2\right) - \frac{x^2 y}{xy} \cdot xy \\ &= y \cdot \left(x^2 + y^2\right) - x \cdot xy \\ &= \left(x^2 y + y^3\right) - x^2 y \\ &= y^3 \end{aligned}$$

Compare this to f_3 and p in examples 1.2 on page 4 and 1.20 on page 21, respectively. ◇

We leave it as an exercise for the reader to show that, for the polynomials given in example 1.23,

$$S_{\succ_{\text{lex}(x,y)}}\,(f_1, f_2) = S_{\succ_{\text{tdeg}(x,y)}}\,(f_1, f_2)$$

However, the S-polynomial can also change if we change the term ordering, as illustrated by example 1.24.

EXAMPLE 1.24. Let f_1, f_2 be as in example 1.23. This time, let $\succ = \text{lex}\,(y, x)$. Now we have $\widehat{f_1} = y^2$. Then

$$\begin{aligned} S_{1,2} &= \frac{\text{lcm}\,(y^2, xy)}{y^2} \cdot \left(x^2 + y^2\right) - \frac{\text{lcm}\,(y^2, xy)}{xy} \cdot xy \\ &= \frac{xy^2}{y^2} \cdot \left(x^2 + y^2\right) - \frac{xy^2}{xy} \cdot xy \\ &= x \cdot \left(x^2 + y^2\right) - y \cdot xy \\ &= \left(x^3 + xy^2\right) - xy^2 \\ &= x^3 \end{aligned}$$

The following lemma formalizes the observation that S-polynomials eliminate leading terms, and it provides an unreachable "upper bound" for the leading terms of S-polynomials.

LEMMA 1.25. *For all* $f_i, f_j \in \mathbb{F}[x_1, \ldots, x_n]$

$$\overline{S_{i,j}} \prec \text{lcm}\left(\overline{f_i}\,,\, \overline{f_j}\right)$$

PROOF. Let $f_i, f_j \in \mathbb{F}[x_1, \ldots, x_n]$ be arbitrary, but fixed. Recall that

$$S_{i,j} = \frac{\text{lcm}\left(\overline{f_i}\,,\, \overline{f_j}\right)}{\overline{f_i}} \cdot f_i - \frac{\text{lcm}\left(\overline{f_i}\,,\, \overline{f_j}\right)}{\overline{f_i}} \cdot f_i$$

Write $f_i = \widehat{f_i} + R_i$ and $f_j = \widehat{f_j} + R_j$. Then

$$\begin{aligned} S_{i,j} =& \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}} \cdot \left(\widehat{f_i} + R_i\right) - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}} \cdot \left(\widehat{f_j} + R_j\right) \\ =& \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right) + \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}} \cdot R_i - \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right) - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}} \cdot R_j \\ =& \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}} \cdot R_i - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_j}} \cdot R_j \end{aligned}$$

Clearly,

$$\overline{S_{i,j}} = \max_{\succ} \left(\overline{\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}} \cdot R_i}, \overline{\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_j}} \cdot R_j} \right)$$

Observe that

$$\begin{aligned} \overline{\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}} \cdot R_i} &= \overline{\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}}} \cdot \overline{R_i} \\ &\prec \overline{\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}}} \cdot \overline{f_i} \\ &= \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right) \end{aligned}$$

Similarly,

$$\overline{\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\overline{f_i}} \cdot R_i} \prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)$$

Thus

$$\overline{S_{i,j}} \prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right) \qquad \square$$

1.3.2. REPRESENTATION OF AN S-POLYNOMIAL MODULO $f_1, \ldots, f_m$. Suppose we perform Gaussian elimination on the linear polynomials $f_1, \ldots, f_m$ and obtain the

linear basis $b_1, \ldots, b_M$. We alluded in example 1.17 on page 18 to the fact that if

$$p = c_1 f_1 + \cdots + c_m f_m$$

where the c_k are scalars in the base field, then we can represent p in terms of $b_1, \ldots, b_M$ by its co-ordinates.

We extend this idea to the concept of the representation of an S-polynomial modulo $f_1, \ldots, f_m$:[12]

DEFINITION 1.26. We say that $h_1, \ldots, h_m$ **give a representation of** $S_{i,j}$ **modulo** $f_1, \ldots, f_m$ if

$$S_{i,j} = h_1 f_1 + \cdots + h_m f_m$$

and for every $k = 1, \ldots, m$ $h_k \neq 0$ implies

$$\overline{h_k} \cdot \overline{f_k} \prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)$$

If $\exists h_1, \ldots, h_m$ such that $h_1, \ldots, h_m$ give a representation of $S_{i,j}$ modulo $f_1, \ldots, f_m$, we say that $S_{i,j}$ **has a representation modulo** $f_1, \ldots, f_m$. We often omit the modulus if it is obvious from context.

With linear polynomials, we can find a representation for a polynomial p by performing row-reduction operations on p using the basis $b_1, \ldots, b_M$. It turns out

[12]We could define this more generally; see the *standard representation of a polynomial* on page 218 of [**BWK93**]. For our purposes, the notion of an *S-polynomial representation* (a special case of the *t-representation* on page 219 of [**BWK93**]) will suffice.

that we can do something similar in the non-linear case using reduction and representation. If we collect the monomial quotients of a reduction path, we can obtain sample h_k by adding the all monomial quotients for f_k. We illustrate this in example 1.27.

EXAMPLE 1.27. Let

$$f_1 = x^2 + x + 1 \qquad f_2 = y - 1$$

Let $\succ$ be any term ordering. Then

$$\overline{f_1} = x^2 \qquad \overline{f_2} = y$$

We have

$$\begin{aligned} S_{1,2} =& \frac{\operatorname{lcm}(x^2, y)}{x^2} \cdot \left(x^2 + x + 1\right) - \frac{\operatorname{lcm}(x^2, y)}{y} \cdot (y - 1) \\ =& y \cdot \left(x^2 + x + 1\right) - x^2 \cdot (y - 1) \\ =& x^2 + xy + y \end{aligned}$$

Then

$$S_{1,2} \underset{1 \cdot f_1}{\longrightarrow} xy + y - x - 1 \underset{x \cdot f_2}{\longrightarrow} y - 1 \underset{1 \cdot f_2}{\longrightarrow} 0$$

Collecting and negating the monomials of the reduction path, we see that

$$S_{1,2} = h_1 f_1 + h_2 f_2$$

where

$$h_1 = 1 \qquad h_2 = x + 1$$

We have

$$\overline{h_1} \cdot \overline{f_1} = 1 \cdot x^2 \prec x^2 y = \operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right)$$

$$\overline{h_2} \cdot \overline{f_2} = x \cdot y \prec x^2 y = \operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right)$$

So h_1 and h_2 give us a representation of $S_{1,2}$. ◇

Generalizing the above, we have the following lemma:

LEMMA 1.28. *Let $f_1, \ldots, f_m$ be polynomials. For all $1 \leq i < j \leq m$ we have (A)⇒(B) where*

(A) $S_{i,j} \xrightarrow[(f_1,\cdots,f_m)]{*} 0$

(B) $S_{i,j}$ has a representation modulo $f_1, \ldots, f_m$

PROOF. Let $i \neq j$ be arbitrary, but fixed.

We want to show (A)⇒(B), so assume (A).

Then

$$S_{i,j} \xrightarrow[(f_1,\cdots,f_m)]{*} 0$$

Write out an explicit reduction path

$$S_{i,j} = p_0 \underset{q_1 \cdot f_{i_1}}{\longrightarrow} p_1 \underset{q_2 \cdot f_{i_2}}{\longrightarrow} \cdots \underset{q_r \cdot f_{i_r}}{\longrightarrow} p_r = 0 \tag{1.1}$$

Notice that by the definition of reduction and lemma 1.25 on page 26, we have for all $\ell = 1, \ldots, r$

$$\overline{q_\ell \cdot f_{i_\ell}} \preceq \overline{p_{\ell-1}} \preceq \cdots \preceq \overline{p_0} = \overline{S_{i,j}} \prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)$$

Working backwards in (1.1), we see that

$$\begin{aligned} 0 = p_r =& p_r - q_r \cdot f_{i_r} \\ =& \left(p_{r-2} - q_{r-1} \cdot f_{i_{r-1}}\right) - q_r \cdot f_{i_r} \\ & \vdots \\ =& p_0 - q_1 \cdot f_{i_1} - \cdots - q_{r-1} \cdot f_{i_{r-1}} - q_r \cdot f_{i_r} \end{aligned}$$

Thus

$$p_0 = q_1 \cdot f_{i_1} + \cdots + q_r \cdot f_{i_r}$$

Since $p_0 = S_{i,j}$, we have

$$S_{i,j} = q_1 \cdot f_{i_1} + \cdots + q_r \cdot f_{i_r}$$

For $k = 1, \ldots, m$ let $h_k = \sum q_j$ such that $q_j \cdot f_k$ appears in the above equation.

Then

$$S_{i,j} = h_1 f_1 + \cdots + h_m f_m$$

and $h_k \neq 0$ implies that

$$\overline{h_k} \cdot \overline{f_k} = \max_{\succ} \left(\overline{q_j} : q_j \cdot f_k \text{ appears above} \right) \prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j} \right) \qquad \square$$

The reader should take heed that *the converse of the above lemma is not, in general, true, even if p is restricted to S-polynomials!* Consider the following example:

EXAMPLE 1.29. Let

$$\begin{aligned} f_1 &= x^3y^2 + 1 \\ f_2 &= x^2y^3 + 1 \\ f_3 &= x^2y + 1 \\ f_4 &= xy^2 + 1 \end{aligned}$$

Let $\succ$ be any admissible term ordering. Observe that

$$\overline{f_1} = x^3y^2 \qquad \overline{f_2} = x^2y^3 \qquad \overline{f_3} = x^2y \qquad \overline{f_4} = xy^2$$

We have

$$\begin{aligned} S_{1,2} &= \frac{\operatorname{lcm}\left(x^3y^2, x^2y^3\right)}{x^3y^2} \cdot \left(x^3y^2 + 1\right) - \frac{\operatorname{lcm}\left(x^3y^2, x^2y^3\right)}{x^2y^3} \cdot \left(x^2y^3 + 1\right) \\ &= y \cdot \left(x^3y^2 + 1\right) - x \cdot \left(x^2y^3 + 1\right) \\ &= y - x \end{aligned}$$

Let

$$h_1 = 0 \qquad h_2 = 0 \qquad h_3 = y \qquad h_4 = -x$$

Then

$$\begin{aligned} h_1f_1 + h_2f_2 + h_3f_3 + h_4f_4 &= y\left(x^2y + 1\right) - x\left(xy^2 + 1\right) \\ &= y - x \end{aligned}$$

So

$$S_{1,2} = h_1 f_1 + h_2 f_2 + h_3 f_3 + h_4 f_4$$

Furthermore,

$$\overline{h_3} \cdot \overline{f_3} = \overline{h_4} \cdot \overline{f_4} = x^2 y^2 \prec x^3 y^3 = \operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right)$$

So for $S_{1,2}$, we have satisfied (B) of lemma 1.28.

However, for $k = 1, 2, 3, 4$ $\overline{f_k} \nmid x$ and $\overline{f_k} \nmid y$, so

$$S_{1,2} \underset{(f_1, \cdots, f_4)}{\not\longrightarrow}$$

As a consequence,

$$S_{1,2} \underset{(f_1, \cdots, f_4)}{\overset{*}{\not\longrightarrow}} 0$$

◇

1.3.3. EQUIVALENT CONDITIONS FOR A GRÖBNER BASIS. Because they capture completely the cancellation of leading monomials, S-polynomials provide the critical key for determining whether $f_1, \ldots, f_m$ are a Gröbner basis with respect to a term ordering $\succ$. Definition 1.18 requires us to verify that *every* polynomial in $\mathcal{I}(f_1, \ldots, f_m)$ reduces to zero; however, there are infinitely many polynomials, so we cannot create an algorithm directly. Theorem 1.30 will circumvent this obstacle: we only have to check that a finite number of polynomials reduce to zero: namely, all the S-polynomials for $f_1, \ldots, f_m$. Moreover, we do not even have to reduce them

to zero; the theorem shows that having representations for all the S-polynomials is also equivalent.

THEOREM 1.30. *For all $f_1, \ldots, f_m$ and for all $\succ$, the following are equivalent.*

(A) $f_1, \ldots, f_m$ are a Gröbner basis with respect to $\succ$.

(B) for all $1 \leq i < j \leq m$, $S_{i,j} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$.

(C) for all $1 \leq i < j \leq m$, $S_{i,j}$ has a representation modulo $f_1, \ldots, f_m$.

The proof is rather long, so we present it at the end of the section. We precede the proof with an algorithm that follows naturally from clause (B), and with some examples.

First, a caution on what the theorem does *not* say. The positions of the quantifiers are *essential*; it is *not* the case that

$$\forall 1 \leq i < j \leq m \quad \left[S_{i,j} \xrightarrow[(f_1,\ldots,f_m)]{*} 0 \;\Leftrightarrow\; S_{i,j} \text{ has a representation modulo } f_1, \ldots, f_m \right]$$

(Recall example 1.29 on page 31.)

AN ALGORITHM FOR THEOREM 1.30. Clause (B) of theorem 1.30 lends itself naturally to an algorithm to decide whether a system of polynomials are a Gröbner basis with respect to a given term ordering, and we present this as algorithm 1.1.

The algorithm is a straightforward implementation of theorem 1.30, so it clearly terminates correctly.

Algorithm 1.1 Is_GB

Inputs: $\succ$, $f_1, \ldots, f_m$

Output: YES if $f_1, \ldots, f_m$ are a Gröbner basis with respect to $\succ$; NO otherwise.

$\mathcal{B} \leftarrow \{(i,j) : 1 \leq i < j \leq m\}$

For $(i,j) \in \mathcal{B}$ **Do**

If $S_{i,j} \underset{(f_1,\ldots,f_m)}{\overset{*}{\nrightarrow}} 0$ **Then**

Return FALSE

Return TRUE

EXAMPLES OF THEOREM 1.30. Now for some examples. The first ones are those that we could not verify previously. The first example is the linear system derived from example 1.1 on page 3.

EXAMPLE 1.31. Recall from example 1.22 on page 24

$$f_2 = x + y$$

Let

$$f_3 = y + 1$$

Notice $f_3 = S_{1,2}$ (where $f_1 = 2x + 3y + 1$ as in example 1.22).

We claim that f_2, f_3 are a Gröbner basis with respect to $\succ$. Observe that

$$\begin{aligned} S_{2,3} =& \frac{\operatorname{lcm}(x,y)}{x} \cdot (x+y) - \frac{\operatorname{lcm}(x,y)}{y} \cdot (y+1) \\ =& \left(xy + y^2\right) - (xy + x) \\ =& y^2 - x \end{aligned}$$

Then

$$S_{2,3} \underset{f_2}{\longrightarrow} y^2 + y \underset{-2y \cdot f_3}{\longrightarrow} 0$$

By theorem 1.30, f_2, f_3 are a Gröbner basis with respect to $\succ$. ◇

We leave it as an exercise to the reader to show that f_1, f_2, f_3 from example 1.22 on page 24 are also a Gröbner basis with respect to $\succ$. However, it is not necessary to include f_1 in the Gröbner basis, since $f_1 \in \mathcal{I}(f_2, f_3)$:

$$f_1 = 2f_2 + f_3$$

Recalling example 1.2 on page 4, we now show that the non-linear f_1, f_2, f_3 *do* have the "nice form", *and* that we cannot drop any one of the three.

EXAMPLE 1.32. Let $\succ = \text{lex}(x, y)$. Recall from examples 1.2 on page 4 and 1.23 on page 25

$$f_1 = x^2 + y^2$$

$$f_2 = xy$$

$$f_3 = y^3$$

According to theorem 1.30, we need to verify that $S_{1,2}, S_{1,3}, S_{2,3}$ all reduce to zero over f_1, f_2, f_3.

We saw in example 1.23 on page 25 that $S_{1,2} = f_3$, so

$$S_{1,2} \underset{(f_1, f_2, f_3)}{\overset{*}{\longrightarrow}} 0$$

We also have

$$\begin{aligned} S_{1,3} =& \frac{\operatorname{lcm}\left(x^2, y^3\right)}{x^2} \cdot \left(x^2 + y^2\right) - \frac{\operatorname{lcm}\left(x^2, y^3\right)}{y^3} \cdot y^3 \\ =& \left(x^2 y^3 + y^5\right) - x^2 y^3 \\ =& y^5 \end{aligned}$$

Here

$$S_{1,3} \underset{y^2 \cdot f_3}{\longrightarrow} 0$$

so

$$S_{1,3} \underset{(f_1, f_2, f_3)}{\overset{*}{\longrightarrow}} 0$$

Finally, $S_{2,3} = 0$ so $S_{2,3} \underset{(f_1, f_2, f_3)}{\overset{*}{\longrightarrow}} 0$.

Since all of $S_{1,2}, S_{1,3}, S_{2,3}$ reduce to zero over f_1, f_2, f_3, theorem 1.30 informs us that f_1, f_2, f_3 are a Gröbner basis with respect to $\succ$. ◇

The reader should note that the steps we followed in example 1.32 are not only the steps necessary to verify that clause (B) of theorem 1.30 holds, but they are also the precise steps that we followed in example 1.2 on page 4, a generalization of Gaussian elimination.

The choice of term ordering can affect whether a set of polynomials is a Gröbner basis. This should make sense, since we have seen already that changing the term ordering can change the leading terms, the S-polynomials, and the possible reduction paths – in other words, everything can hinge on the term ordering.

Example 1.33 illustrates this fact. We reconsider the polynomials of example 1.32 using a different term ordering.

EXAMPLE 1.33. Let f_1, f_2, f_3 be as in example 1.2; that is,

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

We claim that f_1, f_2, f_3 are *not* a Gröbner basis with respect to $\succ = \text{lex}\,(y, x)$.

Notice first that one of the leading terms has changed! We now have

$$\overline{f_1} = y^2 \qquad \overline{f_2} = xy \qquad \overline{f_4} = y^3$$

Then

$$\begin{aligned} S_{1,2} =& \frac{\text{lcm}\,(y^2, xy)}{y^2} \cdot \left(x^2 + y^2\right) - \frac{\text{lcm}\,(y^2, xy)}{xy} \cdot xy \\ =& \left(x^3 + xy^2\right) - xy^2 \\ =& x^3 \end{aligned}$$

We cannot carry out a single reduction! Hence

$$S_{1,2} \underset{(f_1,f_2,f_3)}{\overset{*}{\nrightarrow}} 0$$

We conclude that f_1, f_2, f_3 are not a Gröbner basis with respect to $\succ$. ◇

PROOF OF THEOREM 1.30. We conclude section 1.3.3 with a proof of theorem 1.30.

First, we restate the theorem:

THEOREM. *For all $f_1, \ldots, f_m$ and for all $\succ$, the following are equivalent.*

(A) $f_1, \ldots, f_m$ are a Gröbner basis with respect to $\succ$.

(B) for all $1 \leq i < j \leq m$, $S_{i,j} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$.

(C) for all $1 \leq i < j \leq m$, $S_{i,j}$ has a representation modulo $f_1, \ldots, f_m$.

The proof has three major sections:

- (A)⇒(B) (short)
- (B)⇒(C) (very short)
- (C)⇒(A) (long: pages 40 – 48)

PROOF. (Of theorem 1.30)

Let $f_1, \ldots, f_m$, and $\succ$ be arbitrary, but fixed.

(A)⇒(B): Assume (A). So $f_1, \ldots, f_m$ are a Gröbner basis with respect to $\succ$.

Let $i < j$ satisfy (B).

Recall that

$$S_{i,j} = \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_i}} \cdot f_i - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_j}} \cdot f_j$$

We have

$$S_{i,j} = h_1 f_1 + \cdots + h_m f_m$$

where

$$\begin{aligned} h_i =& \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_i}} \cdot f_i \\ h_j =& \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_j}} \cdot f_j \\ h_k =& 0 \ \forall k \neq i,j \end{aligned}$$

Then

$$S_{i,j} \in \mathcal{I}\left(f_1, \ldots, f_m\right)$$

Recall that $f_1, \ldots, f_m$ are a Gröbner basis. Hence, for every $p \in \mathcal{I}\left(f_1, \ldots, f_m\right)$, $p \xrightarrow[(f_1,\ldots,f_m)]{*} 0$. In particular, $S_{i,j} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$.

But i, j were arbitrary. Hence (B).

(B)⇒(C): This is a consequence of lemma 1.28 on page 30.

(C)⇒(A): Assume (C).[13]

Abbreviate $\mathcal{I}\left(f_1, \ldots, f_m\right)$ as $\mathcal{I}$. We have to show that $p \xrightarrow[(f_1,\ldots,f_m)]{*} 0$ for every $p \in \mathcal{I}$.

We proceed in three steps, each of which is a claim. Claim 1 is by far the longest.

Claim 1. We claim that for every nonzero $p \in \mathcal{I}$ $\exists h_1, \ldots, h_m$ such that

$$p = h_1 f_1 + \cdots + h_m f_m \tag{1.2}$$

and $\forall k = 1, \ldots, m$ $\overline{h_k} \cdot \overline{f_k} \preceq \overline{p}$.

Let $p \in \mathcal{I}$ be arbitrary, but fixed.

[13]The following is derived from the proofs of theorem 5.64, lemma 5.61, and theorem 5.35 of [**BWK93**].

Let

$$\mathcal{R} = \{(h_1, \ldots, h_m) : \ p = h_1 f_1 + \cdots + h_m f\}$$

and

$$\mathcal{S} = \left\{\max\left(\overline{h_1} \cdot \overline{f_1}, \ldots, \overline{h_m} \cdot \overline{f_m}\right) : \ (h_1, \ldots, h_m) \in \mathcal{R}\right\}$$

Since $\mathcal{S} \subset \mathcal{T}(x_1, \ldots, x_n)$, $\mathcal{S}$ has a least element with respect to $\succ$; call it s.

Clearly $s \succeq \overline{p}$: we have $s \succ \overline{p}$ only if two terms on the right-hand side of (1.2) cancel. We claim that by choosing $h_1, \ldots, h_m$ so that s is minimal, we have $\overline{p} = s$. Note that this would imply claim 1.

By way of contradiction, assume that $s \succ \overline{p}$. Then the terms on the right-hand side of (1.2) that contain s must cancel.

Let n be the number of leading terms of the $h_k f_k$ such that $\overline{h_k} \cdot \overline{f_k} = s$. Note that $n > 1$.

We claim that if for some $M \leq n$

$$s = \overline{h_{k_1}} \cdot \overline{f_{k_1}} = \cdots = \overline{h_{k_M}} \cdot \overline{f_{k_M}}$$

and

$$\widehat{h_{k_1}} \cdot \widehat{f_{k_1}} + \cdots + \widehat{h_{k_M}} \cdot \widehat{f_{k_M}} = 0$$

then we can rewrite

$$h_{k_1} f_{k_1} + \cdots + h_{k_M} f_{k_M} \tag{1.3}$$

such that

$$s' = \max_{\succ} \left\{ \overline{h_{k_\ell}} \cdot \overline{f_{k_\ell}} : \ell = 1, \ldots, M \right\} \prec s$$

We proceed by induction on M.

Inductive base: Assume that $M = 2$. Without loss of generality,

$$\overline{h_1} \cdot \overline{f_1} = \overline{h_2} \cdot \overline{f_2} = s$$

and

$$\widehat{h_1} \cdot \widehat{f_1} + \widehat{h_2} \cdot \widehat{f_2} = 0$$

Thus

$$\operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right) \mid s$$

Let u be such that

$$u \cdot \operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right) = s$$

Let $a_k = \operatorname{lc}_{\succ}(h_k)$ and $b_k = \operatorname{lc}_{\succ}(f_k)$; then

$$a_1 b_1 = -a_2 b_2$$

Put

$$c = a_1 b_1 = -a_2 b_2$$

Then

$$\begin{aligned} \widehat{h_1} \cdot f_1 + \widehat{h_2} \cdot f_2 =& a_1 \overline{h_1} \cdot f_1 + a_2 \overline{h_2} \cdot f_2 \\ =& a_1 \overline{h_1} \cdot \widehat{f_1} \cdot \frac{f_1}{\widehat{f_1}} + a_2 \overline{h_2} \cdot \widehat{f_2} \cdot \frac{f_2}{\widehat{f_2}} \end{aligned}$$

$$
\begin{aligned}
&= a_1 \overline{h_1} \cdot b_1 \overline{f_1} \cdot \frac{f_1}{\widehat{f_1}} + a_2 \overline{h_2} \cdot b_2 \overline{f_2} \cdot \frac{f_2}{\widehat{f_2}} \\
&= c \cdot \overline{h_1} \cdot \overline{f_1} \cdot \frac{f_1}{\widehat{f_1}} - c \cdot \overline{h_2} \cdot \overline{f_2} \cdot \frac{f_2}{\widehat{f_2}} \\
&= cs \cdot \frac{f_1}{\widehat{f_1}} - cs \cdot \frac{f_2}{\widehat{f_2}} \\
&= cs \cdot \left(\frac{f_1}{\widehat{f_1}} - \frac{f_2}{\widehat{f_2}} \right) \\
&= c \cdot u \cdot \operatorname{lcm}\left(\overline{f_1}, \overline{f_2} \right) \cdot \left(\frac{f_1}{\widehat{f_1}} - \frac{f_2}{\widehat{f_2}} \right) \\
&= cu \cdot \left(\frac{\operatorname{lcm}\left(\overline{f_1}, \overline{f_2} \right)}{\widehat{f_1}} \cdot f_1 - \frac{\operatorname{lcm}\left(\overline{f_1}, \overline{f_2} \right)}{\widehat{f_2}} \cdot f_2 \right) \\
&= cu \cdot S_{1,2}
\end{aligned}
$$

We had assumed (C), so there exist $H_1, \ldots, H_m$ such that

$$S_{1,2} = H_1 f_1 + \cdots + H_m f_m \tag{1.4}$$

and for $k = 1, \ldots, m$ $H_k \neq 0$ implies

$$\overline{H_k} \cdot \overline{f_k} \prec \operatorname{lcm}\left(\overline{f_1}, \overline{f_2} \right)$$

Thus

$$u \cdot \overline{H_k} \cdot \overline{f_k} \prec u \cdot \operatorname{lcm}\left(\overline{f_1}, \overline{f_2} \right) = s \tag{1.5}$$

Recalling (1.2), we have

$$
\begin{aligned}
p =& h_1 f_1 + h_2 f_2 + h_3 f_3 + \cdots + h_m f_m \\
=& \left[\widehat{h_1} \cdot f_1 + \widehat{h_2} \cdot f_2 \right] + \left[\left(h_1 - \widehat{h_1} \right) \cdot f_1 + \left(h_2 - \widehat{h_2} \right) \cdot f_2 + h_3 f_3 + \cdots + h_m f_m \right]
\end{aligned}
$$

$$
\begin{aligned}
&= cu \cdot S_{1,2} + \left[\left(h_1 - \widehat{h_1} \right) \cdot f_1 + \left(h_2 - \widehat{h_2} \right) \cdot f_2 + h_3 f_3 + \cdots + h_m f_m \right] \\
&= cu \cdot (H_1 f_1 + \cdots + H_m f_m) \\
&= + \left[\left(h_1 - \widehat{h_1} \right) \cdot f_1 + \left(h_2 - \widehat{h_2} \right) \cdot f_2 + h_3 f_3 + \cdots + h_m f_m \right]
\end{aligned}
$$

Collecting on $f_1, \ldots, f_m$ we have

$$
\begin{aligned}
p = &\left(cu \cdot H_1 + h_1 - \widehat{h_1} \right) \cdot f_1 + \left(cu \cdot H_2 + h_2 - \widehat{h_2} \right) \cdot f_2 \\
&+ \left(cu \cdot H_3 + h_3 \right) f_3 + \cdots + \left(cu \cdot H_m + h_m \right) f_m
\end{aligned} \tag{1.6}
$$

Note that we have removed $\overline{h_1} \cdot \overline{f_1}$ and $\overline{h_2} \cdot \overline{f_2}$ from this last equation, so we removed the two instances where s appeared in (1.2).

Recall from (1.5) that $u \cdot \overline{H_k} \cdot \overline{f_k} \prec s$ for $k = 1, \ldots, m$.

Since $M = 2$, we know that $\overline{h_k} \cdot \overline{f_k} \prec s$ for $k = 3, \ldots, m$.

Let

$$
\begin{aligned}
s' = \max \Big\{ & \overline{u \cdot H_1 + h_1 - \widehat{h_1}} \cdot \overline{f_1}, \\
& \overline{u \cdot H_2 + h_2 - \widehat{h_2}} \cdot \overline{f_2}, \\
& \overline{u \cdot H_3 + h_3} \cdot \overline{f_3}, \\
& \ldots, \\
& \overline{u \cdot H_m + h_m} \cdot \overline{f_m} \Big\}
\end{aligned}
$$

Since s' is from the leading terms of (1.6), we see that $s' \neq s$. No term larger than s was added during the construction of (1.6), and s was maximal among the $\overline{h_k} \cdot \overline{f_k}$, so $s' \prec s$.

Inductive step: Assume that $M > 2$, and if

- $\widehat{h_{k_1}} \cdot \widehat{f_{k_1}} + \widehat{h_{k_2}} \cdot \widehat{f_{k_2}} = 0$
- $\dots$
- $\widehat{h_{k_1}} \cdot \widehat{f_{k_1}} + \cdots + \widehat{h_{k_{M-1}}} \cdot \widehat{f_{k_{M-1}}} = 0$

then we can rewrite (1.3) such that $s' = \max_{\succ} \left\{ \overline{h_k} \cdot \overline{f_k} \right\} \prec s$. Since $M > 2$,

$$\widehat{h_{k_1}} \cdot \widehat{f_{k_1}} + \cdots + \widehat{h_{k_M}} \cdot \widehat{f_{k_M}} = 0$$

Without loss of generality, we may assume that

$$\overline{h_1} \cdot \overline{f_1} = \cdots = \overline{h_M} \cdot \overline{f_M} = s$$

so that

$$\widehat{h_1} \cdot \widehat{f_1} + \cdots + \widehat{h_M} \cdot \widehat{f_M} = 0$$

Write

$$\mathrm{lc}_{\succ}(h_k) = a_k \qquad \mathrm{lc}_{\succ}(f_k) = b_k$$

Certainly

$$p = h_1 f_1 - \frac{a_1 b_1}{a_2 b_2} \cdot \widehat{h_2} \cdot f_2 + \left(h_2 + \frac{a_1 b_1}{a_2 b_2} \cdot \widehat{h_2} \right) \cdot f_2 + h_3 f_3 \cdots + h_m f_m \tag{1.7}$$

Notice that the leading monomials of the first two summands are constant multiples of s, *and* they cancel:

$$\begin{aligned} \widehat{h_1} \cdot \widehat{f_1} - \frac{a_1 b_1}{a_2 b_2} \cdot \widehat{h_2} \cdot \widehat{f_2} &= \widehat{h_1} \cdot \widehat{f_1} - a_1 b_1 \cdot \overline{h_2} \cdot \overline{f_2} \\ &= a_1 b_1 s - a_1 b_1 s \\ &= 0 \end{aligned}$$

The inductive hypothesis applies here, so that we can rewrite

$$h_1 f_1 - \frac{a_1 b_1}{a_2 b_2} \cdot \widehat{h_2} \cdot f_2 = \mathcal{H}_1 f_1 + \mathcal{H}_2 f_2$$

with

$$s' = \max_{\succ} \left\{ \overline{\mathcal{H}_1} \cdot \overline{f_1}, \overline{\mathcal{H}_2} \cdot \overline{f_2} \right\} \prec s$$

In the last $m-1$ summands of (1.7), s must cancel. There are exactly $M-2$ occurrences of s in $\overline{h_3} \cdot \overline{f_3}, \ldots, \overline{h_M} \cdot \overline{f_M}$. Further, there is only one occurrence of s in

$$\overline{h_2 + \frac{a_1 b_1}{a_2 b_2} \cdot \widehat{h_2}} \cdot \overline{f_2}$$

So s appears exactly $M-1$ times in the last $m-1$ summands of (1.7); the inductive hypothesis applies to these summands as well.

Regardless of the value of M, we have found an expression

$$p = \mathcal{H}_1 \cdot f_1 + \cdots + \mathcal{H}_m \cdot f_m$$

where

$$s' = \max_{\succ} \left\{ \overline{\mathcal{H}_k} \cdot \overline{f_k} \, : k = 1, \ldots, m \right\} \prec s$$

This contradicts the choice of s, so our assumption that $s \succ \overline{p}$ was wrong. We have shown that (C) implies that

$$\forall p \in I \quad \exists h_1, \ldots, h_m \in \mathbb{F}[x_1, \ldots, x_n] \qquad p = h_1 f_1 + \cdots + h_m f_m \quad \wedge \quad \overline{h_k} \cdot \overline{f_k} \preceq \overline{p}$$

Claim 2. For every nonzero $p \in \mathcal{I}$, $\overline{f_k} \mid \overline{p}$ for some $k = 1, \ldots m$.

Let $p \in \mathcal{I}$ be arbitrary, but fixed.

From claim 1, $\exists h_1, \ldots, h_m$ such that $p = h_1 f_1 + \cdots h_m f_m$ and $\overline{h_k} \cdot \overline{f_k} \preceq \overline{p}$ for $k = 1, \ldots, m$.

Certainly $\overline{h_k} \cdot \overline{f_k} = \overline{p}$ for some $k = 1, \ldots, m$ (otherwise the equations cannot be equal).

For this k, we have $\overline{f_k} \mid \overline{p}$.

Claim 3. We claim that $\forall p \in \mathcal{I}$ $p \xrightarrow[(f_1,\ldots,f_m)]{*} 0$.

Let $p \in I$ be arbitrary, but fixed. Let r be such that

$$p \xrightarrow[(f_1,\ldots,f_m)]{*} r \not\xrightarrow[(f_1,\ldots,f_m)]{} \cdot$$

If $r \neq 0$, then from claim 2 we know $\overline{f_k} \mid \overline{r}$ for some $k = 1, \ldots, m$.

This contradicts $r \not\xrightarrow[(f_1,\ldots,f_m)]{} \cdot$.

Thus $r = 0$ and

$$p \xrightarrow[(f_1,\ldots,f_m)]{*} 0$$

□

1.4. SOME PROPERTIES OF REPRESENTATIONS OF S-POLYNOMIALS

Although the climax of this chapter is theorem 1.30, we will need some additional tools in subsequent chapters. These tools describe elementary properties of representations of S-polynomials, and they pop up in multiple chapters, so we present them here.

We begin by defining notation for the "magic monomials" used to create S-polynomials.[14]

DEFINITION 1.34. For all polynomials f_i, f_j and term orderings $\succ$, we write

$$\sigma_{ij} = \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_i}} \qquad \sigma_{ji} = \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_j}}$$

This gives us an abbreviated notation for S-polynomials:

$$S_{i,j} = \sigma_{ij} \cdot f_i - \sigma_{ji} \cdot f_j$$

This abbreviated notation for S-polynomials is not the reason we introduce the σ-notation. These "magic monomials" will prove very important to subsequent results.

What relationship exists between σ_{ij} and σ_{ji}, the two monomials used to create $S_{i,j}$? It turns out that the two are relatively prime on their indeterminates.

[14] We are adapting this extremely useful notation from [**Hon98**].

LEMMA 1.35. *For all* $i \neq j$, $\gcd\left(\overline{\sigma_{ij}}\,,\,\overline{\sigma_{ji}}\right) = 1$.

PROOF. Let $i \neq j$. Assume $x \mid \sigma_{ij}$.

We have

$$\begin{aligned}
\deg_x \sigma_{ij} &= \deg_x \left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_i}} \right) \\
&= \deg_x \operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right) - \deg_x \widehat{f_i} \\
&= \max\left(\deg_x \overline{f_i}\,, \deg_x \overline{f_j}\right) - \deg_x \overline{f_i} \\
&= \max\left(0, \deg_x \overline{f_j} - \deg_x \overline{f_i}\right)
\end{aligned}$$

Since $x \mid \sigma_{ij}$, $\deg_x \sigma_{ij} > 0$. Thus

$$\deg_x \overline{f_j} > \deg_x \overline{f_i}$$

Now consider

$$\begin{aligned}
\deg_x \sigma_{ji} &= \deg_x \left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_j}} \right) \\
&= \deg_x \operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right) - \deg_x \widehat{f_j} \\
&= \max\left(\deg_x \overline{f_i}\,, \deg_x \overline{f_j}\right) - \deg_x \overline{f_j} \\
&= \deg_x \overline{f_j} - \deg_x \overline{f_j} \\
&= 0
\end{aligned}$$

Since x was an arbitrary indeterminate such that $x \mid \sigma_{ij}$, we know that $\deg_x \sigma_{ji} = 0$ for *any* indeterminate x where $x \mid \sigma_{ij}$.

A symmetric argument shows that $\deg_x \sigma_{ij} = 0$ for *any* indeterminate x where $x \mid \sigma_{ji}$.

Hence $\gcd\left(\overline{\sigma_{ij}}\,,\,\overline{\sigma_{ji}}\right) = 1$ as claimed. □

The next result is a useful consequence of lemma 1.25 on page 26.

LEMMA 1.36. *For all $i \neq j$ (A)⇒(B) where*

(A) $h_1, \ldots, h_m$ give a representation of $S_{i,j}$ modulo $f_1, \ldots, f_m$

(B) $\widehat{(\sigma_{ij} \pm h_i)} = \sigma_{ij}$ and $\widehat{(\sigma_{ji} \pm h_j)} = \sigma_{ji}$

PROOF. Let $i \neq j$ be arbitrary, but fixed.

Assume (A).

The statement of (B) is equivalent to $\sigma_{ij} \succ \widehat{h_i}$ and $\sigma_{ji} \succ \widehat{h_j}$.

By way of contradiction, assume

$$\sigma_{ij} \preceq \widehat{h_i}$$

Using corollary 1.14 on page 16,

$$\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_i}} \preceq \widehat{h_i}$$

$$\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right) \preceq \widehat{h_i} \cdot \widehat{f_i}$$

Recall (A). Since $h_1, \ldots, h_m$ give a representation of $S_{i,j}$, we know

$$\widehat{h_i} \cdot \widehat{f_i} \prec \operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)$$

We have a contradiction.

Hence $\sigma_{ij} \succ \overline{h_i}$. That $\overline{\sigma_{ji}} \succ \overline{h_j}$ is proved similarly. □

We will see in later chapters that it is useful to remove a common divisor from the polynomials to study the representations of their S-polynomials. That is, suppose $c_1, \ldots, c_m, g$ are polynomials such that $f_k = c_k g$. We would like to know how to "descend" from a representation of S_{f_i,f_j} to a representation of S_{c_i,c_j} and how to ascend again. What relationship, if any, exists between a representation of the S-polynomial of c_i, c_j and the S-polynomial of f_i, f_j? Lemma 1.37 provides the answer.

LEMMA 1.37. *For all $f_1, \ldots, f_m$ where $f_k = c_k g$ for some $c_1, \ldots, c_m, g$, the following are equivalent:*

(A) $h_1, \ldots, h_m$ give a representation of S_{f_i,f_j} modulo $f_1, \ldots, f_m$

(B) $\mathcal{H}_1, \ldots, \mathcal{H}_m$ give a representation of S_{c_i,c_j} modulo $c_1, \ldots, c_m$, where $\mathcal{H}_k = \mathrm{lc}_{\succ}(g) \cdot h_k$

PROOF. Let $\succ$ and $f_1, \ldots, f_m$ be arbitrary, but fixed. Assume $\exists c_1, \ldots, c_m, g$ such that $f_k = c_k g$. Let $i \neq j$ be arbitrary, but fixed, and let $h_1, \ldots, h_3$ be arbitrary, but fixed.

Then

$$S_{f_i,f_j} = h_1 f_1 + \cdots + h_m f_m$$

$$\Updownarrow$$

$$\begin{aligned}
\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_i}}\cdot f_i-\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_j}}\cdot f_j =& h_1f_1+\cdots+h_mf_m\\
&\Updownarrow\\
g\cdot\left(\frac{\operatorname{lcm}\left(\overline{gc_i}\,,\,\overline{gc_j}\right)}{\widehat{c_ig}}\cdot c_i-\frac{\operatorname{lcm}\left(\overline{gc_i}\,,\,\overline{gc_j}\right)}{\widehat{c_jg}}c_j\right) =& g\cdot(h_1c_1+\cdots+h_mc_m)\\
&\Updownarrow\\
\frac{\overline{g}\,\cdot\operatorname{lcm}\left(\overline{c_i}\,,\,\overline{c_j}\right)}{\widehat{g}\,\cdot\,\widehat{c_i}}\cdot c_i-\frac{\overline{g}\,\cdot\operatorname{lcm}\left(\overline{c_i}\,,\,\overline{c_j}\right)}{\widehat{g}\,\cdot\,\widehat{c_j}}c_j =& h_1c_1+\cdots+h_mc_m\\
&\Updownarrow\\
\frac{1}{\operatorname{lc}_{\succ}(g)}\cdot\left(\frac{\operatorname{lcm}\left(\overline{c_i}\,,\,\overline{c_j}\right)}{\widehat{c_i}}\cdot c_i-\frac{\operatorname{lcm}\left(\overline{c_i}\,,\,\overline{c_j}\right)}{\widehat{c_j}}c_j\right) =& h_1c_1+\cdots+h_mc_m\\
&\Updownarrow\\
S_{c_i,c_j} =& \mathcal{H}_1c_1+\cdots+\mathcal{H}_mc_m
\end{aligned}$$

Moreover, for any k, if $h_k\neq 0$ then

$$\begin{aligned}
\overline{f_k}\,\cdot\,\overline{h_k}\;&\prec\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)\\
&\Updownarrow\\
\overline{c_kg}\,\cdot\,\overline{h_k}\;&\prec\operatorname{lcm}\left(\overline{c_ig}\,,\,\overline{c_jg}\right)\\
&\Updownarrow\\
\overline{g}\,\cdot\,\overline{c_k}\,\cdot\,\overline{h_k}\;&\prec\overline{g}\,\cdot\operatorname{lcm}\left(\overline{c_i}\,,\,\overline{c_j}\right)\\
&\Updownarrow\\
\overline{c_k}\,\cdot\,\overline{h_k}\;&\prec\operatorname{lcm}\left(\overline{c_i}\,,\,\overline{c_j}\right)
\end{aligned}$$

Since $\mathcal{H}_k$ is a constant multiple of h_k, $\overline{h_k} = \overline{\mathcal{H}_k}$. Thus

$$\overline{c_k} \cdot \overline{\mathcal{H}_k} \prec \operatorname{lcm}(\overline{c_i}, \overline{c_j})$$

From the preceding, we have the equivalence

$$\begin{aligned} S_{f_i,f_j} &= h_1 f_1 + \cdots + h_m f_m \\ &\Updownarrow \\ S_{c_i,c_j} &= \mathcal{H}_1 c_1 + \cdots + \mathcal{H}_m c_m \end{aligned}$$

and for each $k = 1, 2, 3$ we have the equivalence

$$\begin{aligned} \overline{f_k h_k} &\prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right) \\ &\Updownarrow \\ \overline{c_k \mathcal{H}_k} &\prec \operatorname{lcm}(\overline{c_i}, \overline{c_j}) \end{aligned}$$

The statement of the lemma follows from these two equivalences. □

Chapter 2

Skipping S-polynomial reductions

2.1. A BOTTLENECK

The most time-consuming step in algorithm 1.1 on page 35 is the reduction of S-polynomials. Reduction can introduce growth in two ways: the storage size of the coefficients, and the number of monomials. This phenomenon, appropriately called "blowup", has proven a challenge for many applications of Gröbner bases.[1]

Examining the algorithm, we see that for a set of M polynomials, there are $M\,(M-1)$ S-polynomials to check. If we know *a priori* that some S-polynomials reduce to zero, then we can skip their reduction. For example:

LEMMA 2.1. *If f_i and f_j are monomials, then $S_{i,j} \xrightarrow[(f_i,f_j)]{*} 0$.*

[1] I can illustrate the bad reputation this phenomenon has given Gröbner bases using the following anecdote: during a conversation, a specialist in algebraic geometry told me that another algebraic geometer had advised him to steer away from Gröbner bases since, in the latter's opinion, they are unusable for systems of more than 5 or 6 polynomials in 5 or 6 variables.

PROOF. Regardless of the term ordering, we have

$$\widehat{f_i} = f_i$$

$$\widehat{f_j} = f_j$$

Thus

$$\begin{aligned} S_{i,j} &= \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{f_i} \cdot f_i - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{f_j} \cdot f_j \\ &= \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right) - \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right) \\ &= 0 \end{aligned}$$

So we have trivially

$$S_{i,j} \xrightarrow[(f_i,f_j)]{*} 0$$ □

2.2. SKIPPING S-POLYNOMIAL REDUCTIONS

We now formalize the notion of skipping an S-polynomial reduction.

DEFINITION 2.2. Suppose we are given $f_1, \ldots, f_m$ and a term ordering. We say that **condition $\mathcal{C}$ allows us to skip the reduction of $S_{i,j}$ modulo $f_1, \ldots, f_m$** (written $S_{i,j} \rightsquigarrow 0$) if $\mathcal{C}$ implies that $\exists \mathcal{P}$ such that

(A) $\mathcal{P} \subset \{(k, \ell) : 1 \leq k < \ell \leq m\}$ and $(i, j) \notin \mathcal{P}$

(B) If $S_{k,\ell} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$ for every $(k, \ell) \in \mathcal{P}$, then $\mathrm{GB}_{\succ}(f_1, \ldots, f_m)$.

In other words, algorithm `Is_GB` (1.1 on page 35) does not need to reduce $S_{i,j}$ to decide whether $f_1, \ldots, f_m$ are a Gröbner basis.

Certainly, if we knew *a priori* that $S_{i,j}$ reduces to zero, then we could skip its reduction, so this definition makes sense.

On the other hand, what if all we knew was that $S_{i,j}$ has a representation? Algorithm `Is_GB` (1.1 on page 35) checks whether every S-polynomial reduces to zero, and definition 2.2 says nothing about representations of S-polynomials, and we know that representation does not necessarily imply reduction to zero.

This is not such an obstacle as it may first seem. It turns out that having a representation is *equivalent* to being able to skip an S-polynomial reduction:

LEMMA 2.3. *(A) and (B) are equivalent, where*

(A) $S_{i,j}$ has a representation.

(B) $S_{i,j} \rightsquigarrow 0$.

PROOF. Let $f_1, \ldots, f_m$ and $\succ$ be arbitrary, but fixed.

(A)⇒(B): Assume that $S_{i,j}$ has a representation. Let $\mathcal{P} = \{(k,\ell) : (k,\ell) \neq (i,j)\}$. Assume that $S_{k,\ell}$ reduces to zero for every $(k,\ell) \in \mathcal{P}$; applying lemma 1.28, every S-polynomial in $\mathcal{P}$ has a representation. We know that $S_{i,j}$ has a representation; thus every S-polynomial has a representation, so $f_1, \ldots, f_m$ are a Gröbner basis. Thus $S_{i,j} \rightsquigarrow 0$.

(A)⇐(B): We proceed by showing the contrapositive: assume that $S_{i,j}$ does not have a representation. By theorem 1.30 on page 34, $f_1, \ldots, f_m$ cannot be a Gröbner

basis regardless of the choice of $\mathcal{P}$ (keeping in mind that $(i,j) \notin \mathcal{P}$). Since $f_1, \ldots, f_m$ are not a Gröbner basis for any value of $\mathcal{P}$, we cannot skip $S_{i,j}$. □

This result gives us a way to use representation to skip an S-polynomial reduction. In fact, we will never prove directly in this text that if some condition C is true, then $S_{i,j}$ reduces to zero. Rather, we will prove that if some condition C is true, then $S_{i,j}$ has a representation. *Why?* Besides an aesthetic consistency, it's usually easier! I have no idea how to prove most of the results on skipping S-polynomial reduction except by representation.

Notice the following: knowing that we can skip an S-polynomial reduction is not equivalent to knowing that it reduces to zero! *Why not?* Assume that we can skip $S_{i,j}$. It follows from lemma 2.3 that $S_{i,j}$ has a representation. On the other hand, suppose that we know *a priori* that $S_{i,j}$ does not reduce to zero. Then $f_1, \ldots, f_m$ are certainly not a Gröbner basis. Since $S_{i,j}$ has a representation and $f_1, \ldots, f_m$ are not a Gröbner basis, it follows from theorem 1.30 on page 34 that some other S-polynomial does have a representation. By lemma 1.28, this second S-polynomial neither reduces to zero: thus, it still makes sense to say that we can skip $S_{i,j}$. We will see a concrete example of this with example 2.7 on page 68 below.

We conclude by noting that definition 2.2 and lemma 2.3 give a revised algorithm for deciding whether $f_1, \ldots, f_m$ are a Gröbner basis: algorithm `Implied_GB` (2.1). An active area of research is determining what makes for a "minimal" $\mathcal{B}$; al-

Algorithm 2.1 Implied_GB

Inputs: $\succ$, $f_1, \ldots, f_m$

Output: YES if $f_1, \ldots, f_m$ are a Gröbner basis with respect to $\succ$; NO otherwise.

$\mathcal{B} \leftarrow \{(i,j) : \ 1 \leq i < j \leq m\} \setminus \{(k,\ell) : \ S_{k,\ell} \rightsquigarrow 0\}$

For $(i,j) \in \mathcal{B}$ **Do**

If $S_{i,j} \underset{(f_1,\ldots,f_m)}{\overset{*}{\nrightarrow}} 0$ **Then**

Return FALSE

Return TRUE

ready Buchberger had discussed this (in different terms) in [**Buc65**]; later research appears also in [**Buc79**], [**GM88**], [**CKR02**], and [**Fau02**].

2.3. COMBINATORIAL CRITERIA ON LEADING TERMS

Suppose that a criterion C considers only the leading terms of polynomials — not the other terms, and none of the coefficients. Terms are determined by the exponents on the variables. Exponents are natural numbers; thus, we call C a **combinatorial criterion on leading terms**.

If we can apply combinatorial criteria on leading terms to S-polynomial reduction, we avoid completely the bottleneck that reduction causes by its blowup both in coefficient size and in the number of monomials.

2.4. THE BUCHBERGER CRITERIA

During and after his PhD thesis, Bruno Buchberger presented two combinatorial criteria on leading terms.[2]

BUCHBERGER'S FIRST CRITERION. In his PhD thesis **[Buc65]** Buchberger had already discovered the following criterion which allows one to skip some S-polynomial reductions.

THEOREM 2.4. *If* $\mathrm{lt}_{\succ}(f_i)$ *and* $\mathrm{lt}_{\succ}(f_j)$ *are relatively prime, then* $S_{i,j}$ *has a representation modulo* f_i, f_j.

Before presenting the proof, we encourage the reader to consider again the reduction of $S_{1,3}$ in example 1.32 on page 36. Notice that the leading terms were relatively prime. Upon careful examination, we see that the reduction took place with the quotients being the *non*-leading monomial of f_1; we can call such monomials *"trailing monomials"*. By collecting the quotients into a representation (as in the proof of lemma 1.28 on page 30), we discern that $S_{1,3}$ has a form something like

$$S_{1,3} = R_1 \cdot f_3 - R_3 \cdot f_1 \tag{2.1}$$

[2]Because our research considers only "combinatorial criteria on the leading terms," we will refer to them simply as "combinatorial criteria".

where R_1, R_3 consist of the trailing monomials of f_1, f_3 respectively. This is precisely a representation of $S_{1,3}$. We exploit this form to prove theorem 2.4.[3]

PROOF. (of theorem 2.4)

Assume $\mathrm{lt}_\succ(f_i)$ and $\mathrm{lt}_\succ(f_j)$ are relatively prime. Then

$$\mathrm{lcm}\left(\overline{f_i}, \overline{f_j}\right) = \overline{f_i} \cdot \overline{f_j}$$

We have

$$S_{i,j} = \frac{\mathrm{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_i}} \cdot f_i - \frac{\mathrm{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_j}} \cdot f_j$$

The first thing to do is take advantage of the fact that the leading terms are relatively prime. We simplify the least common multiple:

$$\begin{aligned} S_{i,j} &= \frac{\overline{f_i} \cdot \overline{f_j}}{\mathrm{lc}_\succ(f_i) \cdot \overline{f_i}} \cdot f_i - \frac{\overline{f_i} \cdot \overline{f_j}}{\mathrm{lc}_\succ(f_j) \cdot \overline{f_j}} \cdot f_j \\ &= \frac{\overline{f_j}}{\mathrm{lc}_\succ(f_i)} \cdot f_i - \frac{\overline{f_i}}{\mathrm{lc}_\succ(f_j)} \cdot f_j \end{aligned}$$

At this point we introduce the trailing monomials. Write $f_i = \widehat{f_i} + R_i$ and $f_j = \widehat{f_j} + R_j$. Rewrite them as $f_i = \mathrm{lc}_\succ(f_i) \cdot \overline{f_i} + R_i$ and $f_j = \mathrm{lc}_\succ(f_j) \cdot \overline{f_j} + R_j$. Now rewrite $S_{i,j}$ and cancel the leading monomials:

$$\begin{aligned} S_{i,j} &= \frac{\overline{f_j}}{\mathrm{lc}_\succ(f_i)} \cdot \left(\mathrm{lc}_\succ(f_i) \cdot \overline{f_i} + R_i\right) - \frac{\overline{f_i}}{\mathrm{lc}_\succ(f_j)} \cdot \left(\mathrm{lc}_\succ(f_j) \cdot \overline{f_j} + R_j\right) \\ &= \left(\overline{f_i} \cdot \overline{f_j} + \frac{\overline{f_j}}{\mathrm{lc}_\succ(f_i)} \cdot R_i\right) - \left(\overline{f_i} \cdot \overline{f_j} + \frac{\overline{f_i}}{\mathrm{lc}_\succ(f_j)} \cdot R_j\right) \end{aligned}$$

[3] One can, in fact, prove that $S_{1,3} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$; see for example the proof of lemma 5.66 on page 222 of [**BWK93**]. We prove the first criterion using representations in order to maintain consistency with our general approach of using representations of S-polynomials to skip their reduction.

$$= \frac{\overline{f_j}}{\mathrm{lc}_\succ(f_i)} \cdot R_i - \frac{\overline{f_i}}{\mathrm{lc}_\succ(f_j)} \cdot R_j$$

Now we introduce additional polynomials that should help us obtain a representation similar in form to (2.1):

$$S_{i,j} = \left(\frac{\overline{f_j}}{\mathrm{lc}_\succ(f_i)} \cdot R_i - \frac{\overline{f_i}}{\mathrm{lc}_\succ(f_j)} \cdot R_j \right) + \left(\frac{R_i \cdot R_j}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} - \frac{R_i \cdot R_j}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \right)$$

Some careful rewriting follows:

$$\begin{aligned}
S_{i,j} &= \left(\frac{\widehat{f_j}}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \cdot R_i - \frac{\widehat{f_i}}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \cdot R_j \right) \\
&\quad + \left(\frac{R_i \cdot R_j}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} - \frac{R_i \cdot R_j}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \right) \\
&= \frac{1}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \cdot \left(\widehat{f_j} \cdot R_i + R_i \cdot R_j \right) \\
&\quad - \frac{1}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \cdot \left(\widehat{f_i} \cdot R_j + R_i \cdot R_j \right) \\
&= \left(\frac{1}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \cdot R_i \right) \cdot f_j - \left(\frac{1}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \cdot R_j \right) \cdot f_i
\end{aligned}$$

We now have

$$S_{i,j} = h_i f_i + h_j f_j$$

where

$$h_i = -\frac{1}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \cdot R_j$$

and

$$h_j = \frac{1}{\mathrm{lc}_\succ(f_i) \cdot \mathrm{lc}_\succ(f_j)} \cdot R_i$$

Do h_i, h_j give a representation of $S_{i,j}$? They will if

$$\overline{h_i} \cdot \overline{f_i} \prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)$$

and

$$\overline{h_j} \cdot \overline{f_j} \prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)$$

Observe that

$$\begin{aligned}\overline{h_i} \cdot \overline{f_i} &= \overline{R_j} \cdot \overline{f_i} \\ &\prec \overline{f_j} \cdot \overline{f_i} \\ &= \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)\end{aligned}$$

Similarly,

$$\overline{h_j} \cdot \overline{f_j} \prec \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)$$

Hence h_i, h_j give a representation of $S_{i,j}$ modulo f_i, f_j. □

BUCHBERGER'S SECOND CRITERION. In **[Buc79]**, Buchberger presented an additional criterion; this one allows one to skip an S-polynomial reduction based on the knowledge that others reduce to zero. Buchberger calls this criterion a "chain criterion," and we can see why from the form of (A).

THEOREM 2.5. *If* $\operatorname{lt}_\succ(f_k) \mid \operatorname{lcm}\left(\operatorname{lt}_\succ(f_i), \operatorname{lt}_\succ(f_j)\right)$*, then (A)⇒(B) where*

(A) $S_{i,k} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$ *and* $S_{k,j} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$.

(B) $S_{i,j}$ *has a representation modulo* $f_1, \ldots, f_m$.

As with theorem 2.4, theorem 2.5 gives us a representation for $S_{i,j}$. If the other S-polynomials reduce to zero, in particular $S_{i,k}$ and $S_{k,j}$, then they will also have representations; otherwise, we know that $f_1, \ldots, f_m$ are not a Gröbner basis.

How shall we prove the second criterion? If (A) of lemma 2.5 is satisfied, it turns out that we can write $S_{i,j}$ in terms of $S_{i,k}$ and $S_{k,j}$. We illustrate this by an example.

EXAMPLE 2.6. Let $\succ$ be any term ordering, and let

$$f_1 = x^2y + x \qquad f_2 = xz + z \qquad f_3 = yz + y$$

Observe that

$$\overline{f_1} = x^2y \qquad \overline{f_2} = xz \qquad \overline{f_3} = yz$$

We have

$$\operatorname{lcm}\left(\overline{f_1}, \overline{f_3}\right) = x^2yz$$

So (A) of lemma 2.5 is satisfied with $i = 1$, $j = 2$, $k = 3$.

Then

$$\begin{aligned} S_{1,2} &= \frac{x^2yz}{x^2y} \cdot \left(x^2y + x\right) - \frac{x^2yz}{xz} \cdot (xz + z) \\ &= xz - xyz \end{aligned}$$

$$\begin{aligned} S_{2,3} &= \frac{xyz}{xz} \cdot (xz + z) - \frac{xyz}{yz} \cdot (yz + y) \\ &= yz - xy \end{aligned}$$

$$\begin{aligned} S_{1,3} &= \frac{x^2yz}{x^2y} \cdot \left(x^2y + x\right) - \frac{x^2yz}{yz} \cdot (yz + y) \\ &= xz - x^2y \end{aligned}$$

We claim that we can write $S_{1,3}$ in terms of $S_{1,2}$ and $S_{2,3}$. Notice that $S_{1,2}$ and $S_{1,3}$ have a monomial in common, xz. While $S_{2,3}$ and $S_{1,3}$ do not have a monomial in common, the monomial $-xy$ can "multiply up" to $-x^2y$. Let's try combining $S_{1,2}$ with the appropriate multiple of $S_{2,3}$:

$$\begin{aligned} S_{1,2} + x \cdot S_{2,3} &= (xz - xyz) + x \cdot (yz - xy) \\ &= xz - x^2y \\ &= S_{1,3} \end{aligned}$$

It worked! What we did was apply a monomial multiple to other S-polynomials, and we could rewrite them to obtain the desired S-polynomial. If $S_{1,2}$ and $S_{1,3}$ have representations, then we should be able to combine those representations in the same way to obtain a representation of $S_{1,3}$.

How do we find these monomials? This is where Buchberger's second criterion becomes necessary: the "magic monomials" derive from

$$\frac{\operatorname{lcm}\left(\overline{f_1}\,,\,\overline{f_3}\right)}{\operatorname{lcm}\left(\overline{f_1}\,,\,\overline{f_2}\right)} \qquad \frac{\operatorname{lcm}\left(\overline{f_1}\,,\,\overline{f_3}\right)}{\operatorname{lcm}\left(\overline{f_2}\,,\,\overline{f_3}\right)}$$

Since $\overline{f_2}$ divides the least common multiple of $\overline{f_1}$ and $\overline{f_3}$, the two quotients above will be terms and not rational expressions. Inspection shows that in the case of

this example, the first quotient is 1, and the second is x; these were the "magic monomials" that gave us the right combination.

We note that f_1, f_2, f_3 are not a Gröbner basis. There is no need to reduce $S_{1,3}$ to verify this, since $S_{1,2}$ does not reduce to zero. ◇

We apply this insight to prove the theorem.

PROOF. Assume $\overline{f_k} \mid \operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)$.

Assume (A):

$$S_{i,k} \xrightarrow[(f_1,\ldots,f_m)]{*} 0 \quad \text{or} \quad S_{k,j} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$$

Consider

$$S_{i,j} = \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_i}} \cdot f_i - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_j}} \cdot f_j$$

To obtain the S-polynomials involving f_k, we have to introduce f_k to the equation. We use a multiple of f_k that may not remain polynomial if Buchberger's second criterion is not satisfied:

$$\begin{aligned} S_{i,j} &= \left(\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_i}} \cdot f_i - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_j}} \cdot f_j\right) \\ &\quad + \left(\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_k}} \cdot f_k - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_k}} \cdot f_k\right) \\ &= \left(\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_i}} \cdot f_i - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_k}} \cdot f_k\right) \\ &\quad + \left(\frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_k}} \cdot f_k - \frac{\operatorname{lcm}\left(\overline{f_i}, \overline{f_j}\right)}{\widehat{f_j}} \cdot f_j\right) \end{aligned}$$

At this point we need to massage the equation a little, introducing factors that will lead us towards writing $S_{i,j}$ in terms of $S_{i,k}$ and $S_{k,j}$:

$$\begin{aligned}
S_{i,j} &= \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot \left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_i}} \cdot f_i - \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_k}} \cdot f_k \right) \\
&\quad + \frac{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot \left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_k}} \cdot f_k - \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\widehat{f_j}} \cdot f_j \right) \\
&= \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot \left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)}{\widehat{f_i}} \cdot f_i - \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)}{\widehat{f_k}} \cdot f_k \right) \\
&\quad + \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot \left(\frac{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)}{\widehat{f_k}} \cdot f_k - \frac{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)}{\widehat{f_j}} \cdot f_j \right) \\
&= \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot S_{i,k} + \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot S_{k,j}
\end{aligned}$$

Recall that $S_{i,k} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$ and $S_{k,j} \xrightarrow[(f_1,\ldots,f_m)]{*} 0$. By lemma 1.28, there exist $h_1 \ldots, h_m$ such that $h_1, \ldots, h_m$ give a representation of $S_{i,k}$. Also, there exist $H_1, \ldots, H_m$ such that $H_1, \ldots, H_m$ give a representation of $S_{k,j}$. Then

$$\begin{aligned}
S_{i,j} &= \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot S_{i,k} + \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot S_{k,j} \\
&= \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot (h_1 f_1 + \cdots + h_m f_m) + \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot (H_1 f_1 + \cdots + H_m f_m)
\end{aligned}$$

Collecting along $f_1, \ldots, f_m$, we have

$$\begin{aligned}
S_{i,j} &= \left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot h_1 + \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot H_1 \right) \cdot f_1 \\
&\quad + \cdots + \left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot h_m + \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot H_m \right) \cdot f_m
\end{aligned}$$

For $\ell = 1, \ldots, m$ let

$$\mathcal{H}_\ell = \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot h_\ell + \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot H_\ell$$

Then

$$S_{i,j} = \mathcal{H}_1 \cdot f_1 + \cdots + \mathcal{H}_m \cdot f_m$$

For $\ell = 1, \ldots, m$, $\mathcal{H}_\ell \neq 0$ implies

$$\begin{aligned}\overline{\mathcal{H}_\ell} \cdot \overline{f_\ell} &= \overline{\left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot h_\ell + \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot H_\ell\right)} \cdot \overline{f_\ell} \\ &= \max_{\succ}\left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot \overline{h_\ell} \cdot \overline{f_\ell}\,,\quad \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot \overline{H_\ell} \cdot \overline{f_\ell}\right)\end{aligned}$$

Recall that the h_k are a representation for $S_{i,k}$ and the H_k are a representation for $S_{k,j}$. Thus

$$\begin{aligned}\overline{\mathcal{H}_\ell} \cdot \overline{f_\ell} &\prec \max\left(\frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right)} \cdot \operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_k}\right),\quad \frac{\operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)}{\operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)} \cdot \operatorname{lcm}\left(\overline{f_k}\,,\,\overline{f_j}\right)\right) \\ &= \operatorname{lcm}\left(\overline{f_i}\,,\,\overline{f_j}\right)\end{aligned}$$

We see that $\mathcal{H}_1, \ldots, \mathcal{H}_m$ give a representation of $S_{i,j}$ modulo $f_1, \ldots, f_m$. □

We should issue a cautionary note. Unlike the footnote to theorem 2.4 on page 59, Buchberger's second criterion does *not* guarantee that $S_{i,j}$ reduces to zero; it only guarantees that we do not need to check whether it does. *It is entirely possible that $S_{i,j}$ does not reduce to zero!* In this case, it is certain that one of $S_{i,k}$ or $S_{k,j}$ also does not reduce to zero. Since the computation of $S_{i,k}$ and $S_{k,j}$ are already necessary to Buchberger's algorithm, there is no need to check $S_{i,j}$.

We illustrate this warning with example 2.7.

EXAMPLE 2.7. Let $f_1 = x^2y + x$, $f_2 = xy$, and $f_3 = x^3$. Let $\succ$ be any admissible term ordering. Then

$$\overline{f_1} = x^2y \qquad \overline{f_2} = xy \qquad \overline{f_3} = x^3$$

Observe that

$$\overline{f_2} \mid \operatorname{lcm}\left(\overline{f_1}, \overline{f_3}\right)$$

So $S_{1,3} \rightsquigarrow 0$.

However,

$$\begin{aligned} S_{1,3} &= \frac{\operatorname{lcm}(x^2y, x^3)}{x^2y} \cdot \left(x^2y + x\right) - \frac{\operatorname{lcm}(x^2y, x^3)}{x^3} \cdot x^3 \\ &= x \cdot \left(x^2y + x\right) - y \cdot x^3 \\ &= x^2 \end{aligned}$$

Clearly $S_{1,3} \underset{(f_1,f_2,f_3)}{\nrightarrow}$, so

$$S_{1,3} \underset{(f_1,f_2,f_3)}{\overset{*}{\nrightarrow}} 0$$

As expected, the chain that f_2 should build does not hold at $S_{1,2}$:

$$\begin{aligned} S_{1,2} &= \frac{\operatorname{lcm}(x^2y, xy)}{x^2y} \cdot \left(x^2y + x\right) - \frac{\operatorname{lcm}(x^2y, xy)}{xy} \cdot xy \\ &= 1 \cdot \left(x^2y + x\right) - x \cdot xy \\ &= x \end{aligned}$$

and $S_{1,2} \underset{(f_1,f_2,f_3)}{\nrightarrow}$, so

$$S_{1,2} \underset{(f_1,f_2,f_3)}{\overset{*}{\nrightarrow}} 0$$

Since $S_{1,2}$ does not reduce to zero, it should not surprise us that $S_{1,3}$ does not reduce to zero. ◇

SUMMARY. To summarize, we provide the following definition:

DEFINITION 2.8. Buchberger's combinatorial criteria are

$$\begin{aligned} \mathrm{BC1}\,(t_1,t_3) &\Leftrightarrow \gcd(t_1,t_3)=1 \\ \mathrm{BC2}\,(t_1,t_2,t_3) &\Leftrightarrow t_2 \mid \mathrm{lcm}\,(t_1,t_3) \end{aligned}$$

We now have the following corollary to theorems 2.4 and 2.5:

COROLLARY 2.9.

$$\mathrm{BC1}\,(t_1,t_3) \text{ or } \mathrm{BC2}\,(t_1,t_2,t_3) \quad \Rightarrow \quad S_{1,3} \rightsquigarrow 0$$

We conclude this section with an example illustrating the efficacy of Buchberger's criteria.

EXAMPLE 2.10. Let $\succ = \mathrm{lex}\,(x,y,z)$ and[4]

$$f_1 = x+y+z$$

[4]This system derives from *Cyclic-3*, a Gröbner basis benchmark related to the roots of the cyclic polynomial $X^3-1=0$.

$$\begin{aligned} f_2 &= xy + xz + yz \\ f_3 &= xyz - 1 \\ f_4 &= y^2 + yz + z^2 \\ f_5 &= yz^2 + z^3 + 1 \\ f_6 &= y - z^4 \\ f_7 &= z^6 + z^3 + 1 \end{aligned}$$

We claim that Buchberger's criteria allow us to skip every S-polynomial reduction involving f_7.

Notice that our system consists of the following leading terms:

$$\overline{f_1} = x \qquad \overline{f_2} = xy \qquad \overline{f_3} = xyz$$

$$\overline{f_4} = y^2 \qquad \overline{f_5} = yz^2 \qquad \overline{f_6} = y$$

$$\overline{f_7} = z^6$$

We have

$$\gcd\left(\overline{f_i}, \overline{f_j}\right) = 1 \qquad \forall\,(i,j) = (1,7), (2,7), (4,7), (6,7)$$

By corollary 2.9, we can skip the reduction of $S_{1,7}, S_{2,7}, S_{4,7}, S_{6,7}$. This leaves $S_{3,7}$ and $S_{5,7}$.

Observe that

$$\overline{f_1} \mid \operatorname{lcm}\left(\overline{f_3}, \overline{f_7}\right)$$

$$\overline{f_6} \mid \operatorname{lcm}\left(\overline{f_5}, \overline{f_7}\right)$$

By corollary 2.9, we can skip the reduction of $S_{3,7}$ and $S_{5,7}$.

We see that *we need not reduce a single S-polynomial involving f_7.* This saves us considerable time: while the expense of reducing these S-polynomials is relatively significant (1.080s using Maple 9 on a 400MHz G3 iBook), the amount of time required to check Buchberger's criteria is so small as not to register (0.0000s). We will see this difference more dramatically in later chapters. ◇

2.5. TERM DIAGRAMS

We will find it useful in subsequent chapters to compare visually Buchberger's criteria with our results. There is a useful technique for diagramming the locations of leading terms: drawing ***term diagrams***. This technique is both simple and useful for visualizing terms of two or three variables; see for example sections 4.2 and 9.2 of [**CLO97**]. We illustrate it by an example.

EXAMPLE 2.11. Let $t_1 = x^3$, $t_2 = x^2y$, $t_3 = y^5$, $t_4 = x^4y^2$, $t_5 = x^2y^2$, $t_6 = xy^4$. In figure 2.1 on the following page, we let the x-axis of the Cartesian plane represent powers of x, and the y-axis represent powers of y. Graphing exponents of the t_k

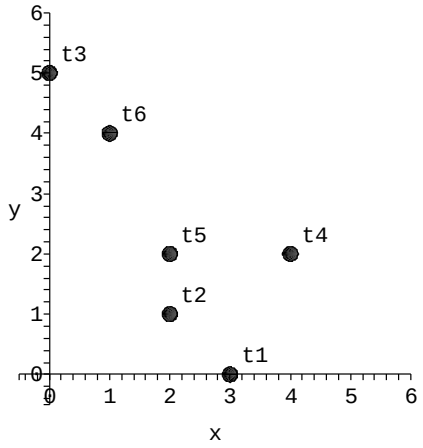


Figure 2.1: Term diagram of $t_1, t_2, \ldots, t_6$

as though they were points, we can visualize where the terms appear in relation to each other.

Obviously, if one term is further to the left of a second, and further below it, then the first term divides the second. We see that illustrated with t_1 and t_4: t_1 is *both* further left *and* below t_4. Thus we have a visual clue that $t_1 \mid t_4$. We also see this illustrated with t_2 and t_5. However, t_6 is *not* divisible by another of the t_k, which we see in the diagram because it does not lie *both* further left *and* below any of $t_1, \ldots, t_5$.

Figure 2.2 on the next page illustrates this divisibility more clearly by shading the northeast quadrant of each term. Any term in a shaded quadrant that lies away from the southwest corner is divisible by the term that does lie in that southwest corner. In figure 2.2, both t_4 and t_5 lie away from the southwest corner of a shaded quadrant (in fact, t_4 lies in a veritable sea of shading). Since the southwest corner

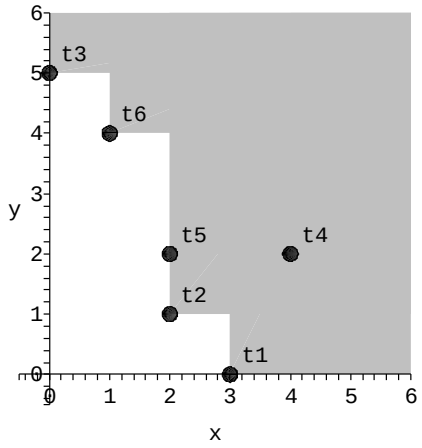


Figure 2.2: Diagram of $t_1, t_2, \ldots, t_6$, with shading added for divisible terms.

corresponds to t_2, we can see easily that t_2 divides t_4 and t_5. Further, t_6 lies at the southwest corner of a shaded region; hence, it is divisible by no other listed term.

We can also determine quickly where the greatest common divisor and the least common multiple of any two terms lie. We illustrate this in figure 2.3 using t_2 and t_6. ◇

How does this relate to Buchberger's criteria? Recall from theorem 2.4 on page 59 that Buchberger's first criterion is satisfied if the leading terms of two polynomials are relatively prime.

EXAMPLE 2.12. Recalling the terms of example 2.11, suppose we know that these are the leading terms of a set of polynomials $f_1, \ldots, f_6$. In example 2.11, only t_1 and t_3 satisfy Buchberger's first criterion. Thus, we can skip the reduction of $S_{1,3}$.

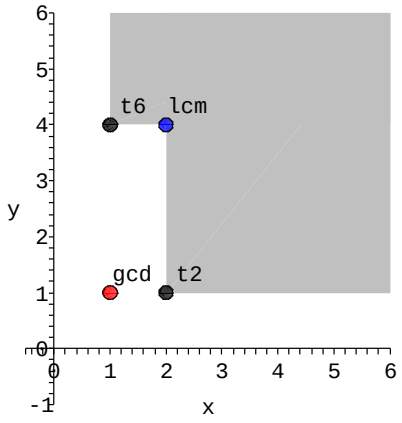


Figure 2.3: Diagram of the greatest common divisor (lower left dot) and least common multiple (upper right dot) of two terms.

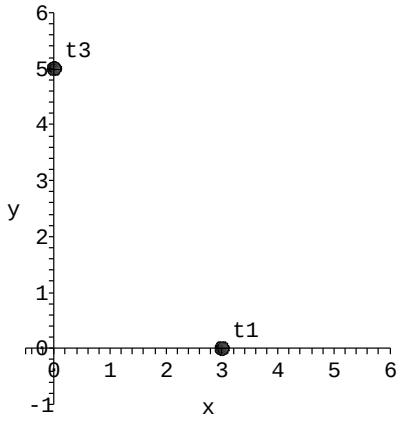


Figure 2.4: Diagram of two relatively prime terms.

As we see in figure 2.4, the geometric consequence is that the two terms lie on different axes. ◇

What about Buchberger's second criterion? Suppose we want to know whether we can skip the reduction of $S_{4,6}$. Recall from theorem 2.5 on page 62 that the

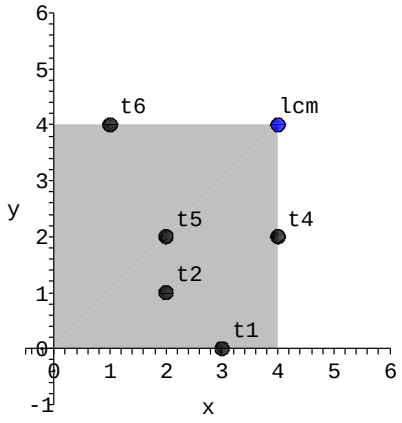


Figure 2.5: Diagram of the divisors (in grey box) that divide $\mathrm{lcm}\,(t_4, t_6)$.

second criterion is satisfied if the leading term of one polynomial divides the least common multiple of the leading terms of two polynomials.

EXAMPLE 2.13. Figure 2.5 shows how we can determine which terms satisfy Buchberger's second criterion, by shading the region that *divides* the least common multiple of t_4 and t_6. It turns out that we can skip $S_{4,6}$, since any one of t_1, t_2, t_5 lie within the shaded region, and hence divide the least common multiple of t_4 and t_6. It is also clear that we cannot skip $S_{1,2}$, since as figure 2.6 shows, no other leading monomial lies within the region of terms that divide their least common multiple. ◇

At this point, we are ready to turn to the main results of our thesis.

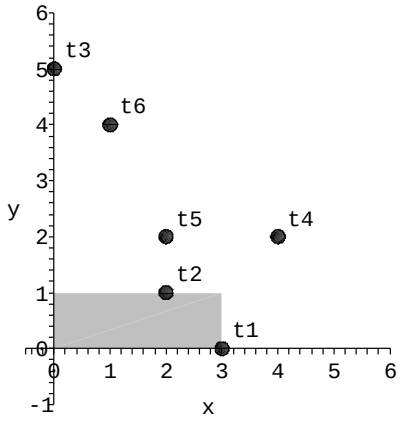


Figure 2.6: No other monomial lies within the region of divisors of t_1 and t_2.

Part 2

New combinatorial criteria for skipping S-polynomial reduction

Chapter 3

Outline of part two

3.1. Buchberger's criteria revisited

Recall Buchberger's criteria from definition 2.8 on page 69. We observed that Buchberger's criteria are both combinatorial and sufficient for skipping S-polynomial reduction.

Two natural questions to ask are,

- *How are Buchberger's criteria sufficient?*
- *Are Buchberger's criteria necessary?*

Related to the second question is a third,

- *If Buchberger's criteria are not necessary, what are the complete combinatorial criteria that allow us to skip S-polynomial reductions?*

The answers to these questions are not immediately obvious. As noted in section 2.2, there has been some research related to this question; [**GM88**] applies Buchberger's criteria in a modified algorithm to compute Gröbner bases, and [**CKR02**] shows that Buchberger's criteria generate minimal bases of syzygy modules, which have a parallel with representations of S-polynomials.[1] Somewhat further afield is the work of Jean-Charles Faugère **[Fau02]** who has found non-combinatorial criteria that allow one to skip S-polynomial reduction.

We can add the following questions:

- *How often do Buchberger's criteria allow us to skip S-polynomial reduction?*
- *How many Gröbner bases do not satisfy Buchberger's criteria?*

We will not consider these latter questions rigorously, but we do have some interesting experimental results. They suggest that Buchberger's criteria arise quite often. This corresponds with example 2.10 on page 69, where Buchberger's criteria allowed us to skip all six reductions involving an S-polynomial of f_7. (They would have allowed us to skip a great deal more, as well.) We present surveys of randomly-generated polynomials in sections 4.3.3, 5.3.3, and 6.3.3.

[1] For example, [**CLO97**] proves Buchberger's second criterion (our corollary 2.9 on page 69) using syzygies (their proposition 10 on page 106).

3.2. FORMAL STATEMENT OF THE PROBLEM CONSIDERED IN PART TWO

To answer the questions posed in section 3.1, we need to formalize the problem. The following definition provides the structure that guides the remainder of part 2.

DEFINITION 3.1. We define CC, the "complete combinatorial criterion," as follows:

Inputs: $t_1, \ldots, t_m, \succ, \mathcal{P} \subset \{(i,j) : 1 \leq i < j \leq m\}$

Output: the boolean value of

$$\left[\forall\,(i,j) \in \mathcal{P}\ S_{i,j} \xrightarrow[(f_1,\ldots,f_m)]{*} 0\right]$$

$$\Downarrow$$

$$\mathrm{GB}_{\succ}\,(f_1, \ldots, f_m)$$

$\forall f_1, \ldots, f_m$ such that $\overline{f_k} = t_k$

What does this say?

First, CC is a test on leading terms, *not* on coefficients or on other terms. So one of its proper inputs is a list of terms $t_1, \ldots, t_m$, *not* a list of polynomials $f_1, \ldots, f_m$. In consequence, CC provides a guarantee about *every* set of polynomials $f_1, \ldots, f_m$ with leading terms $t_1, \ldots, t_m$.

What is this guarantee? Criterion CC guarantees that if the S-polynomials listed in $\mathcal{P}$ reduce to zero, then $f_1, \ldots, f_m$ are a Gröbner basis. In other words, *we can skip the reductions of those S-polynomials not indexed by $\mathcal{P}$.*

On the other hand, if CC is false, then we know that there exists some system $f_1, \ldots, f_m$ with leading terms $t_1, \ldots, t_m$, but $f_1, \ldots, f_m$ are not a Gröbner basis. In other words, we would need more information than the leading terms alone to decide whether polynomials with leading terms $t_1, \ldots . t_m$ are a Gröbner basis.

Notice that, given $t_1, \ldots, t_m$, we cannot try a brute-force method of testing every set of polynomials $f_1, \ldots, f_m$ with those leading terms; we cannot even make a *list* of all such $f_1, \ldots, f_m$: there are infinitely many!

How is CC *related to the definition of skipping S-polynomial reduction (definition 2.2 on page 55)?* It can substitute for $\mathcal{C}$ in the definition of skipping S-polynomial reduction. Because of this, CC does not guarantee that every S-polynomial reduces to zero; so, it does not guarantee that $f_1, \ldots, f_m$ are a Gröbner basis; it merely guarantees that we need not include $S_{i,j}$ in the set $\mathcal{P}$ of S-polynomials whose reduction we check. Using the notation of algorithm `Implied_GB` (2.1 on page 58), CC guarantees only that $(i, j) \notin \mathcal{B}$.

Of course, we might be able to skip S-polynomial reductions for some systems $f_1, \ldots, f_m$ where CC is not satisfied. This is because CC is a condition on the leading terms only: in order to show that CC is *not* true, it suffices to find polynomials $f_1, \ldots, f_m$ with the specified leading terms, one of whose S-polynomials

does not reduce to zero. However, because S-polynomial reduction depends also on the trailing monomials, it may well be that we can skip the reduction of $S_{i,j}$ even though it does *not* reduce to zero.

3.3. OUTLINE OF THE REMAINDER OF PART TWO

Now that we have defined the problem formally, we proceed in a systematic manner by increasing the size of $\mathcal{P}$:

- in chapter 4, we set $\mathcal{P} = \emptyset$, and thus present criteria that decide whether we can skip *all* S-polynomial reductions;
- in chapter 5, we set $\mathcal{P} = \{(1, 2)\}$, and thus present criteria that decide whether we can skip *all but one* S-polynomial reductions;
- in chapter 6, we set $m = 3$ and $\mathcal{P} = \{(1, 2), (2, 3)\}$, so that given f_1, f_2, f_3, we can use the criterion presented in that chapter to decide whether we can skip *all but one* S-polynomial reductions.

Things become somewhat difficult when we consider skipping all but two S-polynomial reductions. We provide a complete criterion for $m = 3$, where m is the number of polynomials, but the more general question for $m > 3$ remains open. The problem also remains open for any m when the size of $\mathcal{P}$ is larger than two.

3.4. AN INVALUABLE LEMMA

We will find it necessary in chapters 4, 5, and 6 to construct sets of polynomials $f_1, \ldots, f_m$ that serve as counterexamples in the following way: the leading terms $\overline{f_1}, \ldots, \overline{f_m}$ do not satisfy CC, and $f_1, \ldots, f_m$ are not a Gröbner basis. How do we prove that $f_1, \ldots, f_m$ are not a Gröbner basis? By theorem 1.30, we need to find $i \neq j$ such that $S_{i,j} \underset{(f_1,\ldots,f_m)}{\overset{*}{\nrightarrow}} 0$.

A great help towards this end would be a clear form for such a counterexample $f_1, \ldots, f_m$. Lemma 3.2 provides this form for chapters 4 and 5. In chapter 6 we apply this lemma for one counterexample (lemma 6.8 on page 131), but require a generalized form of the lemma for another group of counterexamples (lemma 6.9 on page 134).

LEMMA 3.2. *Let τ be a nonzero monomial, and $F = (f_1, \ldots, f_m)$ a system of polynomials. Then (A)⇒(B) where*

(A) $\exists \mu$ with $1 \leq \mu \leq m$ such that [(A1) and (A2)] where

(A1) $\widehat{f_\ell} \nmid \tau \qquad \forall \ell = 1, \ldots, \mu$

(A2) $\forall \ell = \mu + 1, \ldots, m$

$f_\ell = t_\ell + u_\ell$ *with* $t_\ell \neq u_\ell$

$u_\ell \mid t_\ell$

(B) $\tau \underset{F}{\overset{*}{\nrightarrow}} 0$.

Before proving the lemma, we illustrate it with the following example.

EXAMPLE 3.3. Let $p_1 = xy$, $f_1 = y - 1$, $f_2 = x^2$. Let $\succ$ be an arbitrary term ordering. We have

$$\overline{f_1} = y \qquad \overline{f_2} = x^2$$

Clearly $p_1 \underset{f_2}{\nrightarrow}$, since $\deg_x \overline{f_2} > \deg_x p_1$. Observe that

$$p_1 \underset{f_1}{\longrightarrow} x$$

Write $p_2 = x$. We still have $p_2 \underset{f_2}{\nrightarrow}$.

Why? Since the leading monomial of f_1 cancels the monomial p_1, the remainder p_2 is determined by the trailing term of f_1. Comparing the two terms of the binomial f_1, we see $\deg_x y \geq \deg_x 1$. As a consequence, $\deg_x p_2 \leq \deg_x p_1 < \deg_x \overline{f_2}$. Hence $p_2 \underset{f_2}{\nrightarrow}$; in fact, $p_2 \underset{(f_1,f_2)}{\nrightarrow}$, and p_2 is the only possible reduction of p_1 over f_1, f_2. Thus $p_1 \underset{(f_1,f_2)}{\overset{*}{\nrightarrow}} 0$. ◇

The application of lemma 3.2 will occur after we construct f_i, f_j such that $S_{i,j}$ is a monomial; then we set $\tau = S_{i,j}$. A permutation on the polynomial indices $1, \ldots, m$ will sometimes be required for a rigorous application of the lemma; we indicate the necessary permutation in the text.

PROOF. Let $\tau_0, \ldots, \tau_s$ be an arbitrary reduction chain of τ modulo F:

$$\tau = \tau_0 \underset{F}{\longrightarrow} \tau_1 \underset{F}{\longrightarrow} \cdots \underset{F}{\longrightarrow} \tau_s \underset{F}{\nrightarrow}$$

We claim that $\forall k = 0, \ldots, s$, τ_k is a nonzero monomial and $\widehat{f_\ell} \nmid \tau_k \; \forall \ell = 1, \ldots, \mu$.

We proceed by induction.

Inductive base: Observe that $\tau_0 = \tau$, so τ_0 is a nonzero monomial, and $\widehat{f}_\ell \nmid \tau_0$ $\forall \ell = 1, \ldots, \mu$.

Inductive step: Assume that τ_k is a nonzero monomial, and $\widehat{f}_\ell \nmid \tau_k$ $\forall \ell = 1, \ldots, \mu$. We will show that τ_{k+1} is a nonzero monomial, and $\widehat{f}_\ell \nmid \tau_{k+1}$ for all $\ell = 1, \ldots, \mu$.

We have $f_\ell \nmid t_k$ for $\ell = 1, \ldots, m$.

Then $\tau_k \xrightarrow[f_j]{} \tau_{k+1}$ implies $\mu + 1 \leq j \leq m$.

Let $\ell \in \{1, \ldots, m\}$ be arbitrary, but fixed.

Since $\widehat{f}_\ell \nmid \tau_k$, $\exists \lambda$ such that $\deg_{x_\lambda} \widehat{f}_\ell > \deg_{x_\lambda} \tau_k$.

Since $u_\ell \mid t_\ell$, $\deg_{x_\lambda} u_\ell \leq \deg_{x_\lambda} t_\ell$.

We have

$$\begin{aligned} \deg_{x_\lambda} \tau_{k+1} &= \deg_{x_\lambda} \left(\frac{\tau_k}{t_j} \cdot u_j \right) \\ &\leq \deg_{x_\lambda} \left(\frac{\tau_k}{t_j} \cdot t_j \right) \\ &= \deg_{x_\lambda} \tau_k \end{aligned}$$

Hence $\widehat{f}_\ell \nmid \tau_{k+1}$.

Since k was arbitrary, $\tau_k \neq 0$ and $\widehat{f}_\ell \nmid \tau_k$ $\forall \ell = 1, \ldots, \mu$ $\forall k = 0, \ldots, s$.

Since the reduction chain was arbitrary, $\tau \xrightarrow[F]{*} 0$. □

Now we can address the first question: when can we skip all S-polynomial reductions?

Chapter 4

Skipping all S-polynomial reductions

4.1. PROBLEM

It follows from Buchberger's first criterion that if the leading terms of $f_1, \ldots, f_m$ are all pairwise relatively prime, then we can skip the reduction of their S-polynomials (see corollary 2.9 on page 69). Two questions arise:

- If the leading terms of two polynomials are not relatively prime, can we use Buchberger's second criterion to skip the corresponding S-polynomial, and thus skip all S-polynomials reductions?
- Do there exist other combinatorial criteria that would allow us to skip all S-polynomial reductions?

Stated formally, we are looking for an algorithm that decides

$$\mathrm{CC}\left(t_1, \ldots, t_m, \succ, \emptyset\right)$$

By definition 3.1 on page 80, this would be equivalent to an algorithm that decides

$$\mathrm{GB}_{\succ}(f_1, \ldots, f_m) \quad \forall f_1, \ldots, f_m \text{ such that } \overline{f_1} = t_1, \ldots, \overline{f_m} = t_m$$

The answer is given by algorithm 4.1 on page 90, which follows from theorem 4.1.

4.2. RESULT

THEOREM 4.1. *(A) is equivalent to (B) where*

(A) $\mathrm{GB}_{\succ}(f_1, \ldots, f_m)$ *for all* $f_1, \ldots, f_m$ *such that* $\overline{f_1} = t_1$, …, $\overline{f_m} = t_m$

(B) [(B1) or (B2)] where

(B1) $\gcd(t_i, t_j) = 1 \; \forall i \neq j$

(B2) $t_k = 1 \; \exists k$

A few observations before we prove theorem 4.1:

That (A)⇐(B) is obvious: clause (B1) is Buchberger's first criterion, and we apply corollary 2.9 on page 69; clause (B2) is a "trivial" combinatorial criterion: if $\overline{f_k} = 1$, then f_k is constant, so *every* S-polynomial will reduce to zero over f_k.

It is not so obvious that (A)⇒(B). To begin with, Buchberger's second criterion makes only a trivial contribution to skipping every S-polynomial reduction. Further, the theorem asserts that there are no other combinatorial criteria for skipping every S-polynomial reduction, and this was not exactly clear to start with.

The proof that (A)⇒(B) is also not obvious. Our approach is to show the contrapositive: ¬(A)⇐¬(B). This means we have to find a system $f_1, \ldots, f_m$ such that

$\neg\mathrm{GB}_{\succ}(f_1, \ldots, f_m)$. If we picked a random system $f_1, \ldots, f_m$, we could reasonably expect $\neg\mathrm{GB}_{\succ}(f_1, \ldots, f_m)$. However, this would be hard to prove, since we would have to trace all possible reductions for a random, unstructured system of polynomials. What we do, then, is provide a *simple, structured* counterexample. Lemma 3.2 on page 83 becomes very useful at this point.

PROOF. (Of theorem 4.1, (A)⇒(B).)

We show the contrapositive: assume ¬(B). Then ¬(B1) and ¬(B2): there exist $i \neq j$ such that $\gcd(t_i, t_j) \neq 1$, and $\forall k\ t_k \neq 1$. We will show ¬(A).

Let

$$f_i = t_i$$

$$f_k = t_k + 1 \quad \forall k \neq i$$

Observe

$$\begin{aligned} S_{i,j} &= \frac{\mathrm{lcm}(t_i, t_j)}{t_i} \cdot t_i - \frac{\mathrm{lcm}(t_i, t_j)}{t_j} \cdot (t_j + 1) \\ &= \mathrm{lcm}(t_i, t_j) - \mathrm{lcm}(t_i, t_j) - \frac{\mathrm{lcm}(t_i, t_j)}{t_j} \\ &= -\frac{\mathrm{lcm}(t_i, t_j)}{t_j} \end{aligned}$$

Since

$$\mathrm{lcm}(t_i, t_j) = \frac{t_i t_j}{\gcd(t_i, t_j)}$$

we have

$$S_{t_i,t_j} = -\frac{t_i}{\gcd(t_i, t_j)}$$

Since $\gcd(t_i, t_j) \neq 1$, $\overline{f_i} \nmid S_{i,j}$.

Applying lemma 3.2, $S_{i,j} \underset{(f_1,\ldots,f_m)}{\overset{*}{\nrightarrow}} 0$. (The permutation that we need to apply for the lemma is $(1\,i)\,(2\,j)$ – that is, exchange 1 with i and 2 with j, with $\mu = 1$.)

Hence (A)⇒(B). □

4.3. APPLICATION OF RESULT

In this section we illustrate how to apply theorem 4.1 and how not to apply it; then we consider some experimental results.

4.3.1. AN ALGORITHM FOR THEOREM 4.1.

Algorithm 4.1 implements the result. It checks whether any term is constant, then checks whether every pair of terms is relatively prime. Since clause (B) considers only the leading terms – not the term ordering, and not the trailing monomials – we only need to provide these leading terms as the inputs of algorithm `Can_Skip_All_SPolys`. In an application, the user would first calculate the leading terms $t_1, \ldots, t_m$ of $f_1, \ldots, f_m$ with respect to $\succ$; then she would pass these leading terms to the implementation of algorithm 4.1.

4.3.2. EXAMPLES OF THEOREM 4.1.

Algorithm 4.1 `Can_Skip_All_SPolys`

Inputs: $t_1, \ldots, t_m$

Output: `YES` if we can skip all S-polynomial reductions for all polynomials with leading terms $t_1, \ldots, t_m$; `NO` otherwise

For $i = 1, \ldots, m$

  If $t_i = 1$ **Then**

    Return YES

$\mathcal{B} \leftarrow \{(i, j) : 1 \leq i < j \leq m\}$

For $(i, j) \in \mathcal{B}$

  If $\gcd(t_i, t_j) \neq 1$ **Then**

    Return `NO`

Return `YES`

EXAMPLE 4.2. Let $f_1 = x + 2y + 3z - 1$, $f_2 = y - z + 3$, $f_3 = z + 4$. The reader may notice that f_1, f_2, f_3 are linear, and in triangular form.

We consider two different term orderings. If $\succ = \text{lex}(x, y, z)$, then

$$\overline{f_1} = x \quad \overline{f_2} = y \quad \overline{f_3} = z$$

We see that all the leading terms are relatively prime; by theorem 4.1, we can conclude that f_1, f_2, f_3 are a Gröbner basis with respect to $\succ$ without checking a single S-polynomial. This agrees with the triangular form of the linear system.

In the second case, let $\succ = \text{lex}(x, z, y)$. At this point, the leading term of f_2 changes to z, so that the leading terms of f_2 and f_3 are no longer relatively prime.

None of the leading terms is 1. Applying theorem 4.1, we see that we *cannot* conclude that f_1, f_2, f_3 are a Gröbner basis with respect to $\succ$. In fact,

$$\begin{aligned} S_{2,3} &= \frac{\operatorname{lcm}(z,z)}{-z} \cdot (y - z + 3) - \frac{\operatorname{lcm}(z,z)}{z} \cdot (z + 4) \\ &= -1 \cdot (y - z + 3) - (z + 4) \\ &= -y - 7 \end{aligned}$$

None of the monomials of $S_{2,3}$ is divisible by the leading term of any of f_1, f_2, f_3, so that f_1, f_2, f_3 are not a Gröbner basis with respect to $\succ$. In this case, the triangular form of the linear system does not guarantee a Gröbner basis, because the second term ordering prioritizes the pivots differently. The corresponding coefficient matrix is clearly not upper triangular:

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

◇

Since theorem 4.1 considers only the leading terms, we expect to find polynomial systems whose leading terms do not satisfy its hypotheses even though the polynomials are themselves a Gröbner basis. Our second example illustrates this.

EXAMPLE 4.3. Let $f_1 = xy + bx$, $f_2 = x^2 - bx$. Let $\succ$ be any term ordering on terms in x and y. Notice that b is constant in this term ordering. The leading terms of the

polynomials are

$$\overline{f_1} = xy \qquad \overline{f_2} = x^2$$

Since the leading terms are not relatively prime, and neither leading term equals 1, we cannot conclude from theorem 4.1 that they are a Gröbner basis with respect to $\succ$.

It turns out, however, that they are in fact a Gröbner basis with respect to $\succ$. We have

$$\begin{aligned} S_{1,2} &= \frac{\operatorname{lcm}(xy, x^2)}{xy} \cdot (xy + bx) - \frac{\operatorname{lcm}(xy, x^2)}{x^2} \cdot \left(x^2 - bx\right) \\ &= x \cdot (xy + bx) - y \cdot \left(x^2 - bx\right) \\ &= bx^2 + bxy \end{aligned}$$

Then

$$S_{1,2} \underset{b \cdot f_1}{\longrightarrow} bx^2 - b^2x \underset{b \cdot f_2}{\longrightarrow} -b^2x + b^2x = 0$$

◇

4.3.3. EXPERIMENTAL RESULTS. We ran two sets of experiments using Maple.

HOW DOES THEOREM 4.1 APPLY UNDER DIFFERENT CONDITIONS? In the first experiment, we tested how often theorem 4.1 would allow us to skip every S-polynomial reduction. Given a random set of polynomials, we expect that all the leading terms will be relatively prime only rarely, and the data did not provide any surprises here! On the other hand, changing certain parameters (the term ordering, the total degree, and the number of variables) provided some interesting insight.

The program we wrote chose polynomials using Maple's `randpoly()` with the following parameters:

we looped from $n = 2$ to $n = 6$ variables

for each n, we looped from $d = 10$ to $d = 10n$,

where d was the maximum degree of a term,

incrementing d by n with each iteration

for each value of d, we generated 100,000 sets of polynomials

each set consisted of at least 2, at most n sparse polynomials

number of terms per polynomial: `rand(2..20)`

coefficients: `rand(-99..99)`

exponents: `rand(0..5)`

For each set of at most n polynomials, we computed the leading terms with respect to a fixed term ordering, either total-degree or lexicographic. If every pair of leading terms was relatively prime, we knew from theorem 4.1 that the set was a Gröbner basis.

Why did we restrict each set of polynomials to at most n (the number of variables)? If there are n variables, then $n + 1$ polynomials cannot all be relatively prime, so there is no point in testing the theorem there: for *all* systems with $n + 1$ or more polynomials, we will have to check at least one S-polynomial reduction.

We used Maple's `time()` command to keep track of how much time we spent evaluating whether the leading terms were relatively prime. In nearly all cases, the *sum* of these times over all 100,000 sets of polynomials for each n and d was reported as 0 seconds. The only exception was when $n = 6$ and $d = 58$; in this very last case, the software spent 0.009 seconds in evaluation.[1]

It should come as no surprise that the leading terms of *every* pair of polynomials are almost never relatively prime. We see this illustrated in tables 4.1 (when the term ordering is total-degree) and 4.2 (when the term ordering is lexicographic).

For a total-degree term ordering and only two variables, we get a relatively high frequency of success when the total degree is low: about 1.5% of the sets of polynomials for total degree $d = 10$. Naturally, the frequency of success decreases as we increase the total degree, since a higher total degree means that the terms can contain more variables. We have less than 0.5% success when the total degree is 20.

[1]Maple's `time()` command only keeps track of the amount of time spent in evaluation, and not in simplification. It certainly took much more than zero seconds to run the program; in fact, it took about a day. However, whatever time that simplification would add is dwarfed by the amount of simplification in polynomial reduction: see for example table 4.4.

Table 4.1: Number of sets of polynomials where every pair of leading terms is relatively prime, out of 100,000 sets.

	$d = 10$	$d = 10 + n$	$d = 10 + 2n$	$d = 10 + 3n$	$d = 10 + 4n$
$n = 2$	1507	1174	882	683	577
$n = 3$	910	470	264	178	103
$n = 4$	569	190	97	44	31
$n = 5$	407	92	33	15	5
$n = 6$	338	44	14	6	1

	$d = 10 + 5n$	$d = 10 + 6n$	$d = 10 + 7n$	$d = 10 + 8n$
$n = 2$	486			
$n = 3$	67	49		
$n = 4$	13	8	12	
$n = 5$	0	3	3	2
$n = 6$	0	0	0	0

(n variables; $2 \ldots n$ polynomials per set; d the maximum degree of a term; exponents range from 0 to 5; total-degree term ordering with $x_1 \succ \cdots \succ x_n$)

Table 4.2: Number of sets where every pair of leading terms is relatively prime, out of 100,000 sets.

	$d = 10$	$d = 10 + n$	$d = 10 + 2n$	$d = 10 + 3n$	$d = 10 + 4n$
$n = 2$	145	86	54	42	30
$n = 3$	67	31	18	8	2
$n = 4$	65	14	9	3	1
$n = 5$	30	5	1	1	1
$n = 6$	29	8	1	0	0

	$d = 10 + 5n$	$d = 10 + 6n$	$d = 10 + 7n$	$d = 10 + 8n$
$n = 2$	24			
$n = 3$	3	0		
$n = 4$	0	2	0	
$n = 5$	0	0	0	0
$n = 6$	0	0	0	0

(n variables; $2 \ldots n$ polynomials per set; d the maximum degree of a term; exponents range from 0 to 5; lexicographic term ordering with $x_1 \succ \cdots \succ x_n$)

The success rate also drops when we increase the pool of variables. Already with three variables, the number of times we could skip every S-polynomial reduction has dipped below 0.9%, even when $d = 10$. This came as something of a surprise to me; I expected that with more variables available per term and a *fixed* total degree, the probability of single-variable terms would increase. Apparently the addition of these single-variable terms is counterbalanced by the large number of terms that are not single-variable, but have the same total degree. However, this does not explain everything, as we will see in the following paragraph.

The general pattern of table 4.1 is repeated in table 4.2 where the term ordering is lexicographic. However, the totals for each case are drastically smaller than they were in table 4.1. This would seem to be because single-variable terms occur with high degree. Consider $x_1x_2 + x_2^3$: a total-degree term ordering would return x_2^3 as the leading term, while a lexicographic term ordering would return x_1x_2 as the leading term. This latter term, which has more variables, is less likely to be relatively prime with the leading terms of other polynomials.

My explanations for the observed phenomena may appear inconsistent. In the first, I argued that although we should have a higher probability of single-variable terms as we increase n, these do not increase the overall success rate because they are outweighed by other terms in a total-degree term ordering. In the second, I argued that, single-variable terms are more likely to be the leading terms of a polynomial in a total-degree term ordering than in a lexicographic term ordering.

These two arguments are not, however, inconsistent, because I'm arguing in two different contexts. For a *fixed* number of variables n, single-variable terms of high degree will be favored by the total-degree term ordering, while the given lexicographic term ordering will favor any term with x_1 regardless of the total degree.

For *increasing* n, however, the number single-variable terms may increase, but the test program ordered the indeterminates as

$$x_1 \succ x_2 \succ \cdots \succ x_n$$

The additional single-variable terms are powers of "less privileged" indeterminates, so that $x_1 x_2 \succ x_2^2$ for both term orderings.

WHAT IS THE PROBABILITY OF ENCOUNTERING A GRÖBNER BASIS THAT IS NOT SKIPPED? The second experiment was designed to get an idea of the probability that a random set of at most n polynomials will be a Gröbner basis. We also used the opportunity to compare the timings for checking theorem 4.1 and for reducing all S-polynomials. The results are given in tables 4.3 and 4.4.

In table 4.3, we computed 1,000 systems of random polynomials with at least two, at most n polynomials per system, where n is the number of variables. Using a total-degree term order, we checked combinatorially whether we could skip all S-polynomial reductions; then we checked by S-polynomial reduction whether the system was a Gröbner basis. We timed each of these computations.

Table 4.3: Comparison of the number of Gröbner bases found by S-polynomial reduction, to the number found by applying theorem 4.1.

# vars	Skips	other GBs	time to check skip	time to check reduction
2	5	3	.70s	165s
3	0	0	145.91s*	12015s
4	0	0	1.01s	4092s
5	0	0	.67s	115s
6	0	0	.63s	103s

(1000 total polynomials; n the number of variables; $2 \dots n$ polynomials per set, where n =#vars; $10 \times n$ the maximum degree of a term; exponents range from 0 to 5; total-degree term ordering with $x_1 \succ \cdots \succ x_n$)
*This number must be a fluke; see the discussion in the text.

Again, almost none of the random polynomials that we generated were Gröbner bases. In fact, the only time we found any Gröbner bases at all was for $n = 2$ variables. Out of a total of 1,000 polynomials for each value of n, this is not surprising. Why did we keep the total so small? Reduction takes too much time.

Interestingly, theorem 4.1 detected most of the Gröbner bases that we did find (5 out of 8). Keep in mind that these are *unstructured* polynomials, so we naturally do not expect to find many Gröbner bases. In a structured set of polynomials, we would expect more Gröbner bases to be detected by S-polynomial reduction, and very few of them to be detected by theorem 4.1.

As expected, the total time to check the conditions of theorem 4.1 was very small, whereas the time to reduce all S-polynomials to zero was larger by several orders of magnitude. There was one strange result: for $n = 3$ variables, we had the strange result that it took nearly 146 seconds to check the leading terms. I am not

Table 4.4: Comparison of the number of Gröbner bases found by S-polynomial reduction, to the number found by applying theorem 4.1.

# vars	Skips	total GBs	time to check skip	time to check reduction
2	17453	25502	.02s	19885.71s
3	5952	11005	.03s	37295.14s
4	1726	3878	.03s	92538.03s
5	416	1237	.03s	252596.89s

(1,000,000 total systems of two polynomials; n the number of variables; 10×#vars the maximum degree of a term; exponents range from 0 to 5; total-degree term ordering with $x_1 \succ \cdots \succ x_n$)

sure why this happened. We ran the tests in sets of 100, and one of the sets took 144.58 seconds. Take that one away, and we have a far more reasonable result: 1.33 seconds. By contrast, the corresponding set of S-polynomial reductions was not abnormally higher than normal; there were other reductions that were much higher. We are not sure what caused this; later tests did not show a recurrence.

We do notice that the total time increases from $n = 2$ through $n = 3$, then declines, both for checking theorem 4.1 and for checking the S-polynomial reductions. This could be due to a larger number of occasions for $n = 3$ where the first pair of the leading terms are relatively prime, or where the first computed S-polynomial reduces to zero; with a higher number of variables, that could be less likely.

In the second experiment, we held the number of polynomials fixed at $m = 2$. This gave us some confidence that the computed Gröbner bases would not take

too long to compute, so we could use a larger sample size of polynomials.[2] The results are given in table 4.4; clearly, the fixed number of polynomials helped keep the time to check the combinatorial criteria nearly constant. Again, almost none of the random polynomial systems were Gröbner bases: at most 2.5% for $n = 2$. Again, theorem 4.1 detected most of the Gröbner bases that we found: starting above 66%, and decreasing to around 33%.

As expected, the total time to check the conditions of theorem 4.1 remains very small, whereas the time to reduce all S-polynomials to zero grew by several orders of magnitude.

[2]As the reader sees from table 4.4, however, we gave up after $n = 5$.

Chapter 5

Skipping all but one S-polynomial reductions

5.1. PROBLEM

In chapter 4 we characterized completely the combinatorial criteria that allow us to skip every S-polynomial reduction. In this chapter, we turn our attention to the question of skipping all but one S-polynomial reduction: given polynomials $f_1, \ldots, f_m$, we want to know if they are a Gröbner basis, but we will only check one S-polynomial reduction. Without loss of generality, we can assume that the S-polynomial we *do* reduce is $S_{1,2}$. We are looking for an algorithm that decides

$$\mathrm{CC}\left(t_1, \ldots, t_m, \succ, \{(1,2)\}\right)$$

By definition 3.1 on page 80, this is equivalent to

$$\left[S_{1,2} \xrightarrow[(f_1,\ldots,f_m)]{*} 0 \quad \Rightarrow \quad \mathrm{GB}_{\succ}(f_1,\ldots,f_m)\right] \qquad \forall f_1,\ldots,f_m \text{ such that } \overline{f_k} = t_k$$

As in chapter 4, it is fairly clear that satisfying some formulation of Buchberger's first criterion would allow us to skip all but one S-polynomial reduction. We would also like to know whether Buchberger's second criterion will help us to skip all but one S-polynomial reduction, or whether additional criteria on the leading terms will prove useful.

The answer is given by algorithm 5.1 on page 110, which follows from theorem 5.1.

5.2. RESULT

THEOREM 5.1. *(A) is equivalent to (B) where:*

(A) $S_{1,2} \xrightarrow[(f_1,\ldots,f_m)]{*} 0 \Rightarrow \mathrm{GB}_{\succ}(f_1,\ldots,f_m)$

$\forall f_1,\ldots f_m$ *such that* $\overline{f_1} = t_1, \ldots, \overline{f_m} = t_m$

(B) *(B1)* $\vee$ *(B2)* $\vee$ *(B3)* $\vee$ *(B4) where*

(B1) $\gcd(t_i,t_j) = 1 \;\; \forall (i,j) \neq (1,2)$

(B2) $t_1 \mid t_2$ *and* $\gcd(t_i,t_j) = 1 \;\; \forall i \neq j, i \neq 2, j \neq 2$

(B3) $t_2 \mid t_1$ *and* $\gcd(t_i,t_j) = 1 \;\; \forall i \neq j, i \neq 1, j \neq 1$

(B4) $t_k = 1 \; \exists k$

A few comments before the proof.

As with theorem 4.1 on page 87, we see that no additional combinatorial criteria figure into theorem 5.1: (B) is a formulation of Buchberger's two criteria, and the trivial criterion that some polynomial be constant. Note in particular that clauses (B2) and (B3) are applications of the first and the second criteria: if $t_1 \mid t_2$, then certainly $t_1 \mid \operatorname{lcm}(t_2, t_k)$ for all $k > 2$. As a result, it is fairly obvious that (A)⇐(B).

However, proving (A)⇒(B) is more difficult than it was for theorem 4.1. Again, we approach via the contrapositive and employ lemma 3.2 on page 83; this time, however, we need more than one counterexample, because the negation of (B) expands to several cases. It may be possible to resolve all these cases using only one counterexample, but if so, we have not found it.

PROOF. (Of theorem 5.1, (A)⇒(B).)

We show the contrapositive: namely, ¬(A)⇐¬(B). So assume ¬(B). Then ¬(B1) and ¬(B2) and ¬(B3) and ¬(B4).

We will show ¬(A).

From ¬(B1), we know that $\exists\,(i,j) \neq (1,2)$ such that $\gcd(t_i, t_j) \neq 1$.

From ¬(B4), we know that $\forall k\ t_k \neq 1$.

By distribution and De Morgan, we know that ¬(B2) $\wedge$ ¬(B3) is logically equivalent to (D1) $\vee$ (D2) $\vee$ (D3) $\vee$ (D4) where

(D1) $t_1 \nmid t_2$ and $t_2 \nmid t_1$

(D2) $t_1 \nmid t_2$ and $\gcd(t_i, t_j) \neq 1\ \exists i \neq j$, $i \neq 1$, $j \neq 1$

(D3) $t_2 \nmid t_1$ and $\gcd(t_i, t_j) \neq 1\ \exists i \neq j$, $i \neq 2$, $j \neq 2$

(D4) $\gcd(t_i, t_j) \neq 1 \; \exists i \neq j, i \neq 1, j \neq 1$

and $\gcd(t_i, t_j) \neq 1 \; \exists i \neq j, i \neq 2, j \neq 2$

We consider each case in turn.

Case 1: *(D1)* $t_1 \nmid t_2$ and $t_2 \nmid t_1$

Recall $\exists (i, j) \neq (1, 2)$ such that $\gcd(t_i, t_j) \neq 1$. Without loss of generality, $j > 2$.

We have two subcases.

Case 1a: $t_1 \nmid t_j$ and $t_2 \nmid t_j$.

Let $F = (f_1, \ldots, f_m)$ where

$$f_1 = t_1$$

$$f_2 = t_2$$

$$f_j = t_j$$

$$f_k = t_k + 1 \text{ for } k \neq 1, 2, j$$

Observe that $S_{1,2} \xrightarrow[F]{*} 0$ trivially.

Then

$$\begin{aligned} S_{i,j} &= \frac{\operatorname{lcm}(t_i, t_j)}{t_i} \cdot (t_i + 1) - \frac{\operatorname{lcm}(t_i, t_j)}{t_j} \cdot t_j \\ &= \operatorname{lcm}(t_i, t_j) + \frac{\operatorname{lcm}(t_i, t_j)}{t_i} - \operatorname{lcm}(t_i, t_j) \\ &= \frac{\operatorname{lcm}(t_i, t_j)}{t_i} \end{aligned}$$

Since

$$\operatorname{lcm}(t_i, t_j) = \frac{t_i t_j}{\gcd(t_i, t_j)}$$

we have

$$S_{i,j} = \frac{t_j}{\gcd(t_i, f_j)}$$

Obviously $S_{i,j} \mid t_j$.

Since $t_1 \nmid t_j$ and $S_{i,j} \mid t_j$, $\widehat{f_1} \nmid S_{i,j}$.

Since $t_2 \nmid t_j$ and $S_{i,j} \mid t_j$, $\widehat{f_2} \nmid S_{i,j}$.

Since $\gcd(t_i, t_j) \neq 1$, $\widehat{f_j} \nmid S_{i,j}$.

By lemma 3.2, $S_{i,j} \overset{*}{\underset{F}{\nrightarrow}} 0$. (Use the permutation $(3\ j)$ with $\mu = 3$.)

Case 1b: $t_1 \mid t_j$ or $t_2 \mid t_j$

Let $F = (f_1, \ldots, f_m)$ where

$$f_1 = t_1$$

$$f_2 = t_2$$

$$f_k = t_k + 1 \text{ for } k \neq 1, 2$$

Observe that $S_{1,2} \xrightarrow[F]{*} 0$ trivially.

If $t_1 \mid t_j$, then $S_{1,j} = -1$. Recall $t_k \neq 1$ for $k = 1, \ldots, m$. So $S_{1,j} \overset{*}{\underset{F}{\nrightarrow}} 0$.

Otherwise, $t_2 \mid t_j$, whence $S_{2,j} = -1 \overset{*}{\underset{F}{\nrightarrow}} 0$.

Case 2: *(D2)* $t_1 \nmid t_2$and$\gcd(t_i, t_j) \neq 1\ \exists i \neq j$, $i \neq 1$, $j \neq 1$

Without loss of generality, $j \neq 2$.

We have three subcases.

Case 2a: $t_1 \nmid t_i$ and $t_2 \nmid t_i$

This case is proved using a proof similar to that of case 1a, exchanging i and j.

Case 2b: $t_1 \mid t_i$

We note that since $t_1 \nmid t_2$ for case 2, $i \neq 2$.

Let $F = (f_1, \ldots, f_m)$ where

$$f_1 = t_1$$

$$f_2 = t_2$$

$$f_k = t_k + 1 \text{ for } k \neq 1, 2$$

Observe that $S_{1,2} \xrightarrow[F]{*} 0$ trivially.

We have $S_{1,i} = -1 \overset{*}{\underset{F}{\not\to}} 0$.

Case 2c: $t_2 \mid t_i$

Let $F = (f_1, \ldots, f_m)$ where

$$f_1 = t_1$$

$$f_2 = t_2$$

$$f_k = t_k + 1 \text{ for } k \neq 1, 2$$

Observe that $S_{1,2} \xrightarrow[F]{*} 0$ trivially.

If $i \neq 2$, then $S_{2,i} = -1$. Recall $t_k \neq 1$ for $k = 1, \ldots, m$; thus $S_{2,i} \overset{*}{\underset{F}{\not\to}} 0$.

Otherwise $i = 2$; consider

$$\begin{aligned} S_{2,j} &= \frac{\operatorname{lcm}(t_2, t_j)}{t_2} \cdot t_2 - \frac{\operatorname{lcm}(t_2, t_j)}{t_j} \cdot (t_j + 1) \\ &= \operatorname{lcm}(t_2, t_j) - \operatorname{lcm}(t_2, t_j) - \frac{\operatorname{lcm}(t_2, t_j)}{t_j} \\ &= -\frac{\operatorname{lcm}(t_2, t_j)}{t_j} \end{aligned}$$

Since

$$\operatorname{lcm}(t_2, t_j) = \frac{t_2 t_j}{\gcd(t_2, t_j)}$$

we have

$$S_{2,j} = -\frac{t_2}{\gcd(t_2, t_j)}$$

Obviously $S_{2j} \mid t_2$.

Recall $t_1 \nmid t_2$; hence $\widehat{f_1} \nmid S_{2j}$.

Recall $\gcd(t_2, t_j) = \gcd(t_i, t_j) \neq 1$; then $\widehat{f_2} \nmid S_{2j}$.

By lemma 3.2, $S_{2j} \xrightarrow[F]{*} 0$. (Use $\mu = 2$; no permutation is necessary.)

Case 3: *(D3)* $t_2 \nmid t_1$and $\gcd(t_i, t_j) \neq 1$ $\exists i \neq j$, $i \neq 2$, $j \neq 2$

This case is symmetric to case 2, so we can prove it symmetrically.

Case 4: *(D4)* $\gcd(t_i, t_j) \neq 1$ $\exists i \neq j$, $i \neq 1$, $j \neq 1$

and $\gcd(t_i, t_j) \neq 1$ $\exists i \neq j$, $i \neq 2$, $j \neq 2$

For the sake of clarity, we rewrite this case as

$\gcd(t_i, t_j) \neq 1$ $\exists i \neq j$, $i \neq 1$, $j \neq 1$ and $\gcd(t_k, t_\ell) \neq 1$ $\exists k \neq \ell$, $k \neq 2$, $\ell \neq 2$

We have already considered the subcase $t_1 \nmid t_2$ in case 2, and the subcase $t_2 \nmid t_1$ in case 3. We may assume therefore that $t_1 \mid t_2$ and $t_2 \mid t_1$, or $t_1 = t_2$.

We have two subcases.

Case 4a: $t_1 \nmid t_i$

This case is proved using a proof similar to that of case 1a, exchanging i and j.

Case 4b: $t_1 \mid t_i$

This case is proved using a proof similar to that of case 1b, exchanging i and j.

For all four cases:

In each case, $\exists F$ such that $S_{12} \xrightarrow[F]{*} 0$ but $\exists k, \ell$ such that $S_{k\ell} \overset{*}{\underset{F}{\not\to}} 0$.

Hence ¬(A). □

5.3. APPLICATION OF RESULT

We present examples of theorem 5.1, then consider some experimental results.

5.3.1. AN ALGORITHM FOR THEOREM 5.1. Implementing an algorithm that decides clause (B) of theorem 5.1 is still rather straightforward, although not so much as for theorem 4.1; see algorithm 5.1. The extra complication comes from clauses (B2) and (B3): on the first occasion that we encounter terms t_1 and t_2 that are not relatively prime, we need to search for a third term term t_3 that divides either t_1 or t_2. If we cannot find such a term, then (presuming we've checked for a constant polynomial) we can skip all but one S-polynomial reductions only if no other pair

of terms is relatively prime. The one S-polynomial reduction that we have to check is $S_{1,2}$.

If we do find a third term t_3 that divides t_1 (say), then two things follow immediately: (a) $S_{1,3}$ is the only S-polynomial that we can skip (since t_1 and t_3 are clearly not relatively prime) and (b) we no longer worry whether t_1 is relatively prime to the remaining terms. We do have to worry whether t_2 and t_3 are relatively prime to all other terms: if not, then we cannot skip the remaining S-polynomial reductions, since clause (B) of theorem 5.1 is not satisfied.

As with algorithm 4.1, we only need to pass the leading terms as inputs to our implementation of theorem 5.1, since clause (B) does not use the term ordering or any other part of the polynomials.

5.3.2. EXAMPLES OF THEOREM 5.1. We begin with a straightforward example of when the theorem allows us to skip all but one S-polynomial reductions.

EXAMPLE 5.2. Let

$$f_1 = y^2 + 1 \qquad f_2 = xy^3 + 1 \qquad f_3 = x^4 - x^2 + 1$$

Let $\succ$ be any admissible term ordering. Observe that

$$\overline{f_1} = y^2 \quad \overline{f_2} = xy^3 \quad \overline{f_3} = x^4$$

The theorem allows us to skip every S-polynomial reduction except $S_{1,2}$. *Why?* We have

Algorithm 5.1 `Can_Skip_All_But_One_SPolys`

Inputs: $t_1, \ldots, t_m$

Output: `YES` if we can skip all but one S-polynomial reductions for all polynomials with leading terms $t_1, \ldots, t_m$; `NO` otherwise

Local

number_spolys_cannot_skip $\leftarrow 0$

skipped_term $\leftarrow 0$

For $i = 1, \ldots, m$

If $t_i = 1$ **Then**

Return `YES`

$\mathcal{B} \leftarrow \{(i,j) : 1 \leq i < j \leq m\}$

For $(i,j) \in \mathcal{B}$

If $\gcd(t_i, t_j) \neq 1$ **Then**

Increment number_spolys_cannot_skip

If number_spolys_cannot_skip > 1 **and** skipped_term $\neq i, j$ **Then**

Return `NO`

Elseif number_spolys_cannot_skip $= 1$ **Then**

If Exists k: $t_k \mid t_i$ **Then**

skipped_term $\leftarrow i$

$\mathcal{B} \leftarrow \mathcal{B} \setminus \{(i,\ell) : \ell = 1, \ldots, m\}$

Elseif Exists k: $t_k \mid t_j$ **Then**

skipped_term $\leftarrow j$

$\mathcal{B} \leftarrow \mathcal{B} \setminus \{(j,\ell) : \ell = 1, \ldots, m\}$

Return `YES`

- $\overline{f_1} \mid \overline{f_2}$
- $\gcd\left(\overline{f_1}, \overline{f_3}\right) = 1$

This satisfies (B2) of theorem 5.1. Hence, if $S_{1,2} \xrightarrow[(f_1,f_2,f_3)]{*} 0$, we have $\mathrm{GB}_{\succ}(f_1, f_2, f_3)$.

As it turns out, $S_{1,2} \xrightarrow[(f_1,f_2,f_3)]{*} 0$, so f_1, f_2, f_3 are not a Gröbner basis. ———— ◇

Now we consider two more examples, both featuring the same set of polynomials. We will see how the choice of term ordering, as well as the ordering of the polynomials, helps determine whether the theorem applies.

EXAMPLE 5.3. Let

$$f_1 = x^3y^3 + 1 \quad f_2 = x^5y^3z^2 - z^6 - 1 \quad f_3 = z^7 + w^8 + 1 \quad f_4 = z^6 + x^2z^2 + 1$$

In this example, let $\succ = \mathrm{tdeg}(x, y, z, w)$. We have

$$\overline{f_1} = x^3y^3 \quad \overline{f_2} = x^5y^3z^2 \quad \overline{f_3} = w^8 \quad \overline{f_4} = z^6$$

Can we skip every S-polynomial except $S_{1,2}$?

Under the given term ordering, the leading terms satisfy (B2) of theorem 5.1: we have

- $\overline{f_1} \mid \overline{f_2}$
- $\gcd\left(\overline{f_1}, \overline{f_3}\right) = \gcd\left(\overline{f_1}, \overline{f_4}\right) = \gcd\left(\overline{f_3}, \overline{f_4}\right) = 1$

Hence, if $S_{1,2} \xrightarrow[(f_1,\ldots,f_4)]{*} 0$, we know that $\mathrm{GB}_{\succ}(f_1,\ldots,f_m)$. It turns out that we do in fact have a Gröbner basis here:

$$\begin{aligned} S_{1,2} &= \frac{\mathrm{lcm}\left(x^3y^3, x^5y^3z^2\right)}{x^3y^3} \cdot \left(x^3y^3+1\right) - \frac{\mathrm{lcm}\left(x^3y^3, x^5y^3z^2\right)}{x^5y^3z^2} \cdot \left(x^5y^3z^2 - z^6 - 1\right) \\ &= x^2z^2 \cdot \left(x^3y^3+1\right) - \left(x^5y^3z^2 - z^6 - 1\right) \\ &= z^6 + x^2z^2 + 1 \end{aligned}$$

Then

$$S_{1,2} \xrightarrow[1\cdot f_4]{} 0$$

◇

As noted above, the same polynomials give a different result if we change the term ordering:

EXAMPLE 5.4. Recall the polynomials of the previous example:

$$f_1 = x^3y^3 + 1 \quad f_2 = x^5y^3z^2 - z^6 - 1 \quad f_3 = z^7 + w^8 + 1 \quad f_4 = z^6 + x^2z^2 + 1$$

This time, use $\succ = \mathrm{lex}\,(x, y, z, w)$. We have

$$\overline{f_1} = x^3y^3 \quad \overline{f_2} = x^5y^3z^2 \quad \overline{f_3} = z^7 \quad \overline{f_4} = x^2z^2$$

The leading terms of f_3 and f_4 have changed from the previous example.

To approach this example systematically, let's trace through algorithm 5.1:

number_spolys_cannot_skip $\leftarrow 0$

skipped_term $\leftarrow 0$

$\mathcal{B} \leftarrow \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$

$(i,j) = (1,2)$:

Since t_i, t_j are not relatively prime,

number_spolys_cannot_skip $\leftarrow 1$

Since $t_4 \mid t_1$,

skipped_term $\leftarrow 1$

$\mathcal{B} \leftarrow \{(2,3),(2,4),(3,4)\}$

$(i,j) = (2,3)$

Since t_2, t_3 are not relatively prime,

number_spolys_cannot_skip $\leftarrow 2$

Since *number_spolys_cannot_skip* > 1 and *skipped_term* $\neq 2, 3$

Return `NO`

Under this term ordering, the algorithm finds that we *cannot* skip all S-polynomials reductions but one.

It remains the case that $S_{1,2}$ reduces to zero despite the new term ordering. However, $S_{2,3}$ does not:

$$\begin{aligned} S_{2,3} &= \frac{\operatorname{lcm}\left(x^5y^3z^2, z^7\right)}{x^5y^3z^2} \cdot \left(x^5y^3z^2 - z^6 - 1\right) - \frac{\operatorname{lcm}\left(x^5y^3z^2, z^7\right)}{z^7} \cdot \left(z^7 + w^8 + 1\right) \\ &= z^5 \cdot \left(x^5y^3z^2 - z^6 - 1\right) - x^5y^3 \cdot \left(z^7 + w^8 + 1\right) \\ &= -z^{11} - z^5 - x^5y^3w^8 - x^5y^3 \end{aligned}$$

Before showing a reduction path of $S_{2,3}$, we remind the reader of the leading terms:

$$\overline{f_1} = x^3y^3 \quad \overline{f_2} = x^5y^3z^2 \quad \overline{f_3} = z^7 \quad \overline{f_4} = x^2z^2$$

Thus

$$\begin{aligned} S_{2,3} &\underset{-x^2w^8 \cdot f_1}{\longrightarrow} -z^{11} - z^5 - x^5y^3 + x^2w^8 \\ &\underset{-x^2 \cdot f_1}{\longrightarrow} -z^{11} - z^5 + x^2w^8 + x^2 \\ &\underset{-z^4 \cdot f_3}{\longrightarrow} x^2w^8 + x^2 - z^5 + z^4w^8 + z^4 \\ &\underset{(f_1,\ldots,f_4)}{\nrightarrow} \end{aligned}$$

The remaining reduction paths are nearly identical, although too numerous to list here. Hence $S_{2,3} \underset{(f_1,\ldots,f_4)}{\nrightarrow} 0$. ◇

5.3.3. EXPERIMENTAL RESULTS. Again, we ran two kinds of experiments: one to see how often the criteria applied, and one to compare the number of skipped systems to the number of Gröbner bases.

HOW OFTEN DOES THEOREM 5.1 APPLY? The first thing I noticed when running experimental results is that the minimum number of polynomials we test should be three. In my first, naïve attempt to repeat the experiments of section 4.3.3, I ran a slight modification of the first experiment for theorem 4.1 (see page 93). I did not change the number of polynomials generated for each turn. Examining the

Table 5.1: Number of sets where we can skip all but one S-polynomial reduction, out of out of 100,000 sets.

	$d = 10$	$d = 10 + n$	$d = 10 + 2n$	$d = 10 + 3n$	$d = 10 + 4n$
$n = 3$	314	138	67	44	24
$n = 4$	220	41	15	2	1
$n = 5$	130	24	4	1	1
$n = 6$	86	10	0	0	0

	$d = 10 + 5n$	$d = 10 + 6n$	$d = 10 + 7n$	$d = 10 + 8n$
$n = 3$	16	9		
$n = 4$	1	1	0	
$n = 5$	0	0	0	0
$n = 6$	0	0	1	0

(n variables; $3 \ldots n + 1$ polynomials per set; d the maximum degree of a term; exponents range from 0 to 5; total-degree term ordering with $x_1 \succ \cdots \succ x_n$)

preliminary results, I noticed with creeping horror that, for two variables, I was obtaining "a 100% success rate", and I began to panic!

I spent a few minutes in frantic debugging before realizing how foolish I had been: for $n = 2$ variables, the first program would only test two polynomials. With a set of two polynomials, there is only one S-polynomial to reduce: $S_{1,2}$. It comes as no surprise, then, that for the set f_1, f_2, we can *always* skip "every S-polynomial reduction *but one*": $S_{1,2}$.

A revised program produced more reasonable results; see table 5.1. We generated the data in the following manner:

we looped from $n = 2$ to $n = 6$ variables

for each n, we looped from $d = 10$ to $d = 10n$ stepping by n

for each value of d, we generated 100,000 sets of polynomials

each set consisted of at least 3, at most $n + 1$ sparse polynomials

number of terms per polynomial: `rand(2..20)`

each term had maximum degree d

coefficients: `rand(-99..99)`

exponents: `rand(0..5)`

At this point, I made another mistake: I began comparing the data in table 5.1 with that of table 4.1. Again, I began to panic: one would expect that there would be *more* sets of polynomials where we can skip all but one S-polynomial reduction, than when we can skip all reductions, since fewer leading terms have to be relatively prime. A naïve comparison of table 5.1 with table 4.1 suggests that there are *fewer* sets where we skip all but one S-polynomial reduction.

The reality is that the tables are incomparable due to the number of polynomials in each set. Table 5.1 allows $3 \ldots n + 1$ polynomials per set, while table 4.1 allows only $2 \ldots n$. To find data for comparison, we modified the program that generated table 4.1 so that it would test $2 \ldots n + 1$ polynomials per set for $n > 3$ indeterminates, and ran it to see how often all leading terms would be relatively prime. This gave us table 5.2.

The resulting difference is staggering, although hardly surprising: a larger set of polynomials has a drastically lower probability that all the leading terms will be relatively prime. The program that generated table 4.1 had $2 \ldots n$ polynomials, where n is the number of variables; thus, *every* set enjoyed *some* chance that the

Table 5.2: Experimental results: number of sets, out of 100,000, where we can skip all S-polynomial reductions.

	$d = 10$	$d = 10 + n$	$d = 10 + 2n$	$d = 10 + 3n$	$d = 10 + 4n$
$n = 3$	1	0	0	0	0
$n = 4$	1	0	0	0	0
$n = 5$	2	0	0	0	0
$n = 6$	0	0	0	0	0

	$d = 10 + 5n$	$d = 10 + 6n$	$d = 10 + 7n$	$d = 10 + 8n$
$n = 3$	0	0		
$n = 4$	0	0	0	
$n = 5$	0	0	0	0
$n = 6$	0	0	0	0

(n variables; $2 \ldots n + 1$ polynomials per set; d the maximum degree of a term; exponents range from 0 to 5; total-degree term ordering with $x_1 \succ \cdots \succ x_n$)

leading terms would be relatively prime. The program that generated table 5.2, on the other hand, has $2 \ldots n + 1$ polynomials, so that some sets would have more polynomials than variables. In *these* sets, there is *no* chance the leading terms will be relatively prime.

We can make another observation by comparing tables 4.1 and 5.2: nearly all the successful skips of table 4.1 appear to have come from sets of two polynomials. This would explain why table 5.2 generated effectively no sets where we could skip S-polynomial reduction, whereas table 4.1 had a rather high number.

We return to the data of table 5.1. As we see, there are a number of systems where we can skip all but one S-polynomial reductions. Unlike tables 4.1-4.3, however, these systems are not necessarily a Gröbner basis! That depends on whether

Table 5.3: Comparison of the number of Gröbner bases found by S-polynomial reduction, to the number found by applying theorem 5.1.

# vars	skips	total GBs	time to check skip	time to check reduction
2	2301 (0)	0	.04s	39803.68s
3	128 (3)	8	.08s	116615.28s
4	8 (0)	0	5.01s	219152.64s

*Numbers in parentheses indicated the number of Gröbner bases were all but one S-polynomial reduction were skipped.
(1,000,000 total systems of three polynomials; 20×#vars the maximum degree of a term; exponents range from 0 to 5; total-degree term ordering with $x_1 \succ \cdots \succ x_n$)

the remaining S-polynomial reduces to zero. Presumably, some of them are (algorithm 5.1 captures all the occasions that we can skip all) but many of them are probably not.

WHAT IS THE PROBABILITY OF ENCOUNTERING A GRÖBNER BASIS THAT IS (OR IS NOT) SKIPPED? We also ran a test to see how often we might find a Gröbner basis that did *not* apply. The results of this test are given in table 5.3.

In this test, we generated systems of three polynomials. Despite the large number of polynomial systems generated, we did not encounter many Gröbner bases at all: eight out of 3,000,000! Of those eight, we skipped all but one S-polynomial reductions in three systems: that counts as two skips per system, so we could have saved six S-polynomial reductions. This stands in marked contrast to the results of section 4.3.3, but this appears to be because we have found so few Gröbner bases to start with. When we did find a Gröbner basis, we were able to skip two S-polynomial reductions for almost half of them. The time required to check

whether we can skip all but one S-polynomial remains quite small in comparison to the time required to check the system by S-polynomial reduction.

Chapter 6

Skipping all but two S-polynomial reductions (case for three polynomials)

6.1. PROBLEM

After chapters 4 and 5, the next logical step is to find a criterion for skipping all but two S-polynomial reductions. Formally, we want an algorithm that decides

$$\mathrm{CC}\left(t_1, \ldots, t_m, \succ, \{(1,2), (2,3)\}\right)$$

We first approached this problem in the same manner as in the previous two chapters: we tried to build counterexamples to show that Buchberger's two criteria were the best that we could do, as in theorems 4.1 on page 87 and 5.1 on page 102. This turned out to be much more difficult than we anticipated. We have yet to find the solution to this general form for m terms.

We decided to restrict the problem to a more specific form:

$$\mathrm{CC}\left(t_1, t_2, t_3, \succ, \{(1,2), (2,3)\}\right)$$

By definition 3.1 on page 80, this is equivalent to

$$\left[S_{1,2} \underset{(f_1,f_2,f_3)}{\overset{*}{\longrightarrow}} 0 \text{ and } S_{2,3} \underset{(f_1,f_2,f_3)}{\overset{*}{\longrightarrow}} 0 \quad \Rightarrow \quad S_{1,3} \underset{(f_1,f_2,f_3)}{\overset{*}{\longrightarrow}} 0\right]$$
$$\forall f_1, f_2, f_3 \text{ such that } \overline{f_k} = t_k$$

At first, this also turned out to be too difficult (but we will return to it before long).

At this point, we restricted term ordering:

$$\mathrm{CC}\left(t_1, t_2, t_3, \mathrm{lex}\left(x_0, x_1, x_2, x_3\right), \{(1,2), (2,3)\}\right)$$

Again, the problem turned out to be too difficult. We were able to show that Buchberger's criteria were necessary for most cases, but the last case resisted solution. In this case, the leading terms satisfied

$$\gcd\left(t_1, t_3\right) \mid t_2 \tag{6.1}$$

One day, we sat down at the computer and used Maple to trace through all possible reductions for all polynomials with these leading terms:

$$t_1 = x_0 x_1 \quad t_2 = x_0 x_2 \quad t_3 = x_0 x_3$$

Notice that $\gcd(t_1, t_3) = x_0$ and $t_2 = x_0 x_2$, so these leading terms satisfy (6.1). On the other hand, no permutation of the terms gives either $\gcd(t_1, t_3) = 1$ or $t_2 \mid \operatorname{lcm}(t_1, t_3)$, so Buchberger's criteria do not apply to these terms.

When we say that we used Maple to trace through "all polynomials with these leading terms," we mean with respect to lex (x_0, x_1, x_2, x_3), as indicated above. This gives the form

$$f_k = t_0 t_k + t_0 \cdot A + B$$

where, for all monomials m in A or in B, $t_0 \nmid m$.

To our amazement, we learned that in this restricted situation,

$$S_{1,2} \xrightarrow[(f_1,f_2,f_3)]{*} 0 \quad \text{and} \quad S_{2,3} \xrightarrow[(f_1,f_2,f_3)]{*} 0 \qquad \Rightarrow \qquad S_{1,3} \xrightarrow[(f_1,f_2,f_3)]{*} 0$$

This means that Buchberger's criteria are *not* the only combinatorial criteria that allow us to skip S-polynomial reduction.

After writing, correcting, and revising the proof, we generalized it to the form

$$t_1 = x_0 x_1^{\alpha_1} \quad t_2 = x_0 x_2^{\alpha_2} \quad t_3 = x_0 x_3^{\alpha_3}$$

The restriction that $\succ =$ lex (x_0, x_1, x_2, x_3) remained. We tried to remove this condition, but we hit another brick wall; several months would pass before we finally found a criterion independent of the term ordering. We present it in theorem 6.3.

6.2. RESULT

We need to define two new combinatorial criteria.

DEFINITION 6.1. For all indeterminates x, we write

$$\mathrm{VB1}_x\left(t_1, t_3\right) \Leftrightarrow \min\left(\deg_x t_1, \deg_x t_3\right) = 0$$

$$\mathrm{VB2}_x\left(t_1, t_2, t_3\right) \Leftrightarrow \deg_x t_2 \leq \max\left(\deg_x t_1, \deg_x t_3\right)$$

We can consider these two criteria "variable-wise Buchberger criteria": the first is satisfied if t_1 and t_3 are relatively prime with respect to x (but not necessarily with respect to all variables); the second is satisfied if t_2 divides the least common multiple of t_1 and t_3 on x (but not necessarily on all variables).

The following example will help familiarize us with the criteria.

EXAMPLE 6.2. Let

$$t_1 = x_0 x_1 \qquad t_2 = x_0 x_2 \qquad t_3 = x_0 x_3$$

Observe that $\deg_{x_0} t_2 = \deg_{x_0} t_1$, so

$$\mathrm{VB2}_{x_0}\left(t_1, t_2, t_3\right)$$

Also, for $k = 1, 2, 3$ we have at least one of $\deg_{x_k} t_1 = 0$ or $\deg_{x_k} t_3 = 0$, so

$$\mathrm{VB1}_{x_k}\left(t_1, t_3\right)$$

Hence one of the "variable-wise" criteria applies to each indeterminate. ◇

Our main theorem is

THEOREM 6.3. *(A) ⇔ (B) where*

(A) [$S_{1,2} \xrightarrow[(f_1,f_2,f_3)]{*} 0$ *and* $S_{2,3} \xrightarrow[(f_1,f_2,f_3)]{*} 0$ *] implies* $S_{1,3} \rightsquigarrow 0$
$\forall f_1, f_2, f_3$ *such that* $\overline{f_k} = t_k$

(B) (B1) or (B2) where

(B1) $\gcd(t_1, t_3) \mid t_2$ *or* $\mathrm{BC2}(t_1, t_2, t_3)$

(B2) $\mathrm{VB1}_x(t_1, t_3)$ *or* $\mathrm{VB2}_x(t_1, t_2, t_3)$ $\forall x \in \{x_1, \ldots, x_m\}$

We can consider (B) to have two parts: a *divisibility* criterion (B1), and a variable-wise Buchberger criterion (B2). Notice that theorem 6.3 provides criteria for the *second* complete criterion mentioned in the introduction, not the first. We repeat that the first complete criterion remains open for $m > 3$.

Observe that if Buchberger's criteria are satisfied, then (B) is also satisfied. *Why?* Assume first that $\mathrm{BC1}(t_1, t_3)$. Then $\gcd(t_1, t_3) = 1$; (B1) is satisfied by $\gcd(t_1, t_3) \mid t_2$, and (B2) is satisfied by $\forall x\ \mathrm{VB1}_x(t_1, t_3)$. On the other hand, suppose that we have instead $\mathrm{BC2}(t_1, t_2, t_3)$. Then $t_2 \mid \mathrm{lcm}(t_1, t_3)$; (B1) is satisfied by $\mathrm{BC2}(t_1, t_2, t_3)$, and (B2) is satisfied by $\forall x\ \mathrm{VB2}_x(t_1, t_2, t_3)$. (See also lemma 6.19 on page 166 below.)

Note also that if some $t_k = 1$, (B) is also satisfied: one of the divisibility conditions of (B1) is trivial; as is one of the variable-wise Buchberger criteria of (B2).

The proof of theorem 6.3 is long; we present it in three sections:

- useful facts (section 6.2.1)
- proof that (B) is necessary to (A) (section 6.2.2)
- proof that (B) is sufficient for (A) (section 6.2.3)

Let's consider one last example that will show how we discovered the criterion and its proof.

EXAMPLE 6.4. Let $\succ = \text{lex}\,(x, y, z)$ and

$$f_1 = y^6z^2 + z^4 + xz^3 \qquad f_2 = x^2z^6 + xy^6z^5 + x^4y^4z \qquad f_3 = z^3 + y^6z$$

We have

$$\overline{f_1} = xz^3 \qquad \overline{f_2} = x^4y^4z \qquad \overline{f_3} = y^6z$$

The criteria of theorem 6.3 are satisfied; the divisibility criterion because

$$\gcd\left(\overline{f_1}\,,\,\overline{f_3}\right) = z \qquad \overline{f_2} = x^4y^4z$$

and the variable-wise Buchberger criteria because

$$\text{VB1}_x\,(t_1, t_3)$$

$$\text{VB1}_y\,(t_1, t_3)$$

$$\text{VB2}_z\,(t_1, t_2, t_3)$$

We want to see why we can skip the reduction of $S_{1,3}$. First we compute it:

$$S_{1,3} = \frac{xy^6z^3}{xz^3} \cdot \left(y^6z^2 + z^4 + xz^3\right) - \frac{xy^6z^3}{y^6z} \cdot \left(z^3 + y^6z\right)$$

$$= y^{12}z^2 + y^6z^4 - xz^5$$

How does this reduce?

$$S_{1,3} \underset{-z^2 \cdot f_1}{\longrightarrow} y^{12}z^2 + 2y^6z^4 + z^6$$

$$\underset{y^6z \cdot f_3}{\longrightarrow} y^6z^4 + z^6$$

$$\underset{z^3 \cdot f^3}{\longrightarrow} 0$$

Collecting the quotients, we have the representation

$$S_{1,3} = h_1f_1 + h_3f_3$$

where

$$h_1 = -z^2 \qquad h_3 = y^6z + z^3$$

Where do these polynomials come from? Look again at f_1, f_3. They have a greatest common divisor. Separating it from its cofactors, we have

$$f_1 = z\left(y^6z + z^3 + xz^2\right)$$

$$f_2 = z\left(z^2 + y^6\right)$$

The *non*-leading monomials of the cofactors are

$$y^6z + z^3 \qquad z^2$$

These cofactors look suspiciously similar to h_1, h_3! ◇

$$S_{\succ}(f_1, f_2) \xrightarrow[(f_1,f_2,f_3)]{*} 0 \text{ and } S_{\succ}(f_2, f_3) \xrightarrow[(f_1,f_2,f_3)]{*} 0 \qquad S_{\succ}(f_1, f_3) \rightsquigarrow 0$$

$$\text{(6.12, 6.13)} \Downarrow \qquad \Uparrow \text{(1.37)}$$

$$f_k = c_k g \text{ where } \gcd(\overline{c_1}, \overline{c_3}) = 1 \text{ for } k = 1, 2, 3 \quad \underset{\text{(2.4)}}{\Rightarrow} \quad S_{\succ}(c_1, c_3) \rightsquigarrow 0$$

Numbers indicate which lemma or theorem is used to prove the implication.

Figure 6.1: Diagram of proof strategy for section 6.2.3.

The reader may recall a previous theorem whose proof uses a representation of non-leading monomials: Buchberger's first criterion. Indeed, our proof of the sufficiency of the new criterion (section 6.2.3) will use this fact. We can diagram the structure of the proof as in figure 6.1.

6.2.1. USEFUL FACTS. Our first lemma serves the same purpose for lemma 6.9 in this chapter that lemma 3.2 on page 83 serves for the previous two chapters.

The basic idea is the same. We have a monomial τ and polynomials $f_1, \ldots, f_m$. These latter polynomials are either monomials or binomials; we want them to have a structure that implies

$$\tau \xrightarrow[(f_1,\ldots,f_m)]{*} 0$$

How do we ensure this? No monomial f_k may divide τ, so for each k there must be some indeterminate x_{λ_k} with $\deg_{x_{\lambda_k}} f_k > \deg_{x_{\lambda_k}} \tau$. For every binomial f_ℓ, on the other hand, the structure is slightly different from the binomials of lemma 3.2: while the trailing term u_ℓ does not necessarily divide the leading term t_ℓ, we ensure

that for each x_{λ_k} noted for the monomials f_k, $\deg_{x_{\lambda_k}} u_\ell < \deg_{x_{\lambda_k}} t_\ell$. That way, $\tau \underset{f_k}{\longrightarrow} \tau'$ preserves $\deg_{x_{\lambda_k}} f_k > \deg_{x_{\lambda_k}} \tau'$.

LEMMA 6.5. *Let τ be a nonzero monomial, and $F = (f_1, \ldots, f_m)$ a system of polynomials. Then (A)⇒(B) where*

(A) $\exists \mu$ with $1 \leq \mu \leq m$ and $\exists \lambda_1, \ldots, \lambda_\mu$ such that [(A1) and (A2)] where

(A1) $\forall \ell = 1, \ldots, \mu$ such that

$$\deg_{x_{\lambda_\ell}} \widehat{f_\ell} > \deg_{x_{\lambda_\ell}} \tau$$

(A2) $\forall \ell = \mu + 1, \ldots, m$

$$f_\ell = t_\ell + u_\ell$$

$$t_\ell \succ u_\ell$$

$$\deg_{x_{\lambda_i}} t_\ell \geq \deg_{x_{\lambda_i}} u_\ell \quad \forall i = 1, \ldots, \mu$$

(B) $\tau \underset{F}{\overset{*}{\nrightarrow}} 0$.

PROOF. Assume (A). We want to show (B).

Consider an arbitrary reduction path of τ over F:

$$\tau = \tau_0 \underset{f_{k_1}}{\longrightarrow} \tau_1 \underset{f_{k_2}}{\longrightarrow} \cdots \underset{f_{k_r}}{\longrightarrow} \tau_r \underset{F}{\nrightarrow}$$

We want to show $\tau_r \neq 0$. We show this by proving that τ_i and $f_1, \ldots, f_m$ satisfy (A) for $i = 1, \ldots, r-1$; since τ_i can reduce only over a binomial, $\tau_{i+1} \neq 0$. We proceed by induction on i.

Inductive base: $i = 0$

Since $\tau_0 = \tau$, we know by hypothesis that τ_0 and $f_1, \ldots, f_m$ satisfy (A).

Inductive step:

Assume that $\tau_i \neq 0$, and that τ_i and $f_1, \ldots, f_m$ satisfy (A).

We show that $\tau_{i+1} \neq 0$, and that τ_{i+1} and $f_1, \ldots, f_m$ also satisfy (A).

Let ℓ be such that $\tau_i \underset{f_\ell}{\longrightarrow} \tau_{i+1}$.

Since τ_i satisfies (A1), we know that $\widehat{f_k} \nmid \tau_i$ for $k = 1, \ldots, \mu$.

Thus $\ell > \mu$, so $\tau_{i+1} \neq 0$.

Let $k \in \{1, \ldots, \mu\}$ be arbitrary, but fixed.

Again, τ_i satisfies (A1), so $\exists \lambda_k$ such that

$$\deg_{x_{\lambda_k}} f_k > \deg_{x_{\lambda_k}} \tau_i$$

Then

$$\begin{aligned} \deg_{x_{\lambda_k}} \tau_{i+1} &= \deg_{x_{\lambda_k}} \left(\frac{\tau_i}{t_\ell} \cdot u_\ell \right) \\ &\leq \deg_{x_{\lambda_k}} \left(\frac{\tau_i}{t_\ell} \cdot t_\ell \right) \\ &= \deg_{x_{\lambda_k}} \tau_i \end{aligned}$$

Hence

$$\deg_{x_{\lambda_k}} f_k > \deg_{x_{\lambda_k}} \tau_{i+1}$$

Since k was arbitrary, τ_{i+1} and $f_1, \ldots, f_M$ satisfy (A).

Thus every monomial τ_i in the reduction path is nonzero; in particular, $\tau_r \neq 0$ and $\tau \overset{*}{\underset{F}{\twoheadrightarrow}} 0$. $\square$

The second lemma will also be useful for constructing a counterexample in lemma 6.9.

LEMMA 6.6. *The following are equivalent for all terms* t_1, t_2, t_3*:*

(A) $\gcd(t_1, t_3) \mid t_2$

(B) $\gcd(t_1, t_3) \mid \gcd(t_1, t_2)$

(C) $\gcd(t_1, t_3) \mid \gcd(t_2, t_3)$

PROOF. Let t_1, t_2, t_3 be arbitrary, but fixed.

(A)⇒(B): Assume $\gcd(t_1, t_3) \mid t_2$. Equivalently,

$$\forall x \quad \min(\deg_x t_1, \deg_x t_3) \leq \deg_x t_2.$$

If $\deg_x t_1 > \deg_x t_2$, then $\deg_x t_3 \leq \deg_x t_2$; hence $\gcd(t_1, t_3) \mid \gcd(t_1, t_2)$.

(A)⇐(B): Assume $\gcd(t_1, t_3) \mid \gcd(t_1, t_2)$. Equivalently,

$$\forall x \quad \min(\deg_x t_1, \deg_x t_3) \leq \min(\deg_x t_1, \deg_x t_2).$$

If $\deg_x t_1 > \deg_x t_2$, then $\deg_x t_3 \leq \deg_x t_2$. Thus $\gcd(t_1, t_3) \mid t_2$.

(A)⇒(C) is symmetric to (A)⇒(B), exchanging t_1 and t_3.

(A)⇐(C) is symmetric to (A)⇐(B), exchanging t_1 and t_3. □

REMARK 6.7. For any term ordering $\succ$ and for any two polynomials f_i, f_j, if $g \mid f_i$ and $g \mid f_j$, it follows from lemma 1.13 on page 15 that $\overline{g} \mid \overline{f_i}$ and $\overline{g} \mid \overline{f_j}$. So if $\overline{f_i}$ and $\overline{f_j}$ are relatively prime, f_i and f_j have no nontrivial common factors.

6.2.2. NECESSITY OF THE CRITERION. In this section, we show that we can skip the reduction of $S_{1,3}$ only if clause (B) of theorem 6.3 holds true. We do this by showing the contrapositive: if (B) is false, we produce an $F = (f_1, f_2, f_3)$ that violates (A): the leading terms of F are t_1, t_2, t_3, and F has the property that $S_{1,2} \xrightarrow[F]{*} 0$ and $S_{2,3} \xrightarrow[F]{*} 0$, but $S_{1,3} \overset{*}{\not\to}_F 0$.

We consider two different cases: one if (B1) is false (lemma 6.8); the other, if (B2) is false (lemma 6.9).

For the counterexamples, we use a form suggested by lemma 6.5 on page 128: $f_1 = t_1 + u$, $f_2 = t_2$, and $f_3 = t_3$. The question is: how do we structure u?

When (B1) is false, we will arrange for $S_{1,2} \xrightarrow[f_2]{} 0$. We know that

$$\begin{aligned} S_{1,2} &= \frac{\operatorname{lcm}(t_1, t_2)}{t_1} \cdot (t_1 + u) - \frac{\operatorname{lcm}(t_1, t_2)}{t_2} \cdot t_2 \\ &= \frac{\operatorname{lcm}(t_1, t_2)}{t_1} \cdot u \\ &= \frac{t_2}{\gcd(t_1, t_2)} \cdot u \end{aligned}$$

The simplest way to get $S_{1,2} \xrightarrow[f_2]{} 0$ is if $u = \gcd(t_1, t_2)$. That $S_{2,3} \xrightarrow[F]{*} 0$ is trivial.

How then will we ensure that $S_{1,3} \overset{*}{\not\to}_F 0$? This will depend on some "magical properties" of u. These properties exploit the facts that $t_2 \nmid \operatorname{lcm}(t_1, t_3)$ *and* $\gcd(t_1, t_3) \nmid t_2$ (hence $\gcd(t_1, t_3) \nmid \gcd(t_1, t_2)$ by lemma 6.6 on the preceding page).

LEMMA 6.8. *For all terms t_1, t_2, t_3 (A)⇒(B) where*

$$\text{(A)} \left[S_{1,2} \xrightarrow[F]{*} 0 \ \wedge \ S_{2,3} \xrightarrow[F]{*} 0 \right] \ \Rightarrow \ S_{1,3} \xrightarrow[F]{*} 0 \qquad \forall F = (f_1, f_2, f_3) : \forall k \ \overline{f_k} = t_k$$

(B) $\gcd(t_1, t_3) \mid t_2$ *or* $\mathrm{BC2}(t_1, t_2, t_3)$

In the proof of lemma 6.8, we do not need the general machinery of lemma 6.5, so we use the simpler form of lemma 3.2 on page 83.

PROOF. We show (A)⇒(B) by proving its contrapositive.

Assume ¬(B): $\gcd(t_1, t_3) \nmid t_2$ and $\neg\mathrm{BC2}(t_1, t_2, t_3)$. We construct F to show ¬(A): let $F = (f_1, f_2, f_3)$ be such that

$$f_1 = t_1 + \gcd(t_1, t_2)$$

$$f_2 = t_2$$

$$f_3 = t_3$$

We need to show that f_1 is a binomial, and $\widehat{f_1} = t_1$.

Since $\gcd(t_1, t_2) \mid t_1$, we have $\gcd(t_1, t_2) \preceq t_1$.

It remains to show that $\gcd(t_1, t_2) \neq t_1$. By way of contradiction:

$\gcd(t_1, t_2) = t_1 \quad \Rightarrow \quad t_1 \mid t_2 \quad \Rightarrow \quad \gcd(t_1, t_3) \mid t_2$

But ¬(A) has $\gcd(t_1, t_3) \nmid t_2$.

So $\gcd(t_1, t_2) \neq t_1$.

Hence $\gcd(t_1, t_2) \prec t_1$.

Hence f_1 is a binomial, and $\widehat{f_1} = t_1$.

We claim $S_{1,2} \xrightarrow[F]{*} 0$ and $S_{2,3} \xrightarrow[F]{*} 0$ but $S_{1,3} \overset{*}{\underset{F}{\not\to}} 0$.

From the construction of F

$$S_{2,3} = 0$$

Also

$$\begin{aligned} S_{1,2} &= \frac{\operatorname{lcm}(t_1, t_2)}{t_1} \cdot (t_1 + u) - \frac{\operatorname{lcm}(t_1, t_2)}{t_2} \cdot t_2 \\ &= \frac{t_2}{\gcd(t_1, t_2)} \cdot \gcd(t_1, t_2) \\ &= f_2 \end{aligned}$$

So $S_{1,2} \xrightarrow[F]{*} 0$ and $S_{2,3} \xrightarrow[F]{*} 0$.

Consider

$$\begin{aligned} S_{1,3} &= \frac{\operatorname{lcm}(t_1, t_3)}{t_1} \cdot (t_1 + u) - \frac{\operatorname{lcm}(t_1, t_3)}{t_3} \cdot t_3 \\ &= \frac{t_3}{\gcd(t_1, t_3)} \cdot u \end{aligned}$$

We claim that $t_2 \nmid S_{1,3}$.

Assume by way of contradiction that $t_2 \mid S_{13}$.

Then

$$t_2 \mid \frac{t_3}{\gcd(t_1, t_3)} \cdot \gcd(t_1, t_2)$$

This implies that

$$t_2 \mid \frac{t_3}{\gcd(t_1, t_3)} \cdot t_1$$

Then $t_2 \mid \operatorname{lcm}(t_1, t_3)$.

This contradicts $t_2 \nmid \operatorname{lcm}(t_1, t_3)$.

Hence $t_2 \nmid S_{1,3}$.

We further claim that $t_3 \nmid S_{1,3}$.

Assume by way of contradiction that $t_3 \mid S_{1,3}$.

Then $\gcd(t_1, t_3) \mid u$.

Since $u = \gcd(t_1, t_2)$, we have $\gcd(t_1, t_3) \mid \gcd(t_1, t_2)$.

By lemma 6.6 on page 130, $\gcd(t_1, t_3) \mid t_2$.

This contradicts $\gcd(t_1, t_3) \nmid t_2$.

Hence $t_3 \nmid S_{1,3}$.

By lemma 3.2, $S_{1,3} \overset{*}{\underset{F}{\not\to}} 0$. (Use the permutation $(1\ 3\ 2)$ with $\mu = 1$.) □

For clause (B2) in theorem 6.3, we employ a similar approach. As before, we build $F = (f_1, f_2, f_3)$ "as simple as possible": f_2 and f_3 will be monomials, and $f_1 = t_1 + u$ where u will have the "magical properties" that $S_{1,2} \underset{F}{\longrightarrow} 0$ but $S_{1,3} \overset{*}{\underset{F}{\not\to}} 0$. We find the "magical properties" by exploiting the failure of the criterion: in this case, the existence of an indeterminate $y \in \{x_1, \ldots, x_m\}$ such that $\neg \mathrm{VB1}_y(t_1, t_3)$ and $\neg \mathrm{VB2}_y(t_1, t_2, t_3)$. More precisely, we exploit $\deg_y \sigma_{12} > \deg_y \sigma_{13}$: a sufficiently small choice for $\deg_y u$ gives $S_{1,2} \overset{*}{\underset{f_3}{\longrightarrow}} 0$ while $S_{1,3} \overset{*}{\underset{F}{\not\to}} 0$, since

$$\deg_y S_{1,2} = \deg_y(\sigma_{12} u) > \deg_y(\sigma_{13} u) = \deg_y S_{1,3}$$

In this proof, we use the full generality of lemma 6.5 on page 128.

LEMMA 6.9. *For all terms t_1, t_2, t_3, (A)⇒(B) where*

(A) $\left[S_{1,2} \xrightarrow[F]{*} 0 \quad \wedge \quad S_{2,3} \xrightarrow[F]{*} 0\right] \quad \Rightarrow \quad S_{1,3} \xrightarrow[F]{*} 0 \, \forall F = (f_1, f_2, f_3) : \forall k \ \overline{f_k} = t_k$

(B) $\mathrm{VB1}_x\,(t_1, t_3)$ *or* $\mathrm{VB2}_x\,(t_1, t_2, t_3) \quad \forall x \in \{x_1, \ldots, x_n\}$

PROOF. We show (A)⇒(B) by proving its contrapositive.

Assume ¬(B); then $\exists y \in \{x_1, \ldots, x_n\}$ such that

$$\neg\mathrm{VB1}_y\,(t_1, t_3) \quad \text{and} \quad \neg\mathrm{VB2}_y\,(t_1, t_2, t_3)$$

Equivalently, $\exists y$ such that

$$0 < \deg_y t_1, \deg_y t_3 < \deg_y t_2$$

We need to find F such that $S_{1,2} \xrightarrow[F]{*} 0$ and $S_{2,3} \xrightarrow[F]{*} 0$ but $S_{1,3} \overset{*}{\nrightarrow}_F 0$.

Without loss of generality, we may assume $\deg_y t_1 \leq \deg_y t_3$. If not, swap t_1 and t_3 for the remainder of the proof.

Case 1: $t_1 \succeq t_3$

Define u as

$$\forall x \in \{x_1, \ldots, x_n\} \quad \deg_x u = \begin{cases} \deg_x t_3 & x \neq y \\ \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) & x = y \end{cases}$$

Let $F = (f_1, f_2, f_3)$ be such that

$$f_1 = t_1 + u$$

$$f_2 = t_2$$

$$f_3 = t_3$$

Note that $u \mid t_3$ and $u \neq t_3$; hence $u \prec t_3 \preceq t_1$. Hence f_1 is a binomial with $\overline{f_1} = t_1$.

We claim that $S_{1,2} \xrightarrow[F]{*} 0$ and $S_{2,3} \xrightarrow[F]{*} 0$ but $S_{1,3} \overset{*}{\underset{F}{\not\to}} 0$.

Immediately we have $S_{2,3} = 0$, so $S_{2,3} \xrightarrow[(f_1,f_2,f_3)]{*} 0$ trivially.

Next,

$$\begin{aligned} S_{1,2} &= \frac{\operatorname{lcm}(t_1,t_2)}{t_1} \cdot (t_1 + u) - \frac{\operatorname{lcm}(t_1,t_2)}{t_2} \cdot t_2 \\ &= \operatorname{lcm}(t_1,t_2) + \frac{\operatorname{lcm}(t_1,t_2)}{t_1} \cdot u - \operatorname{lcm}(t_1,t_2) \\ &= \frac{\operatorname{lcm}(t_1,t_2)}{t_1} \cdot u \end{aligned}$$

We see that for $x \neq y$

$$\begin{aligned} \deg_x S_{1,2} &= \max(\deg_x t_1, \deg_x t_2) - \deg_x t_1 + \deg_x u \\ &\geq \deg_x u \\ &= \deg_x t_3 \end{aligned}$$

whereas

$$\deg_y S_{1,2} = \max\left(\deg_y t_1, \deg_y t_2\right) - \deg_y t_1 + \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right)$$

Recall $\deg_y t_2 > \deg_y t_1$. Then

$$\begin{aligned} \deg_y S_{1,2} &= \deg_y t_2 - \deg_y t_1 + \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) \\ &= \max\left(\deg_y t_2 - \deg_y t_1, \deg_y t_3\right) \end{aligned}$$

$$\geq \deg_y t_3$$

So $S_{1,2} \xrightarrow[f_3]{*} 0$, as desired.

Now we turn to $S_{1,3}$. By reasoning similar to that for $S_{1,2}$, we have

$$S_{1,3} = \frac{\operatorname{lcm}(t_1, t_3)}{t_1} \cdot u$$

We claim $\deg_y S_{1,3} < \deg_y t_3 < \deg_y t_2$.

We have

$$\deg_y S_{1,3} = \max\left(\deg_y t_1, \deg_y t_3\right) - \deg_y t_1 + \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right)$$

Recall $\deg_y t_1 \leq \deg_y t_3$.

Then

$$\begin{aligned}\deg_y S_{1,3} &= \deg_y t_3 - \deg_y t_1 + \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) \\ &= \max\left(\deg_y t_3 - \deg_y t_1, 2\deg_y t_3 - \deg_y t_2\right)\end{aligned}$$

Recall $\deg_y t_3 < \deg_y t_2$ and $0 < \deg_y t_1$.

Then

$$\deg_y S_{1,3} < \deg_y t_3 < \deg_y t_2$$

Recall $\deg_y t_1 \geq \deg_y t_3 > \deg_y u$.

By lemma 6.5, $S_{1,3} \xrightarrow[F]{*} 0$.

Case 2: $t_1 \prec t_3$

We sketch the proof; it is similar to that for case 1.

Recall $\deg_y t_2 > \max\left(\deg_y t_1, \deg_y t_3\right)$. Let $F = (f_1, f_2, f_3)$ be such that

$$f_1 = t_1$$

$$f_2 = t_2$$

$$f_3 = t_3 + v$$

where v is defined as

$$\forall x \in \{x_1, \ldots, x_n\} \quad \deg_x v = \begin{cases} \deg_x t_1 & x \neq y \\ \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) & x = y \end{cases}$$

We see that $v \mid t_1$ and $v \neq t_1$, so $v \prec t_1 \prec t_3$. Hence $\widehat{f_3} = t_3$.

Again, we claim $S_{1,2} \xrightarrow[F]{*} 0$, $S_{2,3} \xrightarrow[F]{*} 0$, but $S_{1,3} \overset{*}{\underset{F}{\not\to}} 0$.

We have $S_{1,2} \xrightarrow[F]{*} 0$ trivially.

As for $S_{2,3}$:

$$S_{2,3} = -\frac{\operatorname{lcm}(t_2, t_3)}{t_3} \cdot v$$

Inspection shows $S_{2,3} \xrightarrow[f_1]{*} 0$.

We turn to $S_{1,3}$. We have

$$\begin{aligned} \deg_y S_{1,3} &= \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) \\ &< \deg_y t_1 \\ &< \deg_y t_2 \end{aligned}$$

As in case 1, $\deg_y t_3 > \deg_y u$ and by lemma 6.5, $S_{1,3} \overset{*}{\underset{F}{\not\to}}$. □

In lemmas 6.8 and 6.9, we have proven the following *strict boundary* on triplets of terms that guarantee $S_{13} \rightsquigarrow 0$.

COROLLARY 6.10. *For all terms t_1, t_2, t_3 (A)⇒(B) where*

(A) $\left[S_{12} \xrightarrow[F]{*} 0 \ \wedge \ S_{23} \xrightarrow[F]{*} 0\right] \ \Rightarrow S_{13} \xrightarrow[F]{*} 0 \quad \forall F = (f_1, f_2, f_3) : \forall k \ \overline{f_k} = t_k$

(B) clause (B) of theorem 6.3

6.2.3. SUFFICIENCY OF THE CRITERION. We turn our attention to proving that the new combinatorial criterion of theorem 6.3 eliminates the need to check the reduction of an *S*-polynomial. This is the more complicated part of the proof of theorem 6.3; the reader may wish to review figure 6.1 on page 127.

We need the following observation. Note the subtle difference between remark 6.11, which is true only if $\gcd(t_1, t_3) \mid t_2$, and remark 1.35 on page 49, which is true in all cases.

LEMMA 6.11. *If* $\gcd(t_1, t_3) \mid t_2$, *then* $\gcd(\overline{\sigma_{21}}, \overline{\sigma_{23}}) = 1$ *for all* $\overline{f_k} = t_k$.

PROOF. Let t_1, t_2, t_3 be arbitrary, but fixed. Assume $\gcd(t_1, t_3) \mid t_2$. Then $\forall x$

$$\min(\deg_x t_1, \deg_x t_3) \leq \deg_x t_2$$

Assume $\exists y$ such that $y \mid \overline{\sigma_{23}}$. We have

$$\begin{aligned} \deg_y \overline{\sigma_{23}} &= \deg_y \frac{\operatorname{lcm}\left(\overline{f_2}, \overline{f_3}\right)}{\overline{f_2}} \\ &= \max\left(\deg_y t_2, \deg_y t_3\right) - \deg_y t_2 \end{aligned}$$

$$= \max\left(0, \deg_y t_3 - \deg_y t_2\right)$$

Since $y \mid \overline{\sigma_{23}}$, $\deg_y t_3 > \deg_y t_2$.

Recall $\min\left(\deg_y t_1, \deg_y t_3\right) \leq \deg_y t_2$; with the above, this implies $\deg_y t_1 \leq \deg_y t_2$. Hence

$$\deg_y \overline{\sigma_{21}} = \deg_y \frac{\operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right)}{\overline{f_2}} = \max\left(\deg_y t_1, \deg_y t_2\right) - \deg_y t_2 = 0 \qquad \square$$

We come to the meat of the proof. We proceed by factoring the common divisor of f_1, f_3. Lemma 6.12 shows that when the new criterion is satisfied *and* the two "chain" S-polynomials reduce, we have a surprising result: $\gcd(f_1, f_3) \mid f_2$.

LEMMA 6.12. *(A)⇐(B) where*

(A) $S_{1,2} \xrightarrow[F]{*} 0$ *and* $S_{2,3} \xrightarrow[F]{*} 0$ *implies* $g_{13} \mid f_2$ *where* $g_{13} = \gcd(f_1, f_3)$,

(B) $\gcd\left(\overline{f_1}, \overline{f_3}\right) \mid \overline{f_2}$

PROOF. Assume (B). Then $\gcd\left(\overline{f_1}, \overline{f_3}\right) \mid \overline{f_2}$.

Assume $S_{1,2} \xrightarrow[F]{*} 0$ and $S_{2,3} \xrightarrow[F]{*} 0$. We need to show $g_{13} \mid f_2$.

Apply $S_{1,2} \xrightarrow[F]{*} 0$ and lemma 1.28 on page 30 to obtain a representation h_1, h_2, h_3 of $S_{1,2}$. So

$$S_{1,2} = h_1 f_1 + h_2 f_2 + h_3 f_3 \tag{6.2}$$

and $\forall k = 1, 2, 3$, $h_k \neq 0$ implies $\overline{h_k f_k} \prec \operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right)$.

Likewise, from $S_{2,3} \xrightarrow[F]{*} 0$ obtain a representation H_1, H_2, H_3, so that

$$S_{2,3} = H_1 f_1 + H_2 f_2 + H_3 f_3 \tag{6.3}$$

and $\forall k = 1, 2, 3$, $H_k \neq 0$ implies $\overline{H_k f_k} \prec \operatorname{lcm}\left(\overline{f_2}, \overline{f_3}\right)$.

Consider (6.2). We have

$$\begin{aligned} \sigma_{12} f_1 - \sigma_{21} f_2 &= h_1 f_1 + h_2 f_2 + h_3 f_3 \\ (\sigma_{12} - h_1) f_1 - h_3 f_3 &= (\sigma_{21} + h_2) f_2 \end{aligned} \tag{6.4}$$

Likewise (6.3) gives us

$$H_1 f_1 + (\sigma_{32} + H_3) f_3 = (\sigma_{23} - H_2) f_2 \tag{6.5}$$

Let $g_{13} = \gcd(f_1, f_3)$.

Let c_1, c_3 be such that $f_1 = c_1 g_{13}$ and $f_3 = c_3 g_{13}$.

From (6.4), we have

$$g_{13}\left[(\sigma_{12} - h_1) c_1 - h_3 c_3\right] = (\sigma_{21} + h_2) f_2 \tag{6.6}$$

From (6.5), we have

$$g_{13}\left[H_1 c_1 + (\sigma_{32} - H_3) c_3\right] = (\sigma_{23} - H_2) f_2 \tag{6.7}$$

Note $g_{13} \mid (\sigma_{21} + h_2) f_2$ and $g_{13} \mid (\sigma_{23} - H_2) f_2$.

So g_{13} divides the greatest common divisor of $(\sigma_{21} + h_2) f_2$ and $(\sigma_{23} - H_2) f_2$.

Using lemma 1.36 on page 50,

$$\widehat{\sigma_{21} + h_2} = \sigma_{21}$$

and

$$\widehat{\sigma_{23} - H_2} = \sigma_{23}$$

From lemma 6.11, we know $\gcd(\overline{\sigma_{21}}, \overline{\sigma_{23}}) = 1$.

By remark 6.7 on page 130 , $\sigma_{21} + h_2$ and $\sigma_{23} + H_2$ are relatively prime.

Thus f_2 is the greatest common divisor of the right-hand side for both (6.6) and (6.7), and we have $g_{13} \mid f_2$. □

We use lemma 6.13 on the *cofactors* of the greatest common divisor of f_1, f_2, f_3 in lemma 6.14. Note that here we work with representation instead of reduction, for two reasons: (a) I have no idea how to prove this using reduction, and it may not be true; further, (b) reduction implies representation (lemma 1.28 on page 30), while the converse does not hold in general (example 1.29 on page 31).

LEMMA 6.13. *For all t_1, t_2, t_3 (A)⇐(B) where*

(A) $\forall F = (f_1, f_2, f_3)$ such that $\overline{f_k} = t_k$ and $\gcd(f_1, f_3) = 1$,

if $S_{1,2}$ and $S_{2,3}$ have representations modulo f_1, f_2, f_3

then

$$\gcd(t_1, t_3) = 1$$

(B) $\gcd(t_1, t_3) \mid t_2$ and $[\mathrm{VB1}_x(t_1, t_3)$ or $\mathrm{VB2}_x(t_1, t_2, t_3)] \; \forall x \in \{x_1, \ldots, x_n\}$

PROOF. Assume (B).

Let F be arbitrary but fixed.

Assume $S_{1,2}$ and $S_{2,3}$ have representations modulo f_1, f_2, f_3. Choose h_1, h_2, h_3 such that

$$S_{1,2} = h_1 f_1 + h_2 f_2 + h_3 f_3 \quad \text{and} \quad \forall k \; h_k \neq 0 \Rightarrow \overline{h_k} \cdot \overline{f_k} \prec \operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right) \tag{6.8}$$

and H_1, H_2, H_3 such that

$$S_{2,3} = H_1 f_1 + H_2 f_2 + H_3 f_3 \quad \text{and} \quad \forall k \; H_k \neq 0 \Rightarrow \overline{H_k} \cdot \overline{f_k} \prec \operatorname{lcm}\left(\overline{f_2}, \overline{f_3}\right) \tag{6.9}$$

From (6.8),

$$\sigma_{12} f_1 - \sigma_{21} f_2 = h_1 f_1 + h_2 f_2 + h_3 f_3$$

$$(\sigma_{12} - h_1) f_1 - h_3 f_3 = (\sigma_{21} + h_2) f_2$$

$$\frac{(\sigma_{12} - h_1) f_1 - h_3 f_3}{\sigma_{21} + h_2} = f_2 \tag{6.10}$$

Likewise from (6.9),

$$\frac{H_1 f_1 + (\sigma_{32} + H_3) f_3}{\sigma_{23} - H_2} = f_2 \tag{6.11}$$

From (6.10) and (6.11),

$$\frac{(\sigma_{12} - h_1) f_1 - h_3 f_3}{\sigma_{21} + h_2} = \frac{H_1 f_1 + (\sigma_{32} + H_3) f_3}{\sigma_{23} - H_2}$$

$$(\sigma_{23} - H_2)\left[(\sigma_{12} - h_1) f_1 - h_3 f_3\right] = (\sigma_{21} + h_2)\left[H_1 f_1 + (\sigma_{32} + H_3) f_3\right]$$

Collect expressions with f_1 and f_3 on opposite sides:

(6.12)

$$\left[\left(\sigma_{23}-H_2\right)\left(\sigma_{12}-h_1\right)-H_1\left(\sigma_{21}+h_2\right)\right]f_1=\left[h_3\left(\sigma_{23}-H_2\right)+\left(\sigma_{21}+h_2\right)\left(\sigma_{32}+H_3\right)\right]f_3$$

Let

$$P=h_3\left(\sigma_{23}-H_2\right)+\left(\sigma_{21}+h_2\right)\left(\sigma_{32}+H_3\right)$$

Note that P is the cofactor of f_1 in (6.12).

We claim $\widehat{P}=\sigma_{21}\cdot\sigma_{32}$.

As per lemma 1.36,

- $\sigma_{23}\succ\widehat{H_2}$
- $\sigma_{21}\succ\widehat{h_2}$
- $\sigma_{32}\succ\widehat{H_3}$

So the only possible leading monomials of P are $\sigma_{21}\cdot\sigma_{32}$ and $\sigma_{23}\cdot\widehat{h_3}$.

Assume by way of contradiction that

$$\sigma_{23}\cdot\widehat{h_3}\succ\sigma_{21}\cdot\sigma_{32}$$

Then

$$\frac{\operatorname{lcm}\left(\overline{f_2},\overline{f_3}\right)}{\widehat{f_2}}\cdot\widehat{h_3}\quad\succ\quad\frac{\operatorname{lcm}\left(\overline{f_1},\overline{f_2}\right)}{\widehat{f_2}}\cdot\frac{\operatorname{lcm}\left(\overline{f_2},\overline{f_3}\right)}{\widehat{f_3}}$$

Canceling, we find that this implies

$$\widehat{h_3}\succ\frac{\operatorname{lcm}\left(\overline{f_1},\overline{f_2}\right)}{\widehat{f_3}}$$

$$\widehat{f_3} \cdot \widehat{h_3} \succ \operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right)$$

This clearly contradicts (6.8).

Hence $\widehat{P} = \sigma_{21} \cdot \sigma_{32}$.

Observe that f_1 divides the left-hand side of (6.12). So f_1 must also divide the right-hand side of (6.12).

Recall that f_1 and f_3 are relatively prime. Thus

$$f_1 \mid P$$

Then $\overline{f_1} \mid \overline{P}$. That is,

$$\begin{aligned}
t_1 &\mid \overline{\sigma_{21}} \cdot \overline{\sigma_{32}} \\
t_1 &\mid \frac{\operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right)}{\overline{f_2}} \cdot \frac{\operatorname{lcm}\left(\overline{f_2}, \overline{f_3}\right)}{\overline{f_3}} \\
t_1 &\mid \frac{\operatorname{lcm}(t_1, t_2)}{t_2} \cdot \frac{\operatorname{lcm}(t_2, t_3)}{t_3} \\
t_1 &\mid \frac{t_1 t_2}{\gcd(t_1, t_2) \cdot t_2} \cdot \frac{t_2 t_3}{\gcd(t_2, t_3) \cdot t_3}
\end{aligned}$$

$$\gcd(t_1, t_2) \cdot \gcd(t_2, t_3) \mid t_2 \tag{6.13}$$

We claim this proves $\gcd(t_1, t_3) = 1$. *Why?*

Let x be an arbitrary, but fixed indeterminate.

Recall from (B) that:

$\gcd(t_1, t_3) \mid t_2$, and

for all x $\mathrm{VB1}_x(t_1, t_3)$ or $\mathrm{VB2}_x(t_1, t_2, t_3)$.

It will suffice to show that $\mathrm{VB2}_x(t_1, t_2, t_3)$ and (6.13) imply $\mathrm{VB1}_x(t_1, t_3)$.

Assume $\mathrm{VB2}_x(t_1, t_2, t_3)$.

Suppose $\deg_x t_1 \leq \deg_x t_3$

From (B), $\deg_x t_1 \leq \deg_x t_2 \leq \deg_x t_3$.

From (6.13),

$$\deg_x t_1 + \deg_x t_2 \leq \deg_x t_2$$

So $\deg_x t_1 = 0$.

Hence $\mathrm{VB1}_x(t_1, t_3)$.

If instead $\deg_x t_1 > \deg_x t_3$, a similar argument gives $\mathrm{VB1}_x(t_1, t_3)$.

Hence $\mathrm{VB2}_x(t_1, t_2, t_3)$ and (6.13) imply $\mathrm{VB1}_x(t_1, t_3)$.

Since x was arbitrary, $\deg_x t_1 = 0$ or $\deg_x t_3 = 0$, for all indeterminates x.

Thus $\gcd(t_1, t_3) = 1$. □

Lemma 6.14 completes the proof of the main theorem, by showing that the new criterion suffices to skip the reduction of one S-polynomial. Because we switch between two sets of polynomials (f_k and c_k), we maintain the long notation for S-polynomials ($S_\succ(f_i, f_j)$ instead of $S_{i,j}$).

LEMMA 6.14. *For all terms t_1, t_2, t_3 (A)⇐(B) where*

(A) $\left[S_\succ(f_1, f_2) \xrightarrow[F]{*} 0 \text{ and } S_\succ(f_2, f_3) \xrightarrow[F]{*} 0\right] \quad \Rightarrow \quad S_\succ(f_1, f_3) \rightsquigarrow 0$

$\forall F = (f_1, f_2, f_3)$ *such that* $\overline{f_k} = t_k$.

(B) clause (B) of theorem 6.3.

PROOF. Assume (B). Thus we have (B1) and (B2) of theorem 6.3.

Let F be arbitrary, but fixed. Assume $S_{1,2} \xrightarrow[F]{*} 0$ and $S_{2,3} \xrightarrow[F]{*} 0$. We consider two cases.

Case 1: $\mathrm{BC2}\,(t_1, t_2, t_3)$

(A) follows from corollary 2.9 on page 69.

Case 2: $\neg\mathrm{BC2}\,(t_1, t_2, t_3)$

From (B), we have

$$\gcd\,(t_1, t_3) \mid t_2 \text{ and } [\mathrm{VB1}_x\,(t_1, t_3) \text{ or } \mathrm{VB2}_x\,(t_1, t_2, t_3)\ \forall x \in \{x_1, \ldots, x_n\}] \tag{6.14}$$

Let $g = \gcd\,(f_1, f_3)$. Let c_1, c_3 be such that $f_k = c_k g$. Then c_1 and c_3 are relatively prime.

Recall $S_\succ\,(f_1, f_2) \xrightarrow[F]{*} 0$ and $S_\succ\,(f_2, f_3) \xrightarrow[F]{*} 0$. From lemma 6.12, $g \mid f_2$.

Let c_2 be such that $f_2 = c_2 g$.

Since $t_k = \overline{f_k} = \overline{c_k g} = \overline{c_k} \cdot \overline{g}$, (6.14) implies

$$\gcd\,(\overline{c_1}, \overline{c_3}) \mid \overline{c_2} \ \wedge\ \forall x\,[\mathrm{VB1}_x\,(\overline{c_1}, \overline{c_3}) \ \vee\ \mathrm{VB2}_x\,(\overline{c_1}, \overline{c_2}, \overline{c_3})]$$

Recall again $S_\succ\,(f_1, f_3)$ and $S_\succ\,(f_2, f_3) \xrightarrow[F]{*} 0$. It follows from lemma 1.28 on page 30 that $S_\succ\,(f_1, f_2)$ and $S_\succ\,(f_2, f_3)$ have representations modulo F. By lemma 1.37 on page 51, we know that $S_\succ\,(c_1, c_2)$ and $S_\succ\,(c_2, c_3)$ have representations modulo c_1, c_2, c_3. By lemma 6.13, $\overline{c_1}$ and $\overline{c_3}$ are relatively prime.

Algorithm 6.1 `Can_Skip_Third_Spoly`

Inputs: t_1, t_2, t_3 which are terms in $x_1, \ldots, x_n$

Output: `YES` if clause (B) of theorem 6.3 is satisfied; `NO` otherwise

If $t_2 \nmid \operatorname{lcm}(t_1, t_3)$ **and** $\gcd(t_1, t_3) \nmid t_2$ **Then**

    Return `NO`

For $i = 1, \ldots, n$

    If $\deg_{x_i} t_2 > \max\left(\deg_{x_i} t_1, \deg_{x_i} t_3\right)$ **and** $\min\left(\deg_{x_i} t_1, \deg_{x_i} t_3\right) \neq 0$ **Then**

        Return `NO`

Return `YES`

Thus $\mathrm{BC1}\left(\overline{c_1}, \overline{c_3}\right)$. By theorem 2.4 on page 59, $S_{\succ}(c_1, c_3)$ has a representation modulo c_1, c_3. Re-applying lemma 1.37, we see that $S_{\succ}(f_1, f_3)$ has a representation modulo f_1, f_3.

Thus $S_{13} \rightsquigarrow 0$. □

6.3. APPLICATION OF RESULT

6.3.1. AN ALGORITHM FOR THEOREM 6.3. Algorithm 6.1 implements theorem 6.3.

The first conditional statement checks whether (B1) of theorem 6.3 is satisfied; the conditional statement within the loop checks whether (B2) of theorem 6.3 is satisfied.

To extend this algorithm into an algorithm that decides whether a system of polynomials are a Gröbner basis, we have to add the following capabilities which are not necessary for previous decision algorithms:

- Remember the representation of each $S_{i,j}$
- If `Can_Skip_Third_SPoly` returns `YES` for terms t_i, t_j, t_k, ensure that the representations of $S_{i,j}$ and $S_{j,k}$ are modulo f_i, f_j, f_k **only**

If $S_{i,j}$ or $S_{j,k}$ reduces only over f_i, f_j, f_k, then theorem 6.3 guarantees that we can skip $S_{i,k}$. Otherwise, we may not be able to skip $S_{i,k}$: see example 6.18 below.

6.3.2. EXAMPLES OF THEOREM 6.3. Our first example will answer the question, *Is theorem* 6.3 *merely a rearrangement of Buchberger's criteria, or does it contribute something new?*

The theorem does contribute something new. We illustrate this with two examples. The first comes from our discussion at the beginning of this chapter.

EXAMPLE 6.15. Let $t_1 = x_0x_1$, $t_2 = x_0x_2$, and $t_3 = x_0x_3$. Let $\succ$ be any term ordering whatsoever.

Observe that no arrangement of Buchberger's criteria allows us to skip an S-polynomial reduction:

- no pair t_i, t_j is relatively prime;
- no term t_k can serve as a bridge, because no permutation of the indices allows for $t_k \mid \operatorname{lcm}(t_i, t_j)$

On the other hand, t_1, t_2, t_3 *do* satisfy the combinatorial criterion of theorem 6.3. Why? Clause (B1) is satisfied by $\gcd(t_1, t_3) = x_0$, and $x_0 \mid t_2$. Clause (B2) is satisfied by

- $\mathrm{VB2}_{x_0}(t_1, t_2, t_3)$
- $\mathrm{VB1}_{x_k}(t_1, t_3)$ for $k = 1, 2, 3$

Thus, we have a set of terms so that Buchberger's criteria do not allow us to skip an S-polynomial reduction, but theorem 6.3 does. In other words, **theorem** 6.3 **provides a new combinatorial criterion for skipping S-polynomial reduction**.

What is this new criterion? If we assume that both of Buchberger's criteria fail, then to skip an S-polynomial reduction, we must retain the following:

$$\gcd(t_1, t_3) \mid t_2$$

and

$$\forall x \quad \mathrm{VB1}_x(t_1, t_3) \text{ or } \mathrm{VB2}_x(t_1, t_2, t_3)$$

The next two examples use the term diagrams of section 2.5 to give us two-dimensional and three-dimensional visualizations of what is new in the new criterion. In each case, we pose the question: *Given t_1 and t_3, what values of t_2 give $S_{1,3} \rightsquigarrow 0$, where the leading term of f_k is t_k?* The reader may want to take a moment to review term diagrams.

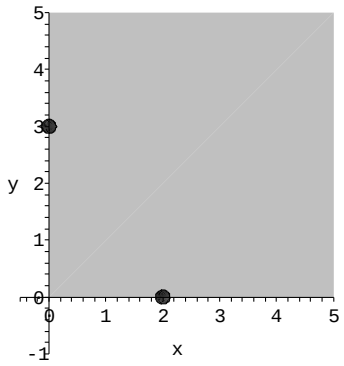
EXAMPLE 6.16. We first consider the question in the two-dimensional case: that is, when the leading terms are in two polynomials.

In the first case suppose t_1 and t_3 have no indeterminates in common; that is, they are relatively prime. This is Buchberger's first criterion, so we know *a priori* that $S_{1,3} \rightsquigarrow 0$. Thus t_2 can have any value we like; see figure 6.2, where we shade the entire x-y plane to represent this fact.

On the other hand, if t_1 and t_3 have *all* their indeterminates in common, then clause (B2) of theorem is true only if $\mathrm{VB2}_x\left(t_1, t_2, t_3\right)$ for every indeterminate x. This is Buchberger's second criterion; we illustrate this in figure 6.3 by shading only that rectangle of the x-y plane that divides $\mathrm{lcm}\left(t_1, t_3\right)$.

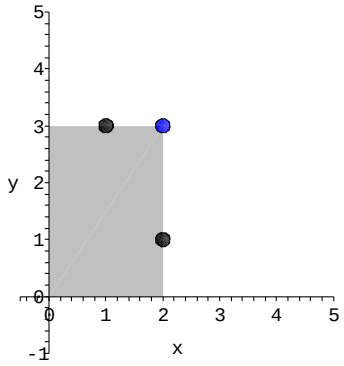
The natural question to ask is, *what if t_1 and t_3 share exactly one of their indeterminates?* In this case, neither of Buchberger's criteria applies, but the new criterion does. If the two terms share x (figure 6.4(a)), then any value of t_2 allows $S_{1,3} \rightsquigarrow 0$ so long as its degree in x is between the degree of the greatest common divisor and the least common multiple of t_1 and t_3. Since t_1 and t_3 do not share y, the degree in y of t_2 is unrestricted. A symmetric result occurs when t_1, t_3 share y, illustrated in figure 6.4(b). ◇

Observe that Buchberger's two criteria stand at opposite poles: at one, the entire quadrant is shaded, because any value of t_2 will allow $S_{1,3} \rightsquigarrow 0$; at the other, only a finite rectangle is shaded, because only the values of t_2 that divide $\mathrm{lcm}\left(t_1, t_3\right)$



Term t_2 can lie anywhere and $S_{1,3} \rightsquigarrow 0$.

Figure 6.2: Terms t_1 and t_3 have no indeterminates in common.

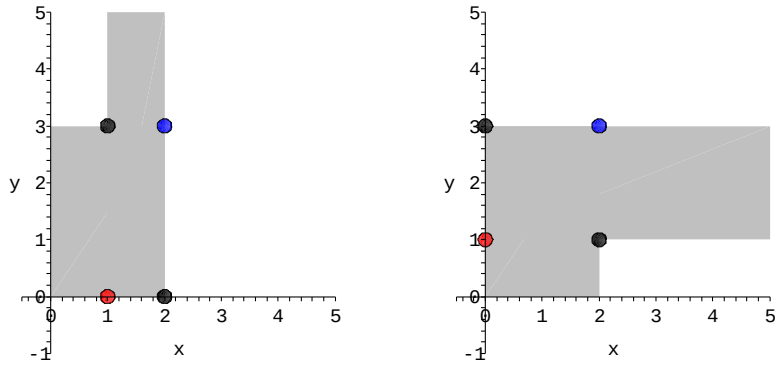


To guarantee $S_{1,3} \rightsquigarrow 0$, t_2 can only lie in that region of the plane that divides $\operatorname{lcm}(t_1, t_3)$ (marked in blue).

Figure 6.3: Terms t_1 and t_3 have all their indeterminates in common.

allow $S_{1,3} \rightsquigarrow 0$. Between these two extremes, we have the case where the new criterion applies, but neither of Buchberger's criteria apply: t_2 can lie anywhere in an infinite region of the plane, but this region does not cover the entire plane.

We can observe this in the three-dimensional case as well.



(a) t_1 and t_3 share x (b) t_1 and t_3 share y

To guarantee $S_{1,3} \rightsquigarrow 0$, t_2 can only lie in the shaded area of the x-y plane. The greatest common divisor is marked in red; the least common multiple in blue.

Figure 6.4: Terms t_1 and t_3 have one determinate in common.

EXAMPLE 6.17. We start with t_1, t_3 sharing all their indeterminates, then peel away one indeterminate after another until they are relatively prime. This adds one infinite region after another, until we have the entire positive orthant.

Begin with $t_1 = x^2y^4z^3$, $t_3 = x^5y^2z$. *What values of* t_2 *allow* $S_{1,3} \rightsquigarrow 0$? Since t_1, t_3 share all their variables, we can only satisfy theorem 6.3 if Buchberger's second criterion is satisfied. See figure 6.5(a).

Now consider $t_1 = x^2y^4z^3$, $t_3 = x^5z$. Here t_1, t_3 do not share y, so t_2 is free with respect to y; to satisfy theorem 6.3; the only constraints are on the degrees of x and z. See figure 6.5(b).

In the next step, consider $t_1 = y^4z^3$, $t_3 = x^5z$. In this case, t_1, t_3 only share z, so t_2 is free with respect to x and y; the only constraints are on the degree of z. See figure 6.5(c).

Finally, let $t_1 = y^4z^3$, $t_3 = x^5$. Now the two terms are relatively prime, so t_2 is free with respect to all indeterminates; we always have $S_{1,3} \rightsquigarrow 0$. We have arrived at the pole of Buchberger's first criterion; see figure 6.5(d). ◇

We close this section with an example that serves as a warning: the new criterion does *not* extend in an obvious way to $m > 3$ leading terms. This is more subtle than might first seem.

EXAMPLE 6.18. Let $F = (f_1, f_2, f_3, f_4)$ where

$$f_1 = x_0x_1 + x_2 \qquad f_2 = x_0x_2 \qquad f_3 = x_0x_3 \qquad f_4 = x_2^2$$

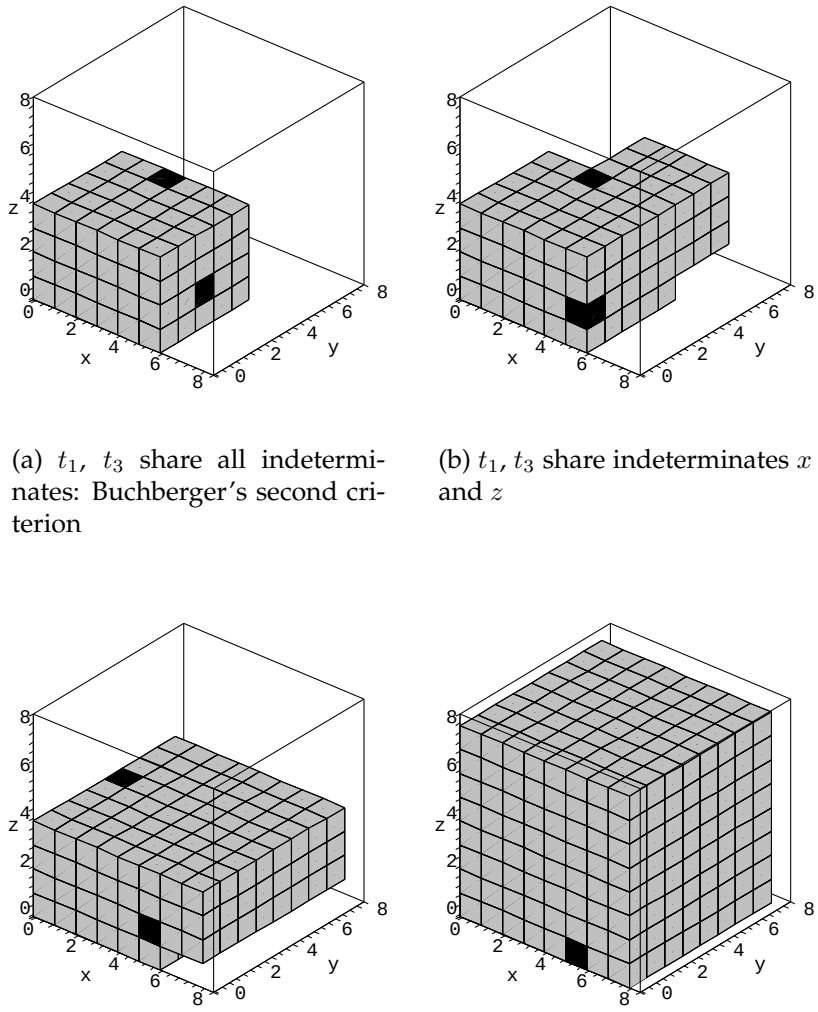
Let $\succ$ be any term ordering such that $\overline{f_1} = x_0x_1$; for example, a total-degree term ordering. Observe that $\overline{f_1}, \overline{f_2}, \overline{f_3}$ are the same as those of example 6.15; hence, they satisfy (B) of theorem 6.3. However,

$$S_{1,2} = x_2^2 \underset{F}{\longrightarrow} 0$$

$$S_{2,3} = 0$$

$$S_{1,3} = x_2x_3 \underset{F}{\nrightarrow}$$

◇



(a) t_1, t_3 share all indeterminates: Buchberger's second criterion

(b) t_1, t_3 share indeterminates x and z

(c) t_1, t_3 only share z

(d) t_1, t_3 share no indeterminates: Buchberger's first criterion

Figure 6.5: Theorem 6.3 allows a progression from Buchberger's second criterion to Buchberger's first criterion.

What is going on? Recall from definition 3.1 on page 80 that the inputs of CC are the terms $t_1, \ldots, t_m$, the term ordering $\succ$, and the set of paired indices $\mathcal{P}$ of

S-polynomials that are assumed to reduce to zero. The algorithm must decide

$$\left[\forall f_1, \ldots, f_m \text{ such that } \overline{f_k} = t_k \quad \forall\, (i,j) \in \mathcal{P}\ S_{i,j} \underset{(f_1,\ldots,f_m)}{\overset{*}{\longrightarrow}} 0\right]$$

$$\Downarrow$$

$$\mathrm{GB}_{\succ}\,(f_1, \ldots, f_m)$$

Clause (A) of theorem 6.3 gives the inputs t_1, t_2, t_3. This means that clause (B) is necessary and sufficient for (A) only if

$$S_{1,2} \underset{(f_1,f_2,f_3)}{\overset{*}{\longrightarrow}} 0 \quad \text{and} \quad S_{2,3} \underset{(f_1,f_2,f_3)}{\overset{*}{\longrightarrow}} 0$$

In other words, the S-polynomials must reduce *only* over the triplet f_1, f_2, f_3 for the new criterion to give us a valid skip. In example 6.18, the S-polynomial reduces over a fourth polynomial; hence CC *cannot* guarantee that $S_{1,3}$ will reduce to zero.

6.3.3. EXPERIMENTAL RESULTS. We ran experiments to answer two questions regarding these results:

- How often can we expect the new criterion to apply in real-life situations?
- How often do S-polynomials reduce over r polynomials?

It should be obvious why we would pose the first question: although the restriction on the number of polynomials means that the theorem is not "complete" enough to expect very many occasions when we can skip one S-polynomial reduction, we would still like an idea of how often the criterion might appear.

The second question also tries to see how often the new criterion could appear, but also whether further research would be useful. If we know how the majority of S-polynomials reduce to zero during a Gröbner basis computation, and over what number of polynomials they reduce to zero, this can help us design strategies for faster Gröbner basis computation.

HOW OFTEN CAN WE EXPECT THE NEW CRITERION TO APPLY IN "REAL-LIFE" SITUATIONS? In a first experiment suggested by Bruno Buchberger, we generated three random terms t_1, t_2, t_3, which we assumed to be the leading terms of unspecified polynomials f_1, f_2, f_3.

In a typical Buchberger algorithm for computing (or even deciding) Gröbner bases, the critical pairs are ordered in some manner. For example, if $t_1 = x^2y$, $t_2 = x^3$, and $t_3 = yz$, using $\succ = \text{lex}\,(x, y, z)$ we could order the critical pairs by increasing least common multiple. Since

$$\text{lcm}\,(t_2, t_3) \succ \text{lcm}\,(t_1, t_2) \succ \text{lcm}\,(t_1, t_3)$$

the algorithm would first reduce $S_{1,3}$, then $S_{1,2}$, and finally $S_{2,3}$.

After ordering the critical pairs, we assumed that the first two S-polynomials reduce to zero. At this point, we checked which combinatorial criteria applied to the leading terms. Since the terms that satisfy Buchberger's criteria are a subset of the terms that satisfy the new criterion, we checked them first. This gives us an

Table 6.1: Statistical analysis of new criterion on leading terms, assuming all S-polynomials reduce to zero.

# vars	BC applies	NC applies
3	53344 (17.8%)	7064 (2.4%)
4	42459 (14.2%)	6618 (2.2%)
5	34882 (11.6%)	5605 (1.9%)
6	28869 (9.6%)	4954 (1.7%)

(Total degree term ordering; critical pairs ordered from lower least common multiple to higher.)

Table 6.2: Statistical analysis of new criterion on leading terms, assuming all S-polynomials reduce to zero.

# vars	BC applies	NC applies
3	53301 (17.8%)	6894 (2.3%)
4	42506 (14.2%)	6743 (2.2%)
5	34795 (11.6%)	5735 (1.9%)
6	29076 (9.7%)	4850 (1.6%)

(Lexicographic term ordering; critical pairs ordered from lower least common multiple to higher.)

idea how often we can expect a triplet whose terms satisfy the new criterion and *not* the Buchberger criteria.

The results of this first experiment are listed in tables 6.1 and 6.2. We generated 100,000 sets of leading terms, whose indeterminates were randomly chosen and whose exponents were randomly generated from 0 to 10; this means that there were 300,000 critical pairs. We assume that the first two critical pairs reduce to zero, and test the third pair against the criteria; hence, we are testing 100,000 leading terms. We find that Buchberger's criteria apply fairly often; the new criterion

appears rarely. The choice of term ordering does not appear to have a significant effect on the results.

In another experiment suggested by Erich Kaltofen, we modified an algorithm that *computed* Gröbner bases and ran it on randomly-generated polynomials as well as some benchmark sets of polynomials. (See the footnote contrasting deciding a Gröbner basis and computing a Gröbner basis on page 23.) The benchmarks used were:

- Cyclic-3
- Cyclic-4
- Cyclic-5
- Katsura-5

The modifications were to keep detailed records of S-polynomial reduction. These records are necessary for the correct implementation of the new criterion (which requires that the S-polynomials reduce only over three polynomials). Both to encourage reduction to zero and to avoid expression swell and rational coefficients, we carried out these computations over a field of characteristic two.

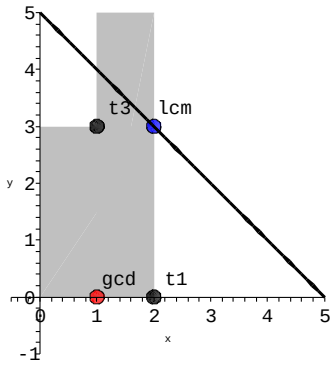
While Buchberger's criteria occurred very frequently in the computation of Gröbner bases for these benchmarks, the new criterion never appeared. In fact, Buchberger's criteria allow us to skip the majority of S-polynomial reductions.

Table 6.3: Number of skips during the computation of a Gröbner basis for three randomly-generated polynomials; total-degree term ordering.

	Buchberger skips	New skips	Reductions	Polys in GB
1	16	1 (empty)	11	8
3	22	0	14	9
5	113	0	77	20
6	13	0	23	9
8	244	1 (empty)	133	28
10	22	4 (empty)	29	11

For randomly-generated polynomials, the results were a little more "positive" (as in, non-zero). We give the results in table 6.3. Observe that with the exception of systems 6 and 10, Buchberger's criteria allow us to skip the majority of S-polynomial reductions. As for skips that are *genuinely new criteria*, we do see six total. However, they were all "empty" S-polynomials; that is, while the new criteria would allow us to skip an S-polynomial reduction, the corresponding polynomials were in fact monomials, so that no reduction would have taken place anyway. (We note that these polynomials were generated with at least 2, at most 5 variables; at least 2, at most 5 terms; exponents ranged from 0 to 10, with total degree 5; coefficients ranged from -99 to 99.)

WHY SO RARE? The results of tables 6.1, 6.2 and 6.3 seem counter-intuitive to the infinite regions of additional bridge terms afforded by the new criterion, as illustrated by figures 6.4 and 6.5. The question arises: why does the new criterion appear so rarely? We can think of three reasons.



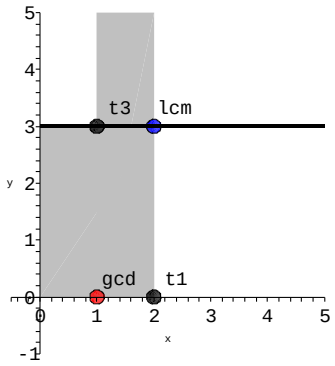
Nearly all bridge terms of the new criterion lie above the grading of total-degree term ordering; thus, nearly all bridge S-polynomials would be considered after $S_{1,3}$ when we order the critical pairs from smallest lcm to greatest.

Figure 6.6: Ordering of critical pairs excludes most occurrences of the new criterion.

First, the new criterion appears only when one of the leading terms lacks at least one indeterminate. We see this illustrated in the figures by the fact that the indeterminate lies against a "wall": an axis in figure 6.4, or a plane in figure 6.5. This is a special case; very rarely will randomly-generated terms fall into special cases.

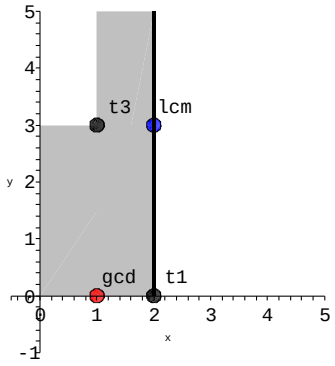
Second, we ordered the S-polynomials of $\mathcal{B}$ (the set of "critical pairs"; see algorithm 1.1) by increasing least common multiple. Look again at the terms illustrated in figures 6.4 and 6.5: in general, the vast majority of additional bridge terms t_2 afforded by the new criterion lie outside the grading of the least common multiple.

If we draw a line to show the gradings created by the term orderings, we have figures 6.6, 6.7, and 6.8. How does this affect the frequency of the new criterion? It



All bridge terms of the new criterion lie above the grading of this lexicographic term ordering ($x \succ y$); thus, bridge S-polynomials would be considered after $S_{1,3}$ when we order the critical pairs from smallest lcm to largest. In this case, the selection of bridge terms is reduced to Buchberger's second criterion.

Figure 6.7: Ordering of critical pairs excludes most occurrences of the new criterion.



"Most" bridge terms of the new criterion lie within the grading of this lexicographic term ordering ($y \succ x$); thus, bridge S-polynomials would be considered before $S_{1,3}$ when we order the critical pairs from smallest lcm to largest.

Figure 6.8: Ordering of critical pairs excludes most occurrences of the new criterion.

means that often we have a triplet that may satisfy the new criterion, but the algorithm will almost always evaluate $S_{1,3}$ *before* $S_{1,2}$ and $S_{2,3}$, the reverse of the order needed for the new criterion to apply!

To test this latter hypothesis, we ran an experiment to estimate the area of regions where one can find possible bridge terms. Increasing from two to six variables, we generated for each turn 1,000 random pairs of terms t_1, t_2. For each pair of terms, we first calculated the area of the region from which Buchberger's criteria would give us a bridge term; since this region is a hypercube, it is immediate to deduce the area from the exponents. Then we calculated the area of the region from which the new criterion would give us a bridge term. To avoid having to average the occasional "infinite" region, we restricted this region so that the maximum degree of a bridge term could be no larger than that of the two endpoints. This is a reasonable restriction, since the random terms we generated for tables were also restricted in their maximum degree. Then we removed from the region any bridge terms t_3 that were larger than $\mathrm{lcm}\,(t_1, t_2)$ with respect to the term ordering. To calculate the area, then, we simply counted the number of terms remaining in the set.

Tables 6.4 and 6.5 show the results. As we see, the area of the regions also suggest that the new criterion provides few additional possibilities for bridge terms. We would caution the reader agaisnt comparing the data too closely to those of tables 6.1 and 6.2; although we kept some conditions similar, we are comparing

Table 6.4: Comparison of areas of regions: Buchberger criteria vs. new criterion (total-degree ordering).

# vars	max degree	BC area	NC area
2	8	32.7%	2.9%
3	7	21.1%	3.6%
4	6	14.3%	3.0%
5	4	12.2%	3.6%
6	3	13.4%	3.7%

Table 6.5: Comparison of areas of regions: Buchberger criteria vs. new criterion (lexicographic ordering).

# vars	max degree	BC area	BC area
2	8	32.1%	4.8%
3	7	21.3%	4.5%
4	6	14.9%	4.1%
5	4	12.8%	3.6%
6	3	12.8%	3.6%

objects that are fundamentally different. What interests us is the fact that the new criterion appears rarely in comparison to Buchberger's criteria.

Finally, recall that the new criterion requires that the S-polynomials reduce only over the triplet f_1, f_2, f_3. (Otherwise, we might skip an S-polynomial that is not unnecessary, as we saw in example 6.18 on page 154.) In other words, the new criterion requires a Gröbner sub-basis. This phenomenon is, again, a "special case;" we would expect it to occur rarely.

HOW OFTEN DO S-POLYNOMIALS REDUCE OVER r POLYNOMIALS? By keeping track of the S-polynomial reductions, we were also able to record the data shown in tables 6.6, 6.7, and 6.8.

Table 6.6: Which $S_{i,j}$ used r polynomials to reduce to zero (system 1).

r	S-polynomials
0	$(1,7)\,,(1,8)\,,(4,6)\,,(5,7)\,,(5,8)\,,(7,8)$
1	$(1,2)\,,(1,3)\,,(1,4)\,,(1,6)\,,(2,5)\,,(2,7)\,,(2,8)\,,(3,5)\,,(3,7)\,,(3,8)\,,$
	$(4,5)\,,(4,7)\,,(4,8)\,,(5,6)\,,(6,7)\,,(6,8)$
2	$(1,5)\,,(2,3)\,,(2,4)\,,(2,6)\,,(3,4)\,,(3,6)$

Table 6.7: Which $S_{i,j}$ used r polynomials to reduce to zero (system 3).

r	S-polynomials
0	$(2,7)\,,(2,8)\,,(7,8)\,,$
1	$(1,2)\,,(1,3)\,,(1,6)\,,(1,7)\,,(1,8)\,,(2,3)\,,(2,5)\,,(2,6)\,,(2,9)\,,(3,8)\,,$
	$(3,9)\,,(4,5)\,,(4,7)\,,(4,8)\,,(5,7)\,,(5,8)\,,(6,7)\,,(6,8)\,,$
2	$(1,4)\,,(1,5)\,,(1,9)\,,(2,4)\,,(3,4)\,,(3,5)\,,(3,6)\,,(3,7)\,,(4,6)\,,(4,9)\,,$
	$(5,6)\,,(5,9)\,,$
3	$(6,9)\,,(7,9)\,,(8,9)$

Table 6.8: Which $S_{i,j}$ used r polynomials to reduce to zero (system 6).

r	S-polynomials
0	$(6,9)$
1	$(3,9)\,,(6,8)\,,(8,9)$
2	$(1,2)\,,(1,3)\,,(2,3)\,,(3,4)\,,(3,7)\,,(3,8)$
3	$(2,4)$
4	$(1,4)$
5	$(1,5)\,,(1,6)\,,(1,7)\,,(1,9)\,,(2,6)\,,(2,9)\,,(3,5)\,,(3,6)\,,(4,5)\,,(4,7)\,,(5,7)$
6	$(1,8)\,,(2,5)\,,(2,7)\,,(2,8)\,,(4,6)\,,(6,7)$
7	$(4,8)\,,(4,9)\,,(5,6)\,,(5,8)$
8	$(5,9)\,,(7,8)\,,(7,9)$

There does not appear to be any discernible pattern. In systems 1 and 3, the S-polynomials all reduce over a very small number of polynomials; in system 6, however, most of the S-polynomials reduce over 5 or more polynomials.

6.3.4. FINAL REMARK. The following "cute" fact provides an "alternate definition" of Buchberger's criteria:

LEMMA 6.19. *(A) and (B) where*

(A) $\forall x \ \mathrm{VB1}_{x_k}(t_1, t_3)$ *if and only if* $\mathrm{BC1}(t_1, t_3)$

(B) $\forall x \ \mathrm{VB2}_{x_k}(t_1, t_2, t_3)$ *if and only if* $\mathrm{BC2}(t_1, t_2, t_3)$

PROOF. Immediate from the definitions of the criteria. □

Part 3

A New Criterion for Gröbner Basis Detection of Two Polynomials

Chapter 7

Gröbner basis detection: introduction

7.1. Introduction to the problem

In previous chapters, we were given a term ordering $\succ$ and the leading terms of a set of polynomials with respect to $\succ$. We looked for criteria on the leading terms that would guarantee that the polynomials were a Gröbner basis with respect to $\succ$, so long as a certain number of S-polynomials reduced to zero.

Suppose instead that we only have a set of polynomials. Rather than picking a term ordering and deciding whether the polynomials were a Gröbner basis with respect to that term ordering, what if we searched for a term ordering that would guarantee the polynomials were already a Gröbner basis? We are asking for criteria that decide for given $f_1, \ldots, f_m$

$$\exists \succ \quad \mathrm{GB}_{\succ}(f_1, \ldots, f_m)$$

We illustrate the idea with example 7.1.

EXAMPLE 7.1. Let $f_1 = x + y$, $f_2 = y + 1$. We know from corollary 2.9 on page 69 that if their leading terms are

$$\overline{f_1} = x \qquad \overline{f_2} = y$$

then we can skip the reduction of their S-polynomial. Hence f_1, f_2 are a Gröbner basis with respect to $\succ = \text{lex}\,(x, y)$.

However, if $\succ = \text{lex}\,(y, x)$, we have

$$\overline{f_1} = y \qquad \overline{f_2} = y$$

Then

$$\begin{aligned} S_{1,2} &= \frac{\text{lcm}\,(y, y)}{y} \cdot (x + y) - \frac{\text{lcm}\,(y, y)}{y} \cdot (y + 1) \\ &= (x + y) - (y + 1) \\ &= x - 1 \end{aligned}$$

Observe that neither $\overline{f_1}$ nor $\overline{f_2}$ divides any term of $S_{1,2}$. Hence

$$S_{1,2} \underset{(f_1, f_2)}{\overset{*}{\nrightarrow}} 0$$

and f_1, f_2 are *not* a Gröbner basis with respect to $\succ = \text{lex}\,(x, y)$. ◇

We do not expect to encounter many sets of polynomials where there exists some term ordering such that the leading terms are all relatively prime. We shall see that we may be able to detect a Gröbner basis nevertheless.

Why would we want to do this? For many Gröbner basis applications, any term ordering will suffice: we don't care if we have a total-degree term ordering, a lexicographic term ordering, or some other term ordering altogether – all that matters is the existence of a Gröbner basis with respect to *some* term ordering. One example application would be the problem we used to introduce Gröbner bases: deciding the existence and cardinality of common roots.

On the other hand, if a specific term ordering is needed – as in the case of finding the common roots, where one typically uses a lexicographic ordering to compute a Gröbner basis – it may still be useful to try detecting a Gröbner basis beforehand. *Why?* To pursue the example: a lexicographic term ordering is generally agreed to give some of the least efficient performance from any algorithm used to compute Gröbner bases, while a total-degree term ordering is more efficient.[1] In most of the cutting-edge work done with Gröbner bases, one computes the Gröbner basis with respect to a "probably efficient" term ordering, then employs a second algorithm that converts to the desired term ordering. Such algorithms exist and are in use; see for example [**FGLM93**] and [**CKM97**]. Thus, if we can detect that a system of polynomials is already a Gröbner basis with respect to

[1]See the remark on page 109 of [**CLO97**], who reference [**BS87**]; see also [**CKM97**] and [**Tra05**].

some term ordering, we could use that as a starting point to convert to the desired term ordering.

A general solution for Gröbner basis detection already exists: Peter Gritzmann and Bernd Sturmfels give it in [**GS93**]; we discuss this solution in chapter 8.

If there is already a general solution, why pursue more research in this area? The general solution is not easily implemented. To our knowledge, there is no current implementation. Indeed, Bernd Sturmfels and Markus Wiegelman followed the first paper with a second that considered the special case of finding a term ordering where all the leading terms are relatively prime; see [**SW97**].

We stumbled on our solution by accident. While conducting the research that led to the results in chapter 6, we observed that Gröbner bases of two polynomials had a special form. This led to a theorem; in turn, this theorem suggested an algorithm for Gröbner basis detection that is easy to implement. How easy? The author implemented the algorithm in two days (see [**HP04**]), most of which he spent persuading Maple that it really could find solutions to *strict* inequalities. We demonstrated this implementation at the 2004 Applications of Computer Algebra conference at Lamar University in Beaumont, Texas.

7.2. MATRIX REPRESENTATIONS OF TERM ORDERINGS

Since "Gröbner basis detection" considers the question of whether a special term ordering exists, we need a way to solve for term orderings. For this, we

need a convenient algebraic representation of term orderings. A well-established technique allows us to represent any admissible term ordering as one of the most familiar of mathematical objects: a matrix.

To treat the theory in full detail is beyond the scope of this thesis; the interested reader should refer to **[Rob86]**, **[Wei87]**, and **[HW99]**. We give the results necessary to understand our results and those of **[GS93]**.

We adopt the following notational conventions:

- α, β represent column vectors;
- $\mathcal{M}, \mathcal{N}$ represent matrices;
- $\alpha_{(i)}$ represents row i of vector α, and $\mathcal{M}_{(i)}$ represents row i of vector $\mathcal{M}$.

7.2.1. ADMISSIBLE MATRICES.

DEFINITION 7.2. For vectors $\alpha, \beta \in \mathbb{R}^n$ we say $\alpha \gg \beta$ if

- $\alpha_{(1)} > \beta_{(1)}$, or
- $\alpha_{(1)} = \beta_{(1)}$ and $\alpha_{(2)} > \beta_{(2)}$, or
- $\ldots$
- $\alpha_{(1)} = \beta_{(1)}$ and $\ldots$ and $\alpha_{(n-1)} = \beta_{(n-1)}$ and $\alpha_{(n)} > \beta_{(n)}$.

We say that α, β are **exponent vectors** if $\alpha, \beta \in \mathbb{Q}^n$. A matrix $\mathcal{M} \in \mathbb{R}^{m \times n}$ is **admissible** if it has full rank over $\mathbb{Q}$ (that is, its column rank over $\mathbb{Q}$ equals n) *and* if $\mathcal{M} \cdot \alpha \gg 0$ for all nonzero vectors $\alpha \in \mathbb{Z}^n_{\geq 0}$.

EXAMPLE 7.3. Let

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathcal{N} = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

We claim that $\mathcal{M}$ is admissible, while $\mathcal{N}$ is not.

Proof that $\mathcal{M}$ is admissible: Since $\det \mathcal{M} \neq 0$, it has full rank. Let α be a nonzero vector in $\mathbb{Z}^3_{\geq 0}$; then

$$\mathcal{M} \cdot \alpha = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha_{(1)} \\ \alpha_{(2)} \\ \alpha_{(3)} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_{(1)} + \alpha_{(2)} + \alpha_{(3)} \\ \alpha_{(2)} + \alpha_{(3)} \\ \alpha_{(3)} \end{pmatrix}$$

Since $\alpha \in \mathbb{Z}^3_{\geq 0}$ and α is nonzero, $\alpha_{(1)}, \alpha_{(2)}, \alpha_{(3)} \geq 0$ and $\alpha_{(1)} + \alpha_{(2)} + \alpha_{(3)} > 0$. Hence $\mathcal{M} \cdot \alpha \gg 0$, as desired.

Proof that $\mathcal{N}$ is not admissible: Let $\alpha = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}^T$. Clearly $\alpha \in \mathbb{Z}^3_{\geq 0}$. However,

$$\mathcal{N} \cdot \alpha = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}$$

$$\ll 0$$

◇

Admissible matrices will prove useful because we can represent terms as exponent vectors with integer entries. For an admissible matrix $\mathcal{M}$, the product of $\mathcal{M}_{(i)}$ with an exponent vector α represents a **weight** w for α. The product of $\mathcal{M}$ with α is a vector of weights $w_1, \ldots, w_m \in \mathbb{R}$. Theorem 7.5 will use these weight vectors to show how $\mathcal{M}$ corresponds to a term ordering on the terms in $x_1, \ldots, x_n$.

DEFINITION 7.4. Let $\mathcal{M}$ be an admissible matrix, and $\succ$ be an admissible term ordering. We say that $\mathcal{M}$ is **an admissible matrix representation** of $\succ$ if for every pair of terms t, u, whose exponent vectors we denote as α, β,

$$t \succ u \quad \Leftrightarrow \quad \mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta$$

In general, we will say that $\mathcal{M}$ **is a representation of** $\succ$, or that $\mathcal{M}$ **induces** $\succ$, or that $\succ$ **induces** $\mathcal{M}$.

It turns out that every admissible matrix induces a term ordering, and vice-versa. This result is due to [**Rob86, Wei87, HW99**].

THEOREM 7.5. *(A) and (B) where*

(A) Every term ordering on terms in $x_1, \ldots, x_n$ is induced by an admissible matrix $\mathcal{M} \in \mathbb{R}^{m \times n}$.

(B) Every admissible matrix $\mathcal{M} \in \mathbb{R}^{m \times n}$ induces a term ordering on $\mathcal{T}(x_1, \ldots, x_n)$ (the set of terms in $x_1, \ldots, x_n$).

Before proving the theorem, we require some background material.

7.2.2. EXTENDING $\succ$ FROM $\mathcal{T}(x_1, \ldots, x_n)$ TO $\mathbb{Q}^n$. One thing we will need to do, is extend a term ordering from an ordering on terms to an ordering on $\mathbb{Q}^n$. How do we do this?[2]

Let $\succ$ be an admissible term ordering. We can extend $\succ$ to an ordering $\succ_{\mathbb{Z}^n_{\geq 0}}$ on $\mathbb{Z}^n_{\geq 0}$ directly: for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$

$$\alpha \succ_{\mathbb{Z}^n_{\geq 0}} \beta \qquad \Leftrightarrow \qquad x_1^{\alpha_{(1)}} \cdots x_n^{\alpha_{(n)}} \succ x_1^{\beta_{(1)}} \cdots x_n^{\beta_{(n)}}$$

Recall that, for terms, t, u, v, we know that

$$t \succ u \qquad \Leftrightarrow \qquad tv \succ uv$$

It follows that for all $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$

$$\alpha \succ_{\mathbb{Z}^n_{\geq 0}} \beta \qquad \Leftrightarrow \qquad \alpha + \gamma \succ_{\mathbb{Z}^n_{\geq 0}} \beta + \gamma \tag{7.1}$$

[2]The following argument appears in numerous sources before this one; for example, proposition 1.4.14 and exercise 8 in chapter 1, section 4 of [**KR00**].

Now that we have $\succ_{\mathbb{Z}^n_{\geq 0}}$, we can extend it immediately to an ordering on all of $\mathbb{Z}^n$. For $\gamma \in \mathbb{Z}^n$, find $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ such that $\gamma = \alpha - \beta$. Begin by defining

$$\gamma \succ_{\mathbb{Z}^n} 0 \qquad \Leftrightarrow \qquad \alpha \succ_{\mathbb{Z}^n_{\geq 0}} \beta$$

We have to check that the ordering is well defined here. Suppose $\gamma = \alpha - \beta = \zeta - \vartheta$ for $\gamma \in \mathbb{Z}^n$, $\alpha, \beta, \zeta, \vartheta \in \mathbb{Z}^n_{\geq 0}$. Assume that $\alpha \succ_{\mathbb{Z}^n_{\geq 0}} \beta$; by (7.1), $\alpha + \vartheta \succ_{\mathbb{Z}^n_{\geq 0}} \beta + \vartheta$. Since $\alpha = \beta + \zeta - \vartheta$,

$$\alpha + \vartheta \succ_{\mathbb{Z}^n_{\geq 0}} \beta + \vartheta$$

$$(\beta + \zeta - \vartheta) + \vartheta \succ_{\mathbb{Z}^n_{\geq 0}} \beta + \vartheta$$

$$\beta + \zeta \succ_{\mathbb{Z}^n_{\geq 0}} \beta + \vartheta$$

Again by (7.1), we have $\zeta \succ_{\mathbb{Z}^n_{\geq 0}} \vartheta$. Hence $\gamma \succ_{\mathbb{Z}^n_{\geq 0}} 0$ is well-defined. We complete the definition by

$$\gamma \succ_{\mathbb{Z}^n_{\geq 0}} \zeta \qquad \Leftrightarrow \qquad \gamma - \zeta \succ_{\mathbb{Z}^n_{\geq 0}} 0$$

How shall we extend the ordering to $\succ_{\mathbb{Q}^n}$? We teach grade-school students to compare rational numbers by finding a common denominator; the same technique extends naturally to $\mathbb{Q}^n$. Proceed in the following way: for $\alpha, \beta \in \mathbb{Q}^n$ in simplest form, let γ be the least common multiple of the denominators of $\alpha_{(1)}, \ldots, \alpha_{(n)}$, $\beta_{(1)}, \ldots, \beta_{(n)}$. Notice that γ is a natural number, and hence a scalar with respect to α, β. Then

$$\alpha \succ_{\mathbb{Q}^n} \beta \qquad \Leftrightarrow \qquad \gamma \cdot \alpha \succ_{\mathbb{Z}^n_{\geq 0}} \gamma \cdot \beta$$

The following example illustrates each of these techniques.

EXAMPLE 7.6. Let $\succ$ represent the lexicographic ordering on x_1, x_2 with $x_1 \succ x_2$.

Consider $\alpha = \begin{pmatrix} 1 & 3 \end{pmatrix}^T, \beta = \begin{pmatrix} 0 & 2 \end{pmatrix}^T$. Note that $\alpha, \beta \in \mathbb{Z}^2_{\geq 0}$. We have

$$x_1 x_2^3 \succ x_2^2 \qquad \Rightarrow \qquad \alpha \succ_{\mathbb{Z}^n_{\geq 0}} \beta$$

Thus

$$\alpha - \beta \succ_{\mathbb{Z}^n} 0$$

Continuing the extension,

$$\alpha - \beta \succ_{\mathbb{Z}^n} 0 \qquad \Rightarrow \qquad 0 \succ_{\mathbb{Z}^n} \beta - \alpha$$

(Put $0 = \gamma$, $\zeta = \beta - \alpha$ and use the definition for $\gamma \succ_{\mathbb{Z}^n} \zeta$.)

Let $\gamma = \begin{pmatrix} -1 & -1 \end{pmatrix}^T$. Note that $\gamma \in \mathbb{Z}^2$ and $\gamma = \beta - \alpha$. Hence $0 \succ_{\mathbb{Z}^n} \gamma$.

Finally, let $\zeta = \begin{pmatrix} 1 & -\frac{2}{3} \end{pmatrix}^T$ and $\vartheta = \begin{pmatrix} \frac{3}{4} & -2 \end{pmatrix}^T$. The least common multiple of the denominators is 12; since $\begin{pmatrix} 12 & -8 \end{pmatrix}^T \succ_{\mathbb{Z}^n} \begin{pmatrix} 9 & -24 \end{pmatrix}^T$, we have $\zeta \succ_{\mathbb{Q}^n} \vartheta$.

$\diamond$

7.2.3. WEIGHT VECTORS FOR A SUBSPACE OF $\mathbb{Q}^n$. If we could assemble different "weight vectors" that order different subspaces of $\mathbb{Q}^n$ in accordance with $\succ_{\mathbb{Q}^n}$, we could construct a matrix that satisfies the requirements of theorem 7.5. How would these weight vectors behave? Suppose ω was one such weight vector; we would

need

$$\omega \cdot \alpha > \omega \cdot \beta \quad \Rightarrow \quad \alpha \succ_{\mathbb{Q}^n} \beta$$

Moreover, for the matrix to be admissible, we would also need the weight vectors to be linearly independent over $\mathbb{Q}$, and

$$\omega \cdot \alpha > 0 \quad \forall \alpha \in \mathbb{N}^n_{\geq 0}$$

The following lemma, adapted with minor cosmetic changes from [**HW99**], provides a constructive proof that such weight vectors exist for any term ordering $\succ$. It is an explicit construction that corresponds to a similar lemma in [**Wei87**].

LEMMA 7.7. *Let $\succ_{\mathbb{Q}^n}$ be the extension to $\mathbb{Q}^n$ of an admissible term ordering $\succ$. For any non-trivial, $\mathbb{Q}$-linear subspace U of $\mathbb{Q}^n$, $\exists m \in \mathbb{R}^n$ such that:*

- *m is in the $\mathbb{R}$-linear extension of U*
- *$m \cdot x > 0$ implies $x \succ_{\mathbb{Q}^n} 0$*
- *$x \in \mathbb{Z}^n_{\geq 0}$ implies $m \cdot x \geq 0$*

PROOF. Let U be a non-trivial $\mathbb{Q}$-linear subspace of $\mathbb{Q}^n$. We prove the lemma by construction of m.

Let $\{v_1, \ldots, v_s\}$ be an arbitrary orthogonal $\mathbb{Q}$-basis of U with $v_1, \ldots, v_s \succ_{\mathbb{Q}^n} 0$. Let k be such that $v_k \succeq_{\mathbb{Q}^n} v_1, \ldots, v_s$.

For $j = 1, \ldots, s$, let

$$\gamma_j = \inf \{q \in \mathbb{Q} : q v_k \succ_{\mathbb{Q}^n} v_j\}$$

Let

$$m = \sum_{i=1}^{s} \gamma_i \cdot \frac{v_i^T}{v_i^T \cdot v_i}$$

We claim that m satisfies the requirements of the lemma.

Let $x \in U$ be arbitrary, but fixed. Let $x'_1, \ldots, x'_s$ be the co-ordinates of x with respect to $v_1, \ldots, v_s$. Then

$$\begin{aligned} m \cdot x &= \left(\sum_{i=1}^{s} \gamma_i \cdot \frac{v_i^T}{v_i^T \cdot v_i} \right) \cdot \left(\sum_{j=1}^{s} x'_j v_j \right) \\ &= \sum_{i=1}^{s} \sum_{j=1}^{s} \gamma_i x'_j \cdot \frac{v_i^T \cdot v_j}{v_i^T \cdot v_i} \end{aligned}$$

For $i \neq j$, v_i and v_j are orthogonal, so $v_i^T \cdot v_j = 0$. Thus

$$\begin{aligned} m \cdot x &= \sum_{i=1}^{s} \gamma_i x'_i \\ &= \gamma \cdot x' \end{aligned}$$

Assume $m \cdot x > 0$; then $\gamma \cdot x' > 0$. We want to show that $x \succ_{\mathbb{Q}^n} 0$. Using the continuity of the real line, choose $\gamma' \in \mathbb{Q}^n$ such that $\gamma' \cdot x' > 0$ and

$$\gamma'_j > \gamma_j \quad \text{if} \quad x'_j < 0$$

$$\gamma'_j < \gamma_j \quad \text{if} \quad x'_j > 0$$

$$\gamma'_j = 0 \quad \text{if} \quad x'_j = 0$$

We claim that

$$0 \prec_{\mathbb{Q}^n} (\gamma' \cdot x') \, v_k \prec_{\mathbb{Q}^n} x$$

We have

$$0 \prec_{\mathbb{Q}^n} (\gamma' \cdot x') v_k = \left(\sum_{j=1}^{s} \gamma'_j x'_j \right) v_k = \sum_{j=1}^{s} \gamma'_j \left(x'_j v_k \right)$$

Let $j \in \{1, \ldots, s\}$ be arbitrary, but fixed.

Case 1: $x'_j < 0$

Then $\gamma'_j > \gamma_j$. Recall that $\gamma_j = \inf \{q \in \mathbb{Q} : q v_k \succ_{\mathbb{Q}^n} v_j\}$, so

$$\gamma'_j v_k \succ_{\mathbb{Q}^n} v_j$$

Multiplying both sides by the scalar x'_j, we have

$$x'_j \cdot \left(\gamma'_j v_k \right) \prec_{\mathbb{Q}^n} x'_k \cdot v_j$$

Case 2: $x'_j > 0$

Then $\gamma'_j < \gamma_j$. Recall again that $\gamma_j = \inf \{q \in \mathbb{Q} : q v_k \succ_{\mathbb{Q}^n} v_j\}$. Then

$$\gamma'_j v_k \prec_{\mathbb{Q}^n} \gamma_j v_k \preceq_{\mathbb{Q}^n} v_j$$

Multiplying both sides by the scalar x'_j,

$$x'_j \left(\gamma'_j v_k \right) \prec_{\mathbb{Q}^n} x'_j v_j$$

From cases 1 and 2,

$$0 \prec_{\mathbb{Q}^n} (\gamma' \cdot x') v_k = \left(\sum_{j=1}^{s} \gamma'_j \cdot x'_j \right) v_k = \sum_{j=1}^{s} \left(x'_j \left(\gamma'_j v_k \right) \right) \prec \sum_{j=1}^{s} x'_j v_j = x$$

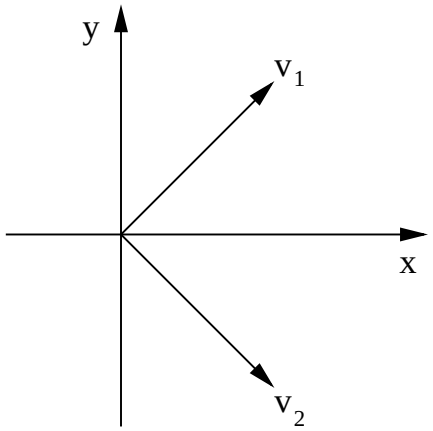


Figure 7.1: Diagram of vectors v_1, v_2 in example 7.8.

Finally, let $x \in \mathbb{N}^n$. Then $x \succ_{\mathbb{Q}^n} 0$. Assume by way of contradiction that $m \cdot x < 0$. Then $-m \cdot x > 0$, whence $m \cdot (-x) > 0$. This implies that $-x \succ_{\mathbb{Q}^n} 0$, thus $0 \succ_{\mathbb{Q}^n} x$, which contradicts $x \succ_{\mathbb{Q}^n} 0$. □

Before proving the theorem, we illustrate concretely how lemma 7.7 works.

EXAMPLE 7.8. Let $\succ = \text{lex}\,(x, y)$. We construct m for $U = \mathbb{Q}^2$.

Following the proof, take

$$v_1 = \begin{pmatrix} 1 & 1 \end{pmatrix}^T$$
$$v_2 = \begin{pmatrix} 1 & -1 \end{pmatrix}^T$$

(See figure 7.1.) We claim that v_1, v_2 are an orthogonal basis with

$$v_1 \succ_{\mathbb{Q}^2} v_2 \succ_{\mathbb{Q}^2} 0$$

For the orthogonality (which is geometrically clear),

$$v_1 \cdot v_2 = 1 - 1 = 0$$

We can see that the two vectors are linearly independent from

$$\begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} = -2 \neq 0$$

As for the ordering, it is intuitively clear from the geometry: compare how far right the vectors lie, in case of a tie, how far up. Algebraically,

$$y^2 \succ 1 \quad \Rightarrow \quad \begin{pmatrix} 0 & 2 \end{pmatrix}^T \succ_{\mathbb{Z}^2_{\geq 0}} 0 \quad \Rightarrow \quad \begin{pmatrix} 1 & 1 \end{pmatrix}^T - \begin{pmatrix} 1 & -1 \end{pmatrix}^T \succ_{\mathbb{Z}^2} 0$$

and by extension

$$\begin{pmatrix} 1 & 1 \end{pmatrix}^T \succ_{\mathbb{Q}^2} \begin{pmatrix} 1 & -1 \end{pmatrix}^T$$

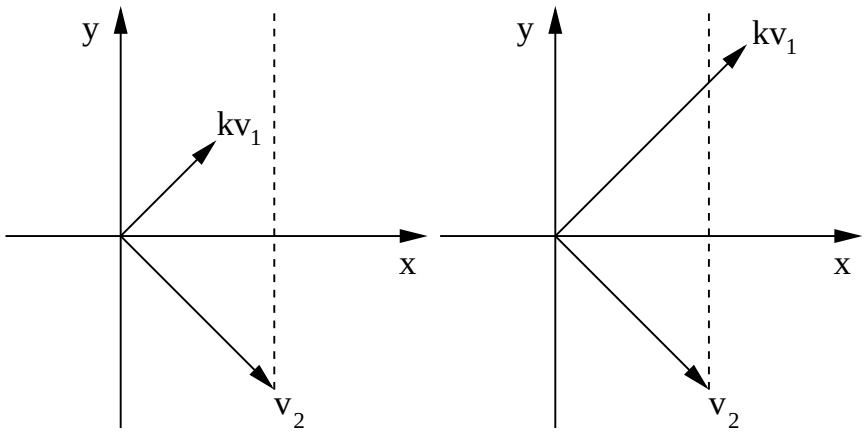
A similar argument will show that $\begin{pmatrix} 1 & -1 \end{pmatrix}^T \succ_{\mathbb{Q}^2} 0$.

Following the proof, we set

$$\gamma_1 = \inf \{q \in \mathbb{Q} : qv_1 \succ_{\mathbb{Q}^2} v_1\}$$

Geometrically, this says that γ_1 is the maximum scaling of v_1 that is no larger than itself with respect to $\succ_{\mathbb{Q}^2}$; this is obviously 1. Similarly, set

$$\gamma_1 = \inf \{q \in \mathbb{Q} : qv_1 \succ_{\mathbb{Q}^2} v_2\}$$



(a) kv_1 for $k < 1$ (b) kv_1 for $k > 1$

Figure 7.2: How lemma 7.7 generates γ_1, γ_2 for example 7.8.

Geometrically, this says that γ_2 is the maximum scaling of v_1 that is no larger than v_2 with respect to $\succ_{\mathbb{Q}^2}$: that is, the scaling of v_1 whose rightmost entry is less than or equal to the rightmost entry of v_2. Again, this is 1; see figure 7.2.

Then

$$\begin{aligned} m &= \gamma_1 \cdot \frac{v_1^T}{v_1^T v_1} + \gamma_2 \cdot \frac{v_2^T}{v_2^T v_2} \\ &= \frac{\begin{pmatrix} 1 & 1 \end{pmatrix}}{\begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \end{pmatrix}^T} + \frac{\begin{pmatrix} 1 & -1 \end{pmatrix}}{\begin{pmatrix} 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \end{pmatrix}^T} \\ &= \frac{\begin{pmatrix} 1 & 1 \end{pmatrix}}{2} + \frac{\begin{pmatrix} 1 & -1 \end{pmatrix}}{2} \\ &= \begin{pmatrix} 1 & 0 \end{pmatrix} \end{aligned}$$

Not surprisingly, if we take

$$m \cdot \alpha$$

for any exponent vector α, m selects the first co-ordinate as the weight. This is precisely the first test of the lexicographic ordering. ——————————◇

7.2.4. PROOF OF THEOREM 7.5. Now we can prove theorem 7.5. We restate it and present the proof:

THEOREM. *(A) and (B) where*

(A) Every term ordering on terms in $x_1, \ldots, x_n$ is induced by an admissible matrix $\mathcal{M} \in \mathbb{R}^{m \times n}$.

(B) Every admissible matrix $\mathcal{M} \in \mathbb{R}^{m \times n}$ induces a term ordering on $\mathcal{T}(x_1, \ldots, x_n)$ (the set of terms in $x_1, \ldots, x_n$).

PROOF. We prove (A) by construction.

Using lemma 7.7, find $\mathcal{M}_{(1)}$ on $\mathbb{Q}^n$.

For $i > 1$, let $V_j = \left\{x \in \mathbb{Q}^n : \mathcal{M}_{(j)} \cdot x = 0\right\}$ for $j = 1, \ldots, i-1$, and $U_i = V_1 \cap \cdots \cap V_{i-1}$. Using lemma 7.7, find $\mathcal{M}_{(i)}$ for the non-trivial subspaces U_i of $\mathbb{Q}^n$.

Since $\dim U_{i-1} > \dim U_i$ and $\dim U_1 < n$, this process must terminate at some trivial subspace $U_m = \{0\}$. It is clear from the construction in the proof of lemma 7.7 that $\mathcal{M}$ has full rank; we further have $\mathcal{M} \cdot x \gg 0$ for $x \in \mathbb{N}^n \setminus \{0\}$. Hence $\mathcal{M}$ is admissible; also from the lemma, $\mathcal{M}$ induces $\succ$.

To prove (B), let $\mathcal{M}$ be arbitrary, but fixed. Define in the following way a relation $\succ_{\mathcal{M}}$ on $\mathcal{T}(x_1, \ldots, x_n)$, the set of terms in $x_1, \ldots, x_n$: for all $t, u \in \mathcal{T}(x_1, \ldots, x_n)$, whose exponent vectors we denote as α, β,

$$t \succ_{\mathcal{M}} u \quad \Leftrightarrow \quad \mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta$$

We claim that $\succ_{\mathcal{M}}$ is an admissible term ordering. We verify that $\succ_{\mathcal{M}}$ satisfies the three parts of the definition.

First claim: $\forall t \neq u \in \mathcal{T}(x_1, \ldots, x_n)$, $t \succ_{\mathcal{M}} u$ or $u \succ_{\mathcal{M}} t$.

Let $t, u \in \mathcal{T}(x_1, \ldots, x_n)$. Let α, β be the exponent vectors of t, u, respectively.

We approach by the contrapositive: assume neither $t \succ_{\mathcal{M}} u$ nor $u \succ_{\mathcal{M}} t$. Then $\mathcal{M} \cdot \alpha = \mathcal{M} \cdot \beta$.

Certainly $\mathcal{M} \cdot \alpha = \mathcal{M} \cdot \beta$ iff $\mathcal{M} \cdot (\alpha - \beta) = 0$. Since $\mathcal{M}$ has full rank, $\alpha = \beta$.

Hence $t = u$.

So, $t \neq u$ implies $t \succ_{\mathcal{M}} u$ or $u \succ_{\mathcal{M}} t$.

Second claim: $\forall t \in \mathcal{T}(x_1, \ldots, x_n)$, $t \neq 1$ implies $t \succ_{\mathcal{M}} 1$.

Let $t \in \mathcal{T}(x_1, \ldots, x_n)$, and write α for the exponent vector of t. Observe that 0 is the exponent vector of 1.

Assume $t \neq 1$. We have $\alpha \in \mathbb{Z}^n_{\geq 0}$, and $\alpha \neq 0$. By definition of an admissible matrix, $\mathcal{M} \cdot \alpha \gg 0$. Thus $\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot 0$.

Hence $t \succ_{\mathcal{M}} 1$.

Third claim: $\forall t, u, v \in \mathcal{T}(x_1, \ldots, x_n)$, $t \succ_{\mathcal{M}} u$ implies $tv \succ_{\mathcal{M}} uv$.

Let $t, u, v \in \mathcal{T}(x_1, \ldots, x_n)$, and write α, β, γ for their exponent vectors, respectively.

Assume $t \succ_{\mathcal{M}} u$. Then

$$\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta$$

$$\mathcal{M} \cdot \alpha + \mathcal{M} \cdot \gamma \gg \mathcal{M} \cdot \beta + \mathcal{M} \cdot \gamma$$

$$\mathcal{M} \cdot (\alpha + \gamma) \gg \mathcal{M} \cdot (\beta + \gamma)$$

It follows that $tv \succ_{\mathcal{M}} uv$.

We have shown that $\succ_{\mathcal{M}}$ satisfies the three criteria for an admissible term ordering. Since $\mathcal{M}$ was an arbitrary admissible matrix, we conclude that every admissible matrix induces a term ordering on $\mathcal{T}(x_1, \ldots, x_n)$. □

7.3. SOLVING FOR ADMISSIBLE MATRICES

Suppose we want a term ordering that satisfies a finite number of constraints. The following theorem shows that we can construct an admissible matrix that induces such a term ordering.

THEOREM 7.9. *Let $t_1, \ldots, t_{2r}$ be terms with exponent vectors $\alpha_1, \ldots, \alpha_{2r}$. We have (A)⇔(B) where*

(A) There exists an admissible term ordering $\succ$ such that

$$t_1 \succ t_2 \quad \cdots \quad t_{2r-1} \succ t_{2r}$$

(B) There exists an admissible matrix $\mathcal{M} \in \mathbb{Q}^n_{\geq 0}$ whose first row ω satisfies

$$\omega \cdot \alpha_1 \gg \omega \cdot \alpha_2 \quad \cdots \quad \omega \cdot \alpha_{2r-1} \gg \omega \cdot \alpha_{2r}$$

and $\mathcal{M}$ represents a term ordering $\succ_{\mathcal{M}}$ such that

$$t_1 \succ_{\mathcal{M}} t_2 \cdots \quad t_{2r-1} \succ_{\mathcal{M}} t_{2r}$$

We do *not* claim that $\mathcal{M}$ is an admissible matrix representation of $\succ$! It could be that $\mathcal{M}$ represents $\succ$, but $\mathcal{M}$ may represent another term ordering altogether. Rather, $\succ$ and $\succ_{\mathcal{M}}$ both satisfy the given constraints on $t_1, \ldots, t_{2r}$.

To prove the theorem, we need some technical lemmas that are interesting on their own. One of the lemmas requires a definition.

DEFINITION 7.10. Two admissible matrices $\mathcal{M}$ and $\mathcal{N}$ are **equivalent** if for all exponent vectors $\alpha, \beta \in \mathbb{Q}^n$

$$\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta \quad \Leftrightarrow \quad \mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$$

The underlying idea is that $\mathcal{M}$ and $\mathcal{N}$ represent the same term ordering; even if they are distinct matrices, they nevertheless behave identically on exponent vectors.

EXAMPLE 7.11. The admissible matrices

$$\mathcal{M} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \mathcal{N} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

are equivalent.

We leave it as an exercise for the reader to show that $\mathcal{M}$ and $\mathcal{N}$ are admissible.

Why are they equivalent? Let $\alpha, \beta \in \mathbb{Q}^n$. Assume $\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta$. Note that

$$\mathcal{M} \cdot \alpha = \begin{pmatrix} \alpha_{(1)} + \alpha_{(2)} \\ \\ \alpha_{(2)} \end{pmatrix} \qquad \mathcal{M} \cdot \beta = \begin{pmatrix} \beta_{(1)} + \beta_{(2)} \\ \\ \beta_{(2)} \end{pmatrix}$$

and

$$\mathcal{N} \cdot \alpha = \begin{pmatrix} \alpha_{(1)} + \alpha_{(2)} \\ \\ -\alpha_{(1)} \end{pmatrix} \qquad \mathcal{M} \cdot \beta = \begin{pmatrix} \beta_{(1)} + \beta_{(2)} \\ \\ -\beta_{(1)} \end{pmatrix}$$

Case 1: $\alpha_{(1)} + \alpha_{(2)} > \beta_{(1)} + \beta_{(2)}$

It is immediate that $\mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$.

Case 2: $\alpha_{(1)} + \alpha_{(2)} = \beta_{(1)} + \beta_{(2)}$ and $\alpha_{(2)} > \beta_{(2)}$.

Then

$$\begin{aligned} -\alpha_{(1)} &= -\alpha_{(1)} + \big(\alpha_{(2)} - \alpha_{(2)}\big) \\ &= \alpha_{(2)} - \big(\alpha_{(1)} + \alpha_{(2)}\big) \\ &= \alpha_{(2)} - \big(\beta_{(1)} + \beta_{(2)}\big) \\ &> \beta_{(2)} - \big(\beta_{(1)} + \beta_{(2)}\big) \\ &= -\beta_{(1)} \end{aligned}$$

Thus $\mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$.

We have shown that

$$\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta \quad \Rightarrow \quad \mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$$

A similar argument shows the converse.

Thus, $\mathcal{M}$ and $\mathcal{N}$ are equivalent. ◇

Now we present the lemmas. We use the notation $\mathcal{M}_{(i,j)}$ to represent the entry in row i, column j of $\mathcal{M}$.

The first lemma is proposition 1.4.12 on page 53 of [**KR00**].

LEMMA 7.12. *For any admissible matrix $\mathcal{M}$, the first non-zero entry in every column is positive.*

PROOF. We show the contrapositive. Suppose that entry j is the first nonzero entry of column i of $\mathcal{M}$; suppose further that $\mathcal{M}_{(i,j)} < 0$. Let α be the elementary column vector e_j; that is, let α have one in the jth entry, and zeros elsewhere. Then

$$\mathcal{M} \cdot \alpha = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \mathcal{M}_{(i,j)} \\ \vdots \\ \mathcal{M}_{(m,j)} \end{pmatrix}$$

Recall that $\mathcal{M}_{(i,j)}$ is negative. Then $0 \gg \mathcal{M} \cdot \alpha$, so $\mathcal{M}$ is not admissible.

Hence, if $\mathcal{M}$ is admissible, the first nonzero entry in every column is positive.

□

The following lemma makes use of the previous result; we have found it to be enormously useful for computational purposes.

LEMMA 7.13. *Let $\mathcal{M}$ be an admissible matrix. There exists $\mathcal{N}$ such that $\mathcal{N}$ is equivalent to $\mathcal{M}$, and all the entries of $\mathcal{N}$ are nonnegative.*

The strategy for proving lemma 7.13 is quite simple: we add sufficiently large multiples of upper rows to lower rows to create $\mathcal{N}$. In example 7.11 for instance, we obtained $\mathcal{M}$ from $\mathcal{N}$ by adding the first row of $\mathcal{M}$ to the second. This does not change the term ordering, since the second row of $\mathcal{M}$ is only necessary to order terms in the null space of the first row; the third row is only necessary to order terms in the null space of the first two rows; etc.

PROOF. Construct $\mathcal{N}$ as follows:

put $\mathcal{N}_{(1)} = \mathcal{M}_{(1)}$;

for $i > 1$

choose $\rho_i \in \mathbb{N}$ such that $\rho_i \cdot \mathcal{N}_{(i-1,j)} \geq \left|\mathcal{M}_{(i,j)}\right|$ for $j = 1, \ldots, n$

put $\mathcal{N}_{(i)} = \rho_i \cdot \mathcal{N}_{(i-1)} + \mathcal{M}_{(i)}$

Recall from lemma 7.12 that the first nonzero entry of every column of $\mathcal{M}$ is nonnegative; the choice of ρ_i makes it clear that all the entries of $\mathcal{N}$ are nonnegative.

Now we claim that, for all exponent vectors $\alpha, \beta \in \mathbb{Q}^n$, $\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta$ if and only if $\mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$.

Let $\alpha, \beta \in \mathbb{Q}^n$. Assume $\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta$. Thus

$$\mathcal{M} \cdot (\alpha - \beta) \gg 0$$

Hence, $\exists R \in \mathbb{N}$ such that

$$\mathcal{M}_{(\ell)} \cdot (\alpha - \beta) \gg 0 \qquad \text{for } \ell = 1, \ldots, R-1$$

$$\mathcal{M}_{(R)} \cdot (\alpha - \beta) = 0$$

We claim that $\mathcal{N}_{(\ell)} \cdot (\alpha - \beta) = 0$ for $\ell = 1, \ldots, R-1$ and $\mathcal{N}_{(R)} \cdot (\alpha - \beta) > 0$. We proceed by induction on ℓ.

Inductive base: Since $\mathcal{N}_{(1)} = \mathcal{M}_{(1)}$, it follows that $\mathcal{N}_{(1)} \cdot (\alpha - \beta) \geq 0$. The inequality is strict only if $\mathcal{M}_{(1)} \cdot (\alpha - \beta) > 0$; that is, if $R = 1$.

Inductive step: Let $1 < \ell \leq R$, and assume $\mathcal{N}_{(k)} \cdot (\alpha - \beta) = 0$ for $1 \leq k < \ell$. Recall

$$\mathcal{N}_{(\ell)} = \rho_\ell \cdot \mathcal{N}_{(\ell-1)} + \mathcal{M}_{(\ell)}$$

Then

$$\begin{aligned} \mathcal{N}_{(\ell)} \cdot (\alpha - \beta) &= \left(\rho_\ell \cdot \mathcal{N}_{(\ell-1)} + \mathcal{M}_{(\ell)}\right) \cdot (\alpha - \beta) \\ &= \rho_\ell \cdot \mathcal{N}_{(\ell-1)} \cdot (\alpha - \beta) + \mathcal{M}_{(\ell)} \cdot (\alpha - \beta) \end{aligned}$$

Since $\mathcal{N}_{(\ell-1)} \cdot (\alpha - \beta) = 0$,

$$\mathcal{N}_{(\ell)} \cdot (\alpha - \beta) = \mathcal{M}_{(\ell)} \cdot (\alpha - \beta)$$

Hence $\mathcal{N}_{(\ell)} \cdot (\alpha - \beta) \geq 0$; the inequality is strict only if $\mathcal{M}_{(\ell)} \cdot (\alpha - \beta) > 0$; that is, if $\ell = R$.

Thus

$$\mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$$

We have shown that $\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta$ implies $\mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$. It remains to show the converse. Assume that

$$\mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$$

Thus

$$\mathcal{N} \cdot (\alpha - \beta) \gg 0$$

Hence, there exists $R \in \mathbb{N}$ such that

$$\mathcal{N}_{(\ell)} \cdot (\alpha - \beta) = 0 \qquad \ell = 1, \ldots, R-1$$

$$\mathcal{N}_{(R)} \cdot (\alpha - \beta) > 0$$

We claim that $\mathcal{M}_{(\ell)} \cdot (\alpha - \beta) = 0$ for $\ell = 1, \ldots, R-1$, and $\mathcal{M}_{(R)} \cdot (\alpha - \beta) > 0$. We proceed by induction on ℓ.

Inductive base: Since $\mathcal{M}_{(1)} = \mathcal{N}_{(1)}$, we have $\mathcal{M}_{(1)} \cdot (\alpha - \beta) \geq 0$. The inequality is strict only if $\mathcal{N}_{(1)} \cdot (\alpha - \beta) > 0$; that is, if $R = 1$.

Inductive step: For $1 < \ell \leq R$, assume $\mathcal{N}_{(k)} \cdot (\alpha - \beta) = 0$ for $1 \leq k < \ell$. Recall

$$\mathcal{N}_{(\ell)} = \rho_\ell \cdot \mathcal{N}_{(\ell-1)} + \mathcal{M}_{(\ell)}$$

Then

$$\begin{aligned}\mathcal{N}_{(\ell)} \cdot (\alpha - \beta) &= \left(\rho_\ell \cdot \mathcal{N}_{(\ell-1)} + \mathcal{M}_{(\ell)}\right) \cdot (\alpha - \beta) \\ &= \rho_\ell \cdot \mathcal{N}_{(\ell-1)} \cdot (\alpha - \beta) + \mathcal{M}_{(\ell)} \cdot (\alpha - \beta)\end{aligned}$$

Since $\mathcal{N}_{(\ell-1)} \cdot (\alpha - \beta) = 0$, we have

$$\mathcal{M}_{(\ell)} \cdot (\alpha - \beta) = \mathcal{N}_{(\ell)} \cdot (\alpha - \beta) \geq 0$$

The inequality is strict only if $\mathcal{N}_{(\ell)} \cdot (\alpha - \beta) > 0$; that is, if $\ell = R$. Thus

$$\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta$$

We have shown that for arbitrary $\alpha, \beta \in \mathbb{Q}^n$,

$$\mathcal{M} \cdot \alpha \gg \mathcal{M} \cdot \beta \quad \Leftrightarrow \mathcal{N} \cdot \alpha \gg \mathcal{N} \cdot \beta$$

It follows that $\mathcal{N}$ has full column rank over $\mathbb{Q}^n$, and that $\mathcal{N} \cdot \alpha \gg 0$ for all nonzero $\alpha \in \mathbb{Q}^n$. Hence $\mathcal{N}$ is admissible; it is equivalent to $\mathcal{M}$; and all its entries are non-negative. □

Now we prove theorem 7.9. At the end of the section, we discuss how the proof suggests a way to construct a term ordering satisfying the requirements of clause (A) of the theorem, *assuming such a term ordering exists.* First we restate the theorem:

THEOREM. *Let $t_1, \ldots, t_{2r}$ be terms with exponent vectors $\alpha_1, \ldots, \alpha_{2r}$. We have (A)⇔(B) where*

(A) There exists an admissible term ordering $\succ$ such that

$$t_1 \succ t_2 \quad \cdots \quad t_{2r-1} \succ t_{2r}$$

(B) There exists an admissible matrix $\mathcal{M} \in \mathbb{Q}_{\geq 0}^{n \times n}$ whose first row ω satisfies

$$\omega \cdot \alpha_1 \gg \omega \cdot \alpha_2 \quad \cdots \quad \omega \cdot \alpha_{2r-1} \gg \omega \cdot \alpha_{2r}$$

and $\mathcal{M}$ represents a term ordering $\succ_{\mathcal{M}}$ such that

$$t_1 \succ_{\mathcal{M}} t_2 \cdots \quad t_{2r-1} \succ_{\mathcal{M}} t_{2r}$$

PROOF. That (A)⇐(B) is immediate, since $\mathcal{M}$ induces a term ordering that satisfies (A). It remains to show that (A)⇒(B).

Assume (A). We have an admissible term ordering $\succ$ such that

$$\tau_1 \succ \tau_2 \quad \tau_3 \succ \tau_4 \quad \cdots \quad \tau_{2r-1} \succ \tau_{2r}$$

Claim 1: We claim that $\exists \omega \in \mathbb{R}_{\geq 0}^n$ satisfying

$$\omega \cdot \alpha_1 > \omega \cdot \alpha_2 \quad \cdots \quad \omega \cdot \alpha_{2r-1} > \omega \cdot \alpha_{2r}$$

Let $\mathcal{M}$ be an admissible matrix representation of $\succ$. Certainly

$$\mathcal{M} \cdot \alpha_1 \gg \mathcal{M} \cdot \alpha_2 \quad \cdots \quad \mathcal{M} \cdot \alpha_{2r-1} \gg \mathcal{M} \cdot \alpha_{2r}$$

(If $\mathcal{M} \cdot \alpha_{2i-1} \not\gg \mathcal{M} \cdot \alpha_{2i}$, then $\tau_{2i-1} \preceq \tau_{2i}$, which contradicts the hypothesis.) By lemma 7.13, we may assume that the entries of $\mathcal{M}$ are nonnegative. Thus we can put $\omega \in \mathbb{R}^n_{\geq 0}$ such that

$$\omega = \rho_1 \mathcal{M}_{(1)} + \rho_2 \mathcal{M}_{(2)} + \cdots + \rho_m \mathcal{M}_{(m)}$$

where $\rho_m = 1$ and for $k = 1, \ldots, m-1$ $\rho_k \in \mathbb{N}$ is sufficiently large that for every $\ell = 1, \ldots, r$

$$\begin{aligned} \rho_k \left| \mathcal{M}_{(k)} \cdot (\alpha_{2\ell-1} - \alpha_{2\ell}) \right| &> \rho_{k+1} \left| \mathcal{M}_{(k+1)} \cdot (\alpha_{2\ell-1} - \alpha_{2\ell}) \right| \\ &+ \cdots \\ &+ \rho_m \left| \mathcal{M}_{(m)} \cdot (\alpha_{2\ell-1} - \alpha_{2\ell}) \right| \end{aligned}$$

We claim that for $\ell = 1, \ldots, r$ we have

$$\omega \cdot (\alpha_{2\ell-1} - \alpha_{2\ell}) > 0$$

Let $j \in \{1, \ldots, r\}$. Using $\mathcal{M} \cdot \alpha_{2j-1} \gg \mathcal{M} \cdot \alpha_{2j}$, choose R such that such that

$$\begin{aligned} \mathcal{M}_{(\ell)} \cdot (\alpha_{2j-1} - \alpha_{2j}) &= 0 \qquad \forall \ell = 1, \ldots, R-1 \\ \mathcal{M}_{(R)} \cdot (\alpha_{2j-1} - \alpha_{2j}) &> 0 \end{aligned}$$

Then

$$\begin{aligned} \omega \cdot (\alpha_{2j-1} - \alpha_{2j}) &= \left(\rho_1 \mathcal{M}_{(1)} + \cdots + \rho_m \mathcal{M}_{(m)} \right) \cdot (\alpha_{2j-1} - \alpha_{2j}) \\ &= \rho_1 \mathcal{M}_{(1)} \cdot (\alpha_{2j-1} - \alpha_{2j}) + \cdots + \rho_m \mathcal{M}_{(m)} \cdot (\alpha_{2j-1} - \alpha_{2j}) \end{aligned}$$

$$
\begin{aligned}
&= \rho_1 \mathcal{M}_{(1)} \cdot (\alpha_{2j-1} - \alpha_{2j}) + \cdots + \rho_{R-1} \mathcal{M}_{(R-1)} \cdot (\alpha_{2j-1} - \alpha_{2j}) \\
&\quad + \rho_R \mathcal{M}_{(R)} \cdot (\alpha_{2j-1} - \alpha_{2j}) + \cdots + \rho_m \mathcal{M}_{(m)} \cdot (\alpha_{2j-1} - \alpha_{2j}) \\
&= 0 + \rho_R \mathcal{M}_{(R)} \cdot (\alpha_{2j-1} - \alpha_{2j}) + \cdots + \rho_m \mathcal{M}_{(m)} \cdot (\alpha_{2j-1} - \alpha_{2j}) \\
&= \rho_R \mathcal{M}_{(R)} \cdot (\alpha_{2j-1} - \alpha_{2j}) \\
&\quad + \rho_{R+1} \mathcal{M}_{(R+1)} \cdot (\alpha_{2j-1} - \alpha_{2j}) + \cdots + \rho_m \mathcal{M}_{(m)} \cdot (\alpha_{2j-1} - \alpha_{2j})
\end{aligned}
$$

Recall $\mathcal{M}_{(R)} \cdot (\alpha_{2j-1} - \alpha_{2j}) > 0$. Then

$$
\begin{aligned}
\omega \cdot (\alpha_{2j-1} - \alpha_{2j}) &= \rho_R \left| \mathcal{M}_{(R)} \cdot (\alpha_{2j-1} - \alpha_{2j}) \right| \\
&\quad + \rho_{R+1} \mathcal{M}_{(R+1)} \cdot (\alpha_{2j-1} - \alpha_{2j}) + \cdots + \rho_m \mathcal{M}_{(m)} \cdot (\alpha_{2j-1} - \alpha_{2j}) \\
&> \rho_{R+1} \left| \mathcal{M}_{(R+1)} \cdot (\alpha_{2j-1} - \alpha_{2\ell}) \right| + \cdots + \rho_m \left| \mathcal{M}_{(m)} \cdot (\alpha_{2j-1} - \alpha_{2\ell}) \right| \\
&\quad + \rho_{R+1} \mathcal{M}_{(R+1)} \cdot (\alpha_{2j-1} - \alpha_{2j}) + \cdots + \rho_m \mathcal{M}_{(m)} \cdot (\alpha_{2j-1} - \alpha_{2j}) \\
&\geq 0
\end{aligned}
$$

Since j was arbitrary,

$$
\omega \cdot \alpha_1 > \omega \cdot \alpha_2 \quad \cdots \quad \omega \cdot \alpha_{2r-1} > \omega \cdot \alpha_{2r} \tag{7.2}
$$

for every $j = 1, \ldots, r$.

Claim 2: There is some $\mathcal{N} \in \mathbb{R}^{n \times n}_{\geq 0}$ whose first row ω satisfies

$$
\omega \cdot \alpha_1 > \omega \cdot \alpha_2 \qquad \cdots \qquad \omega \cdot \alpha_{2r-1} > \omega \cdot \alpha_{2r}
$$

and $\mathcal{N}$ represents a term ordering $\succ_{\mathcal{N}}$ such that

$$t_1 \succ_{\mathcal{N}} t_2 \qquad \cdots \qquad t_{2r-1} \succ_{\mathcal{N}} t_{2r}$$

Define $\mathcal{N}$ as follows:

- Let $\mathcal{N}_{(1)} = \omega$, where ω is constructed to satisfy claim 1.
- Let

$$\mathcal{E} = \{e_1, \ldots, e_n\} \subset \mathbb{N}^{1\times n} \text{ where } e_i = (\delta_{ik})_{k=1}^{n}$$

  (By δ_{ik}, we mean the Kronecker delta.)

- Fill the remaining $n-1$ rows of $\mathcal{N}$ with $\mathcal{E}\backslash e_j$ where j is the first nonzero element of u.

Observe that $\mathcal{N}$ has rank n, since the permutation $\begin{pmatrix} 1 & j & j-1 & \cdots & 3 & 2 \end{pmatrix}$ on the rows of $\mathcal{N}$ gives an upper-triangular matrix. Furthermore, all the entries of $\mathcal{N}$ are nonnegative, so $\mathcal{N} \cdot \alpha \gg 0$ for all vectors $\alpha \in \mathbb{Z}_{\geq 0}^{n}$. Hence $\mathcal{N}$ is an admissible matrix.

Let $\succ_{\mathcal{N}}$ be the term ordering induced by $\mathcal{N}$. Since ω is the first row of $\mathcal{N}$ and ω was constructed as in claim 1, it follows from (7.2) that

$$\tau_1 \succ_{\mathcal{N}} \tau_2 \qquad \cdots \qquad \tau_{2r-1} \succ_{\mathcal{N}} \tau_{2r}$$

Thus $\mathcal{N}$ satisfies (B).

Claim 3: There is some $\mathcal{N}' \in \mathbb{Q}_{\geq 0}^{n\times n}$ that satisfies (B).

Let $\mathcal{N}$ be constructed as in claim 2, with first row ω. If $\omega \in \mathbb{Q}^n$, then we are done, for $\mathcal{N} \in \mathbb{Q}_{\geq 0}^{n \times n}$. Otherwise, let R be the number of irrational elements of ω. We claim that we can construct $v \in \mathbb{R}_{\geq 0}^n$ with $R-1$ irrational elements, and v satisfies

$$v \cdot \alpha_1 > v \cdot \alpha_2 \quad \cdots \quad v \cdot \alpha_{2r-1} > v \cdot \alpha_{2r}$$

We prove this claim by applying the following algorithm:

Step 1: Let i be such that $\omega_{(i)}$ is irrational.

Step 2: For unknown z_i define

$$z = \begin{pmatrix} \omega_{(1)} & \cdots & \omega_{(i-1)} & z_i & \omega_{(i+1)} & \cdots & \omega_{(n)} \end{pmatrix}$$

Step 3: Let

$$\epsilon = \inf_{\substack{z_i \in \mathbb{R} \\ \exists j \; z \cdot \alpha_{2j} \leq z \cdot \alpha_{2j+1}}} \left\{ \left| z_i - \omega_{(i)} \right| \right\} \in \mathbb{R}$$

Clearly $\epsilon > 0$, since $\omega \cdot \alpha_{2j} > \omega \cdot \alpha_{2j+1}$ for every $j = 1, \ldots, r$.

Step 4: Use the density of the rationals in the reals to choose $v_i \in \mathbb{Q}_{\geq 0}$ such that

$$\left| v_i - \omega_{(i)} \right| < \epsilon$$

Step 5: Put

$$v = \begin{pmatrix} \omega_{(1)} & \cdots & \omega_{(i-1)} & v_i & \omega_{(i+1)} & \cdots & \omega_{(n)} \end{pmatrix}$$

Since $\left| v_i - \omega_{(i)} \right| < \epsilon$,

$$v \cdot \alpha_1 > v \cdot \alpha_2 \quad \cdots \quad v \cdot \alpha_{2r-1} > v \cdot \alpha_{2r}$$

Step 6: If $v \in \mathbb{Q}^n_{\geq 0}$, we are done; otherwise, repeat steps 1–6 with v in place of ω.

Each iteration finds a vector with $R - 1$ irrational elements, so this algorithm terminates in at most n iterations with $v \in \mathbb{Q}^n_{\geq 0}$ satisfying

$$v \cdot \alpha_1 > v \cdot \alpha_2 \quad \cdots \quad v \cdot \alpha_{2r-1} > v \cdot \alpha_{2r} \tag{7.3}$$

Construct $\mathcal{N}'$ from $\mathcal{N}$ by replacing $\mathcal{N}_{(1)}$ with v. Since we have replaced ω by v, $\mathcal{N}' \in \mathbb{Q}^{n\times n}_{\geq 0}$. Since v satisfies (7.3), $\mathcal{N}'$ satisfies (B). □

We conclude with a brief discussion on how to construct a term ordering to satisfy clause (A) of theorem 7.9.

First, we determine constraints on the exponent vectors of the terms in (A); these constraints are as given for ω in (B). By the theorem, a term ordering satisfying (A) exists only if there exists a row vector $\omega \in \mathbb{Q}^n_{\geq 0}$ that satisfies (B). Furthermore, the proof of claim 2 shows how to construct a matrix $\mathcal{M}$ satisfying (B) by adjoining elementary row vectors to ω: if j is the first non-zero entry of ω, adjoin $\mathcal{E}\backslash e_j$, where e_j are the elementary row vectors described.

Thus, for given $t_1, \ldots, t_{2r-1}$, the problem reduces to solving the inequalities in (B) for $\omega_{(1)}, \ldots, \omega_{(n)}$: that is, finding a rational solution to a system of integer inequalities. The solution to this latter problem is well-established in the literature.

Chapter 8

Gröbner basis detection: general solution by polytopes

8.1. PROBLEM

In 1993, Peter Gritzmann and Bernd Sturmfels [**GS93**] used Minkowski sums of Newton polyhedra to find an algorithm for Gröbner basis detection. That is, they found an algorithm that solves

$$\exists \succ \qquad \mathrm{GB}_{\succ}\left(f_1, \ldots, f_m\right)$$

This chapter serves as a review of their result; we contribute nothing new to their research. Readers familiar with Newton polyhedra and Minkowski sums may choose to skip to section 8.3.

8.2. POLYTOPES, POLYHEDRA AND MINKOWSKI SUMS

The reader may need to review the background material on term diagrams; see section 2.5 on page 71.

A two-dimensional Newton polytope is similar to a term diagram, in that we plot terms in the positive quadrant of an x-y axis. However, rather than represent the *leading* terms of *several* polynomials, a Newton polytope encloses *all* the terms of *one* polynomial in the smallest possible convex polygon.

The following definition is adapted from those found on pages 290 and 291 of [**CLO98**] and page 247 of [**GS93**].

DEFINITION 8.1. For any finite set $A = \{m_1, \ldots, m_r\} \subset \mathbb{R}^n$, its **polytope** is

$$\left\{ \lambda_1 m_1 + \cdots + \lambda_r m_r : \lambda_i \geq 0, \sum_{i=1}^{r} \lambda_i = 1 \right\}$$

The **Newton polytope** $N(f)$ of the polynomial f is the polytope enclosing the points corresponding to the exponent vectors of the terms of f.

EXAMPLE 8.2. Let

$$f = x^2y + 3xy - x + 7y^3$$

The Newton polytope of f is given in figure 8.1.[1] ◇

We can manipulate the Newton polytope to obtain a so-called Newton polyhedron. The following definition comes from page 250 of [**GS93**]:

[1] Images of the convex polytopes in figures 8.1–8.4 were generated using [**Fra04**].

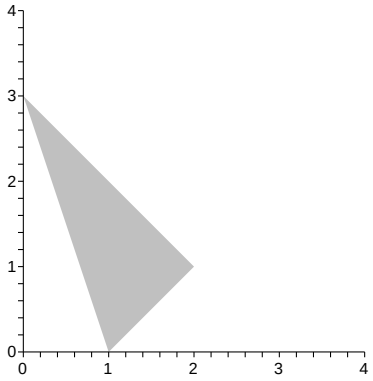


Figure 8.1: Newton polytope of f in example 8.2.

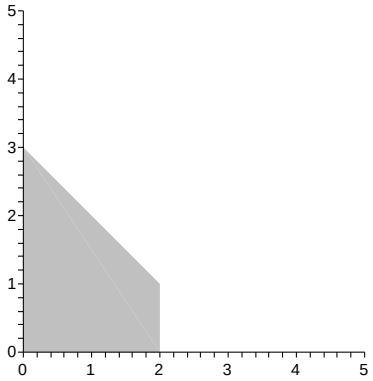


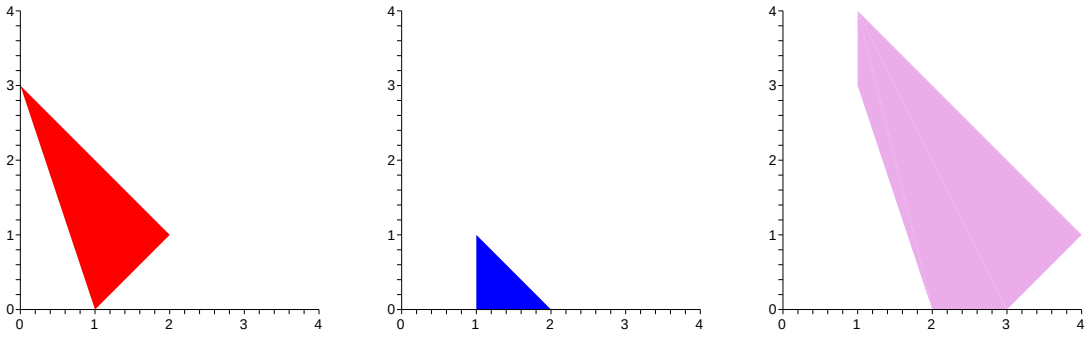
Figure 8.2: Newton polyhedron of f in example 8.2 (first quadrant view only).

DEFINITION 8.3. The **Newton polyhedron** of the polynomial f is the set

$$N_{\text{aff}}(f) = \left\{a + b : a \in N(f), b \in \mathbb{R}^n_{\leq 0}\right\}$$

Visually, a polynomial's poly*hedron* looks as if the corresponding poly*tope* is casting its shadow onto the axes; see figure 8.2.

Next we introduce the Minkowski sum of polytopes and polyhedra, taken from pg. 246 of [**GS93**].



(a) Newton polytope of f in 8.5

(b) Newton polytope of g in 8.5

(c) Minkowski sum of the Newton polytopes of f, g in 8.5

Figure 8.3: The Minkowski sum of the Newton polytopes $N(f)$ and $N(g)$, from example 8.5

DEFINITION 8.4. The **Minkowski sum** of two polytopes (or polyhedra) P_1 and P_2 is

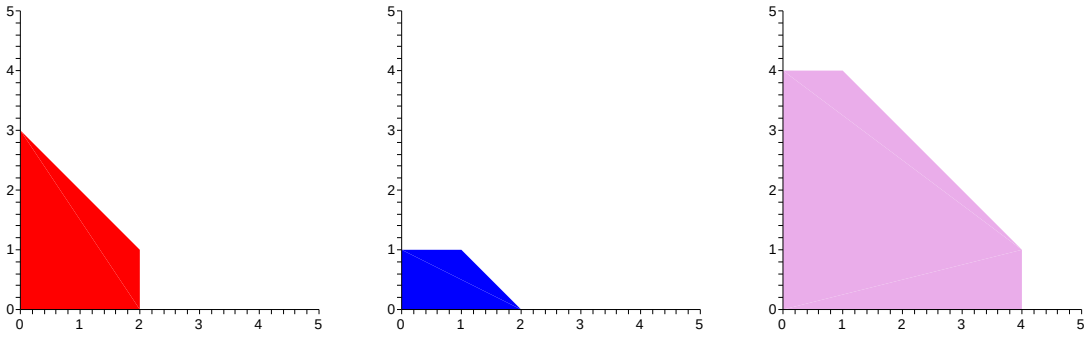
$$P_1 + P_2 = \{a + b : a \in P_1, b \in P_2\}$$

EXAMPLE 8.5. Let

$$f = x^2y + 3xy - x + 7y^3 \quad g = x^2 + x + xy$$

We illustrate the Minkowski sum of $N(f)$ and $N(g)$ in figure 8.3; figure 8.4 illustrates the Minkowski sum of $N_{\text{aff}}(f)$ and $N_{\text{aff}}(g)$. ◇

Finally, we introduce the *normal cone* of a vertex, from pg. 253 of [**GS93**]. We can think of the normal cone as the collection of vectors "inside" the borders created by the vectors normal to the faces that meet at a vertex.



(a) Newton polyhedron of f in 8.5

(b) Newton polyhedron of g in 8.5

(c) Minkowski sum of Newton polyhedra of f, g in 8.5

Figure 8.4: The Minkowski sum of the Newton polyhedra $N_{\text{aff}}(f)$ and $N_{\text{aff}}(g)$, from example 8.5

DEFINITION 8.6. Let P be a Newton polytope (or polyhedron); let F be a face of P, and let v be a vertex of P. The normal cone of F is the relatively open collection of outer normal vectors of P on the interior of F; the normal cone of v is the collection of vectors lying within the limiting faces of the normal cones of each face that meets at v.

EXAMPLE 8.7. Let P be the Minkowski sum of the Newton polyhedra of

$$f = x^2y + 3xy - x + 7y^3 \quad g = x^2 + x + xy$$

(see figure 8.4). The normal cones of P are illustrated in figure 8.5; they lie within the dotted lines. ◇

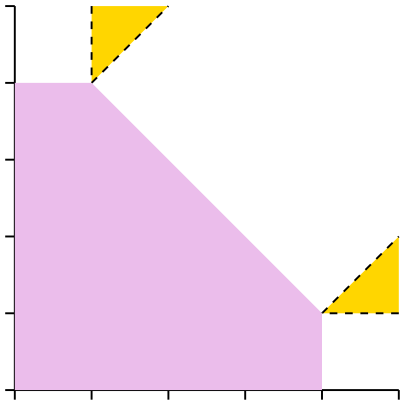


Figure 8.5: Normal cones of the Minkowski sum illustrated in figure 8.4.

8.3. RESULT

We start with the following observation. It is easy to see that for some polynomials, changing the term ordering may not change the leading term. For example, if $f = x + 1$ and $g = y + 1$, then the leading terms of f and g are x and y regardless of the term ordering. There are more complicated examples as well; consider 8.8:

EXAMPLE 8.8. Let

$$f = x^3 + 5 \qquad g = x^2y + y^3$$

There are only two possible pairs of leading terms of f, g:

$$\left(x^3, x^2y\right) \qquad \left(x^3, y^3\right)$$

Let $\succ_1 = \text{lex}(x, y)$, $\succ_2 = \text{lex}(y, x)$, and $\succ_3 = \text{tdeg}(x, y)$. We have

$$\text{lt}_{\succ_1}(f) = x^3 \quad \text{lt}_{\succ_1}(g) = x^2y$$

$$\text{lt}_{\succ_2}(f) = x^3 \quad \text{lt}_{\succ_2}(g) = y^3$$

$$\text{lt}_{\succ_3}(f) = x^3 \quad \text{lt}_{\succ_3}(g) = x^2y$$

We see that $\succ_1$ and $\succ_3$ have the same leading terms; we might say that they are equivalent with respect to $\{f, g\}$. On the other hand, $\succ_2$ has different leading terms, so it is not equivalent to $\succ_1$ and $\succ_3$. ◇

We can generalize this observation with the following definition:

DEFINITION 8.9. Two term orderings $\succ_1$ and $\succ_2$ are said to be **equivalent with respect to** $F = \{f_1, \ldots, f_m\}$ if

$$\text{lt}_{\succ_1}(f_1) = \text{lt}_{\succ_2}(f_1) \quad \cdots \quad \text{lt}_{\succ_1}(f_m) = \text{lt}_{\succ_2}(f_m)$$

It is obvious that this relation satisfies the axioms of an equivalent relation: it is reflexive, symmetric, and transitive.

A result of Teo Mora and Lorenzo Robbiano **[MR88]** is that given any set of polynomials $F = \{f_1, \ldots, f_m\}$, there are finitely many equivalence classes of term orderings with respect to F. The consequence is that we can collect all terms orderings into a finite number of equivalence classes with respect to F.

Gritzmann and Sturmfels point out that, since there are finitely many equivalence classes of term orderings, we can solve Gröbner basis detection by choosing

a representative $\succ$ from each class, then reducing the S-polynomials with respect to $\succ$. If all of them reduce to zero for a given representative $\succ$, then we know that $f_1, \ldots, f_m$ are a Gröbner basis with respect to $\succ$.

The question becomes, *how do we find the equivalence classes, then a representative term orderings of each equivalence class?* The answer is found in the following theorem, which is proposition 3.2.1 of [**GS93**].

THEOREM 8.10. *Let $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, and let M be the Minkowski sum of $N_{\text{aff}}(f_1), \ldots, N_{\text{aff}}(f_m)$. The vertices of M are in a one-to-one correspondence with the equivalence classes of term orderings with respect to $\{f_1, \ldots, f_m\}$.*

Using this fact, one can fashion an algorithm for Gröbner basis detection; see algorithm 8.1. The algorithm works in the following manner: from the normal cone of each vertex of M, choose an integer vector ω. The product of ω and the exponent vectors of $f_1, \ldots, f_m$ gives greatest weight to those terms whose exponent vectors sum to the given vertex of M. We then extend ω to a term ordering $\succ$ using theorem 7.9 on page 186. We calculate the S-polynomials with respect to $\succ$. If all the S-polynomials reduce to zero, we can report success with $\succ$; otherwise, we proceed to the next normal cone. If none of the normal cones produces a term ordering that gives us a Gröbner basis for $f_1, \ldots, f_m$, we can report that no such term ordering exists. We know that the algorithm terminates correctly, because there are finitely many vertices, hence finitely many normal cones from which to

Algorithm 8.1 GB_Detection_by_Minkowski_Sums

Inputs: $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$

Outputs: $\succ$ such that $\mathrm{GB}_{\succ}(f_1, \ldots, f_m)$ if such $\succ$ exists; `NULL` otherwise

$M \leftarrow N\left(N_{\mathrm{aff}}(f_1) + \cdots + N_{\mathrm{aff}}(f_m)\right)$

Compute $v_1, \ldots, v_r$, the vertices of M

Loop $k = 1, \ldots, r$

Pick c_k from the normal cone of v_k

Extend c_k to an admissible matrix $\mathcal{M}$

If $\mathrm{GB}_{\succ_{\mathcal{M}}}(f_1, \ldots, f_m)$ **Then**

Return $\succ_{\mathcal{M}}$

Return `NULL`

pick a representative, and because the weight vectors from these normal cones characterize the equivalence classes of term orderings completely.

Chapter 9

Gröbner basis detection of two polynomials by factoring

9.1. PROBLEM

We consider the following special case of the general Gröbner basis detection problem: an algorithm for

$$\exists \succ \quad \mathrm{GB}_{\succ}(f_1, f_2)$$

We present a new solution to this problem in section 9.3.1; it follows from theorem 9.1.

9.2. RESULT

THEOREM 9.1. *For all $f_1, f_2 \in \mathbb{F}[x_1, \ldots, x_n]$, for all term orderings $\succ$, the following are equivalent:*

(A) $\mathrm{GB}_{\succ}(f_1, f_2)$

(B) $\gcd\left(\overline{c_1}\,,\,\overline{c_2}\right) = 1$ *where* $f_1 = c_1 g$, $f_2 = c_2 g$ $\exists c_1, c_2, g \in \mathbb{F}[x_1, \ldots, x_n]$

A brief example before we prove the theorem.

EXAMPLE 9.2. Let $\succ_1$= lex (x, y), $\succ_2$= lex (b, x, y),and

$$f_1 = xy + bx \qquad f_2 = x^2 - bx$$

Note that

$$f_1 = x\,(y + b) \qquad f_2 = x\,(x - b)$$

The greatest common divisor of f_1, f_2 is $g = x$; its cofactors are

$$c_1 = y + b \qquad c_2 = x - b$$

Then

$$\mathrm{lt}_{\succ_1}(c_1) = y \qquad \mathrm{lt}_{\succ_1}(c_2) = x$$

while

$$\mathrm{lt}_{\succ_1}(c_1) = b \qquad \mathrm{lt}_{\succ}(c_2) = b$$

By theorem 9.1, f_1, f_2 are a Gröbner basis with respect to $\succ_1$, because the leading terms of c_1 and c_2 are relatively prime. Since the leading terms of c_1, c_2 are not relatively prime with respect to $\succ_2$, f_1, f_2 are not a Gröbner basis with respect to $\succ_2$. ◇

The proof of the theorem is short, because we unload the details into .

PROOF. (of theorem 9.1) Let $f_1, f_2, \succ$ be arbitrary, but fixed.

(B)⇒(A) is a consequence of lemma 1.37 on page 51; the requirement that S_{f_1,f_2} have a representation modulo f_1, f_2 is satisfied by the assumption of (B) that $\gcd(\overline{c_1}, \overline{c_2}) = 1$ and theorem 2.4 on page 59.

(A)⇒(B): Let f_1, f_2, $\succ$ be arbitrary but fixed. Assume $\mathrm{GB}_{\succ}(f_1, f_2)$. Then $\exists h_1, h_2$ such that h_1, h_2 give a representation of $S_{\succ}(f_1, f_2)$ modulo f_1, f_2. Recall σ_{12} and σ_{21} from definition 1.34 on page 48.

We have

$$S_{\succ}(f_1, f_2) = h_1 f_1 + h_2 f_2$$

$$\sigma_{12} f_1 - \sigma_{21} f_2 = h_1 f_1 + h_2 f_2$$

$$(\sigma_{12} - h_1) f_1 = (\sigma_{21} + h_2) f_2 \tag{9.1}$$

From lemma 1.36 on page 50,

$$\widehat{\sigma_{12} - h_1} = \sigma_{12} \qquad \widehat{\sigma_{21} + h_2} = \sigma_{21}$$

Write

$$c_1 = \sigma_{21} + h_2 \qquad c_2 = \sigma_{12} - h_1$$

From (9.1),

$$c_2 f_1 = c_1 f_2 \tag{9.2}$$

Observe that c_2 divides the left-hand side of (9.2), so it must divide the right-hand side. By 1.35 on page 49, their leading monomials σ_{12} and σ_{21} are relatively prime

on their indeterminates. So c_1 and c_2 have no common factors. Hence

$$c_1 \mid f_1 \quad \text{and} \quad c_2 \mid f_2$$

Let g_1, g_2 be such that

$$f_1 = c_1 g_1 \quad \text{and} \quad f_2 = c_2 g_2$$

Recall (9.2):

$$c_2 f_1 = c_1 f_2$$

$$c_2 \left(c_1 g_1 \right) = c_1 \left(c_2 g_2 \right)$$

$$g_1 = g_2$$

Let $g = g_1$; it is clear that

$$f_1 = c_1 g \quad \text{and} \quad f_2 = c_2 g$$

and

$$\gcd \left(\overline{c_1} \, , \, \overline{c_2} \right) = \gcd \left(\overline{\sigma_{21}} \, , \, \overline{\sigma_{12}} \right) = 1$$

as claimed. □

The proof of (A)⇒(B) has the following interesting corollary:

COROLLARY 9.3. *For all $f_1, f_2 \in \mathbb{F}[x_1, \ldots, x_n]$ and for all term orderings $\succ$, if h_1, h_2 give a representation of S_{f_1,f_2} modulo f_1, f_2, then*

$$\gcd \left(f_1, f_2 \right) = \frac{f_1}{\sigma_{21} + h_2} = \frac{f_2}{\sigma_{12} - h_1}$$

PROOF. Let $f_1, f_2, \succ$ be arbitrary, but fixed. We saw above that for some g,

$$f_1 = (\sigma_{21} + h_2) \cdot g$$

$$f_2 = (\sigma_{12} - h_1) \cdot g$$

We also observed that $\sigma_{21} + h_2$ and $\sigma_{12} - h_1$ were relatively prime. Thus g is the greatest common divisor of f_1, f_2. Dividing each equation by the cofactor of g gives corollary. □

9.3. APPLICATION OF RESULT

9.3.1. AN ALGORITHM FOR THEOREM 9.1. Theorem 9.1 tells us that two polynomials are a Gröbner basis with respect to a term ordering if and only if the leading terms of the cofactors of their greatest common divisor are relatively prime. For any pair of relatively prime terms taken from each cofactor, theorem 9.1 provides us with constraints like those of theorem 7.9 on page 186.

From theorem 7.9 we can find a matrix representation $\mathcal{M} \in \mathbb{Q}^n$ of a term ordering that satisfies the constraints – assuming such a term ordering exists. We rewrite the constraints as linear inequalities on the first row of $\mathcal{M}$ (called u in the theorem) and solve the inequalities. We fill the remaining rows of $\mathcal{M}$ with appropriately-chosen elementary row vectors.

We have outlined this as algorithm 9.1.

Algorithm 9.1 TO_for_GB

Inputs: $f_1, f_2 \in \mathbb{F}[x_1, \ldots, x_n]$

Output: $\succ$ such that $\mathrm{GB}_{\succ}(f_1, f_2)$ if such $\succ$ exists; `NULL` otherwise

$c_1 \leftarrow$ cofactor of $\gcd(f_1, f_2)$ in f_1

$c_2 \leftarrow$ cofactor of $\gcd(f_1, f_2)$ in f_2

$\mathcal{P} = \{(t_1, t_2) : t_k \text{ is a term of } c_k\}$

— remove pairs that are not relatively prime

For $p \in \mathcal{P}$

If $\gcd(t_1, t_2) \neq 1$ **Then**

$\mathcal{P} \leftarrow \mathcal{P} \backslash p$

— *search for the desired term ordering* $\succ$

For $p \in \mathcal{P}$

$\succ \leftarrow$ Exists_tord_with_given_leadterms(t_1, t_2, f_1, f_2)

If $\succ \neq$ `NULL` **Then**

Return $\succ$

— *if we get this far, no term ordering exists*

Return `NULL`

Algorithm 9.1 requires an additional algorithm, which we present as algorithm 9.2. Given t_1, t_2, f_1, f_2, this latter algorithm finds a term ordering such that $\overline{f_1} = t_1$ and $\overline{f_2} = t_2$, assuming such a term ordering exists. Note that the inequalities of algorithm 9.2 solve for a weight vector ω; to extend this to a full term ordering, we need to employ the technique indicated in the discussion at the end of section 7.3.

Algorithm 9.2 Exists_Tord_with_given_leadterms

Inputs: terms t_1, t_2, polynomials $f_1, f_2 \in \mathbb{F}[x_1, \ldots, x_n]$

Output: $\succ$ such that $t_1 = \mathrm{lt}_{\succ}(f_1)$, $t_2 = \mathrm{lt}_{\succ}(f_2)$ if such $\succ$ exists; `NULL` otherwise

For $i = 1, \ldots, n$

$\alpha_i \leftarrow \deg_{x_i} t_1$

$\beta_i \leftarrow \deg_{x_i} t_2$

$\mathcal{F}_1 \leftarrow \{u : u \text{ is a trailing term of } f_1\}$

$\mathcal{F}_2 \leftarrow \{v : v \text{ is a trailing term of } f_2\}$

$inequalities \leftarrow \{\}$

For $u \in \mathcal{F}_1$

For $i = 1, \ldots, n$

$\gamma_i \leftarrow \deg_{x_i} u$

$inequalities \leftarrow inequalities$

$$\cup \{\omega_1\alpha_1 + \cdots + \omega_n\alpha_n > \omega_1\gamma_1 + \cdots + \omega_n\gamma_n\}$$

For $v \in \mathcal{F}_2$

For $i = 1, \ldots, n$

$\gamma_i \leftarrow \deg_{x_i} v$

$inequalities \leftarrow inequalities$

$$\cup \{\omega_1\beta_1 + \cdots + \omega_n\beta_n > \omega_1\gamma_1 + \cdots + \omega_n\gamma_n\}$$

If $inequalities$ are feasible **Then**

Return solution of $inequalities$

Else

Return `NULL`

Algorithms 9.1 and 9.2 are unoptimized beyond the requirements of theorem 9.1. There is one obvious optimization: terms that divide other terms cannot possibly be leading terms. Hence they can be left out of the construction of $\mathcal{P}$ in algorithm 9.1 and of $\mathcal{F}_1$ and $\mathcal{F}_2$ in algorithm 9.2. Our Maple implementation **[HP04]** includes these optimizations.

9.3.2. EXAMPLES OF THEOREM 9.1.

EXAMPLE 9.4. Let

$$f_1 = x^2 + xy$$

$$f_2 = xy^2 + x$$

Is there a term ordering such that f_1, f_2 are a Gröbner basis? According to theorem 9.1, they are a Gröbner basis only if the cofactors of the greatest common divisor have relatively prime leading terms. Without going into too many details, we apply algorithm 9.1.

First we need the cofactors of the greatest common divisor of f_1 and f_2. Inspection shows that the greatest common divisor of f_1, f_2 is x; the cofactors are thus

$$c_1 = x + y$$

$$c_2 = y^2 + 1$$

Construct

$$\mathcal{P} = \left\{ \left(x, y^2\right), (x, 1), \left(y, y^2\right), (y, 1) \right\}$$

One pair is not relatively prime, so we can remove it:

$$\mathcal{P} = \left\{ \left(x, y^2\right), (x, 1), (y, 1) \right\}$$

Now we want a term ordering such that one of these pairs contains the leading terms of c_1, c_2. We know this is impossible for the last two pairs, since 1 cannot be the leading term of a non-constant polynomial. Thus, the question rests on whether there exists a term ordering $\succ$ such that

$$\mathrm{lt}_{\succ}(c_1) = x \qquad \mathrm{lt}_{\succ}(c_2) = y^2$$

Clearly lex (x, y) is one such term ordering. ——————————————————◇

In example 9.4, computing a Gröbner basis with one of the "routine" term orderings with $x \succ y$ (say a lexicographic or a total-degree term ordering) would have returned f_1, f_2. Even if we had tried computing a Gröbner basis with $y \succ x$, the resulting basis would have had only three elements.

The next example, by contrast, is a Gröbner basis with respect to "non-obvious" term orderings; a "bad" guess leads to a significant increase in the size of the Gröbner basis.

EXAMPLE 9.5. Let

$$f_1 = x^{22}y^8 + x^{20}y^8z - x^{22} - x^{20}z - x^2y^8 - y^8z + x^2 + z$$

$$f_2 = x^{10}y^{16}w + x^{11}y^{16}z + y^{16}w + xy^{16}z - x^{10}w - x^{11}z - w - xz$$

Again, we ask ourselves: is there a term ordering such that f_1, f_2 are a Gröbner basis? Again, we apply algorithm 9.1, but this time we will need the details.

First we need the cofactors of the greatest common divisor of f_1 and f_2. Since

$$f_1 = \left(x^{10} - 1\right)\left(x^2 + z\right)\left(x^{10} + 1\right)\left(y^8 - 1\right)$$

$$f_2 = \left(y^8 + 1\right)\left(xz + w\right)\left(x^{10} + 1\right)\left(y^8 - 1\right)$$

the cofactors of the greatest common divisor are

$$c_1 = \left(x^{10} - 1\right)\left(x^2 + z\right)$$

$$c_2 = \left(y^8 + 1\right)\left(xz + w\right)$$

Construct

$$\mathcal{P} = \left\{\left(x^{12}, xy^8z\right), \left(x^{12}, y^8w\right), \left(x^{10}z, xy^8z\right), \left(x^{10}z, y^8w\right)\right\}$$

(Recall that $1 \prec x^{10}$ and $1 \prec y^8$ for every term ordering $\succ$.) We eliminate the two that are not relatively prime; this leaves

$$\mathcal{P} = \left\{\left(x^{12}, y^8w\right), \left(x^{10}z, y^8w\right)\right\}$$

Now we turn to algorithm 9.2 to determine whether there is a term ordering such that either of these pairs contains the leading terms of c_1, c_2. Consider the expansions of c_1, c_2:

$$c_1 = x^{12} + x^{10}z - x^2 - z$$

$$c_2 = xy^8z + y^8w + xz + w$$

The first pair to try is (x^{12}, y^8w). We need

$$x^{12} \succ x^{10}z \quad \text{and} \quad x^{12} \succ x^2 \quad \text{and} \quad x^{12} \succ z$$

and

$$y^8w \succ xy^8z \quad \text{and} \quad y^8w \succ xz \quad \text{and} \quad y^8w \succ w$$

Recall that for any two terms t_1, t_2 we know $t_1 \mid t_2$ implies $t_1 \preceq t_2$. That means we can disregard four of the constraints on $\succ$, reducing the problem to:

$$x^{12} \succ x^{10}z$$

and

$$y^8w \succ xy^8z$$

By theorem 7.9 on page 186, such a term ordering exists if and only if we can find a weight vector ω that satisfies

$$\omega \cdot \begin{pmatrix} 12 & 0 & 0 & 0 \end{pmatrix}^T > \omega \cdot \begin{pmatrix} 10 & 0 & 1 & 0 \end{pmatrix}^T$$

and

$$\omega \cdot \begin{pmatrix} 0 & 8 & 0 & 1 \end{pmatrix}^T > \omega \cdot \begin{pmatrix} 1 & 8 & 1 & 0 \end{pmatrix}^T$$

That is,

$$12\omega_{(1)} > 10\omega_{(1)} + \omega_{(3)} \qquad \text{and} \qquad 8\omega_{(2)} + \omega_{(4)} > \omega_{(1)} + 8\omega_{(2)} + \omega_{(3)}$$

By lemma 7.12 on page 189, we can restrict our search to nonnegative values. So we want a solution to

$$\begin{aligned} 2\omega_{(1)} - \omega_{(3)} &> 0 \\ -\omega_{(1)} - \omega_{(3)} + \omega_{(4)} &> 0 \\ \omega_{(i)} &\geq 0 \qquad \text{for } i = 1, 2, 3, 4 \end{aligned}$$

We can solve this using the Fourier-Motzkin method. Eliminating m_{11}, we obtain

$$\begin{aligned} -3\omega_{(3)} + 2\omega_{(4)} &> 0 \\ -\omega_{(3)} + \omega_{(4)} &> 0 \\ \omega_{(i)} &\geq 0 \qquad \text{for } i = 2, 3, 4 \end{aligned}$$

Eliminating $\omega_{(3)}$, we have

$$\omega_{(4)} > 0$$

We will take $\omega_{(4)} = 1$.

Now for $\omega_{(3)}$. Back-substituting into the previous inequalities, we obtain

$$-3\omega_{(3)} + 2 > 0$$

$$-\omega_{(3)} + 1 > 0$$

$$\omega_{(3)} \geq 0$$

These are satisfied by $\omega_{(3)} = 0$.

The only restriction on $\omega_{(2)}$ is that it be nonnegative; we may choose $\omega_{(1)} = 0$.[1]

Finally, we want $\omega_{(1)}$. Back-substituting these values into the original system, we have

$$2\omega_{(1)} - 0 > 0$$

$$-\omega_{(1)} - 0 + 1 > 0$$

$$\omega_{(1)} \geq 0$$

This is equivalent to

$$0 < \omega_{(1)} < 1$$

This is satisfied by $\omega_{(1)} = 1/2$.

At this point, we know that a term ordering exists such that f_1, f_2 are a Gröbner basis, because we have found a weight vector ω that can serve as the first row of a matrix representation of a term ordering that, along with f_1, f_2, satisfies theorem

[1]We would not necessarily have been able to choose this, had our previous choices been $\omega_{(3)} = \omega_{(4)} = 0$. It is best to take a non-negative value as soon as possible.

9.1. We fill the remaining rows with elementary row vectors in such a way as to obtain a nonsingular matrix, as described at the end of chapter 9:

$$\mathcal{M} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

If we let $\succ$ be the term ordering having $\mathcal{M}$ as a matrix representation, then f_1, f_2 will be a Gröbner basis. Indeed,

$$S_{\mathcal{M}}(f_1, f_2) = h_1 f_1 + h_2 f_2$$

where

$$h_1 = -w - xy^8 z - xz$$

$$h_2 = x^{10} z - x^2 - z$$

and

$$\overline{h_1} \cdot \overline{f_1} = w \cdot x^{22} y^8$$

$$\overline{h_2} \cdot \overline{f_2} = x^{10} z \cdot x^{10} y^{16} w$$

which, with respect to $\succ_{\mathcal{M}}$, are less than

$$\operatorname{lcm}\left(\overline{f_1}, \overline{f_2}\right) = x^{22} y^{16} z w$$

(This becomes clear from comparing their weights with respect to the first row of $\mathcal{M}$.) Notice that the representation corresponds to the trailing terms of c_1, c_2, which is consistent with the proof of 2.4. (The reader will recall that theorem 2.4 is used in the proof of theorem 9.1.) ◇

Computing a Gröbner basis for f_1, f_2 of example 9.5 with Maple using either the term orderings tdeg (x, y, z, w) or plex (x, y, z, w) gives us a set of 13 or 14 polynomials (it depends on the polynomial). Different permutations of the variables gives us smaller sets; some give a set of only 2 polynomials. However, there is no clear way to guess which permutation of the variables gives us a "small" Gröbner basis, apart from the algorithm that we have described.

9.3.3. EXPERIMENTAL RESULTS. We conducted two kinds of tests: *unstructured* and *structured*.

UNSTRUCTURED TESTS. For these tests we ran the algorithm on randomly-generated polynomials. We timed the algorithm and kept track of how many times we detected a Gröbner basis. We ran three different tests, varying both the number of terms, the total degree of each term, and the number of indeterminates.

All the random polynomials had the following features in common:

- coefficients were random, over $-99 \ldots 99$
- exponents for indeterminates were random, over $0 \ldots 5$

Table 9.1: Number of times we detected a Gröbner basis for f_1, f_2 (six terms of total degree six).

# vars	# pairs	# detections	time per test
2	1000	80	.10s
3	1000	275	.23s
4	1000	489	.48s
5	1000	670	.76s
6	1000	800	0.98s
7	1000	889	1.43s

This leaves it to the experiment to specify the number of indeterminates, the number of terms, and their total degree, and we experimented with each of these values.

For the data in table 9.1, we kept the number of terms and the total degree fixed, varying only the number of indeterminates. As the number increases, the number of detections skyrocket. By the time we reach $n = 7$ indeterminates, we are detecting a Gröbner basis for the vast majority of the generated polynomials. *Why?* Maple's `randpoly()` appears to generate terms in such a way as to favor single-indeterminate terms when the total degree is not much higher than the maximum power of an indeterminate. The resulting polynomials have a large number of terms in only one indeterminate, so that the polynomials are prime. It is unlikely that a corresponding percentage of real-world polynomial systems would look like this, since most real-world problems have some sort of structure; nevertheless, the data give us some idea about the possibility for success in these cases.

Table 9.2: Number of times we detected a Gröbner basis for f_1, f_2 (10% sparse, total degree 6).

# vars	# pairs	# detections	time per test
2	1000	159	.05s
3	1000	296	.41s
4	1000	569	7.50s
5	1000	855	94.83s

The data of table 9.2 varied the number of terms, while keeping the total degree constant. The number of terms was kept at 10% sparsity, by which we mean

$$.1 \times \left(\begin{array}{c} \text{\# vars} + \text{degree} \\ \\ \text{degree} \end{array} \right) \tag{9.3}$$

With the total degree fixed at six, this gives us three terms for $n = 2$ variables, nine terms for $n = 3$, twenty-one terms for $n = 4$, and forty-six terms for $n = 5$. We did not proceed beyond $n = 5$ since at that point it was taking a long time to complete the tests (94.83 seconds on average).

Despite the increased number of terms, the number of detections continues to skyrocket; in fact, we find *even more* detections for a given n than in table 9.1. We believe that this is due to the fixed low total degree of each polynomial (later data will bear this out). It is useful to observe how the time per test also skyrocketed. Since most randomly-generated polynomials will be relatively prime, we believe that this increase in time is due to the increased complexity of solving the associated system of linear inequalities (there are more than 80 inequalities for $n = 5$).

Table 9.3: Number of times we detected a Gröbner basis for f_1, f_2 (six terms of total degree 6×#vars).

# vars	# pairs	# detections	avg time per test (s)
2	1000	45	.06
3	1000	56	.09
4	1000	32	.09
5	1000	21	.08
6	1000	3	.09
7	1000	0	.11

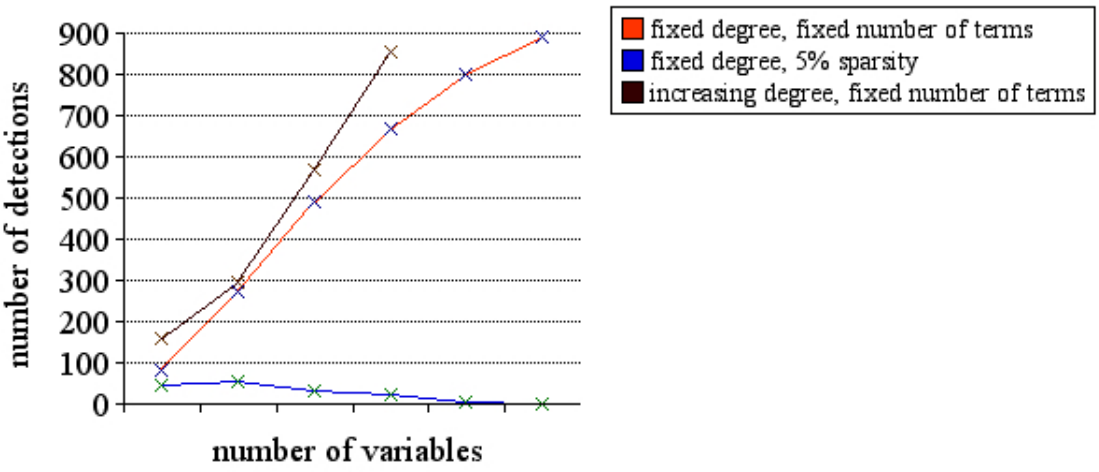


Figure 9.1: Summary of the number of detections of Gröbner bases for different cases of unstructured systems.

For the data in table 9.3, we fixed the number of terms again, but varied their total degree. Without the low value for the total degree, the number of detected Gröbner bases plummets not merely from the heights of tables 9.1 and 9.2, but to the point where we no longer detect *any* Gröbner bases for $n = 7$. This is because Maple's `randpoly()` function is much less likely to generate terms of one variable

Table 9.4: Number of times we detected a Gröbner basis for gc_1, gc_2 (three terms in each of g, c_1, c_2; maximum degree per term is 10).

# vars	# pairs	# detections	average time per test
2	1000	127	0.000418
3	1000	189	0.010091
4	1000	269	0.023830
5	1000	265	0.048970
6	1000	251	0.100545
7	1000	239	0.158870

with the increased total degree. Correspondingly, the average time per test grows very slowly.

STRUCTURED TESTS. Erich Kaltofen suggested the following tests. Since we know that the algorithm works for pairs of polynomials that have a common divisor, and since it is unlikely that we will generate many such polynomials using the `randpoly()` function, we can generate three random polynomials g, c_1, c_2, then expand $f_1 = c_1 g$, $f_2 = c_2 g$, and try the algorithm on these. All the polynomials had these features in common:

- random coefficients, range $-99 \ldots 99$
- random power on each variable, range $0 \ldots 5$

This leaves the number of indeterminates, the number of terms, and the maximum degree per term free for the experiment.

For the data in table 9.4, we kept the number of terms of g, c_1, c_2 fixed at three, and the maximum degree per term fixed at ten. Once again we find the number of detections increasing as we increase the number of variables. Again, we expect

Table 9.5: Number of times we detected a Gröbner basis for gc_1, gc_2 (number of terms in each of g, c_1, c_2 fixed at 5% sparsity, minimum two terms for c_1, c_2; maximum degree per term is 10).

# vars	# pairs	# detections	average time per test
2	1000	237	0.028550
3	1000	344	0.041150
4	1000	350	0.050120
5	1000	340	0.077490
6	1000	331	0.071000
7	1000	283	0.075450

that this is due to the fixed total degree. We find that the number of detections does not vary so much as for the unstructured polynomials: from a low of 13%, we reach a plateau of 30%, compared to a low of 8% and a high of 89% in table 9.4.

Of course, the data of table 9.4 are not entirely comparable to previous tests. This is due to differences in the polynomials generated; for example, the polynomials in the unstructured case were almost always relatively prime, whereas the polynomials in the structured case are *never* relatively prime. Also, we might not always have six terms in each of f_1, f_2; we would expect fewer terms on occasion, due to simplification.

For table 9.5, we kept the maximum degree of the polynomials fixed, while increasing the number of terms of g, c_1, c_2 to reflect a sparsity of 5%. We used the formula of equation (9.3) on page 225. For a low number of variables, however, this meant that f_1, f_2 were always monomials; to avoid that, we restricted c_1, c_2 to a minimum of two terms.

Table 9.6: Number of times we detected a Gröbner basis for gc_1, gc_2 (three terms in each of g, c_1, c_2; maximum degree per term is 10×#vars).

# vars	# pairs	# detections	average time per test
2	1000	133	0.017440
3	1000	197	0.049060
4	1000	239	0.089670
5	1000	252	0.139160
6	1000	276	0.259470
7	1000	270	0.361990

There is not very much change in the number of detections, nor do the numbers vary much. We go from a low of 20% to a high of 40%, but unlike 9.2, the average time per test remains low. This is probably because f_1, f_2 are guaranteed to factor, and the cofactors thus have fewer terms than did those of the unstructured polynomials of table 9.2. Fewer terms means fewer inequalities, which means a faster solution.

In our final test, we fixed g, c_1, c_2 at three terms, and we increased the maximum degree per term. When we did the same for the unstructured polynomials of table 9.3, we encountered a catastrophic drop in the number of Gröbner basis detections. This time, however, the numbers do not vary much. The only significant difference from tables 9.4 and 9.5 is for $n = 2$ indeterminates; we have only 8 detections out of 100 random polynomials, a value much lower than in the two previous experiments.

In any case, we detect a high proportion of Gröbner bases for both structured and unstructured polynomials. In the structured case, adjusting the sparsity, the

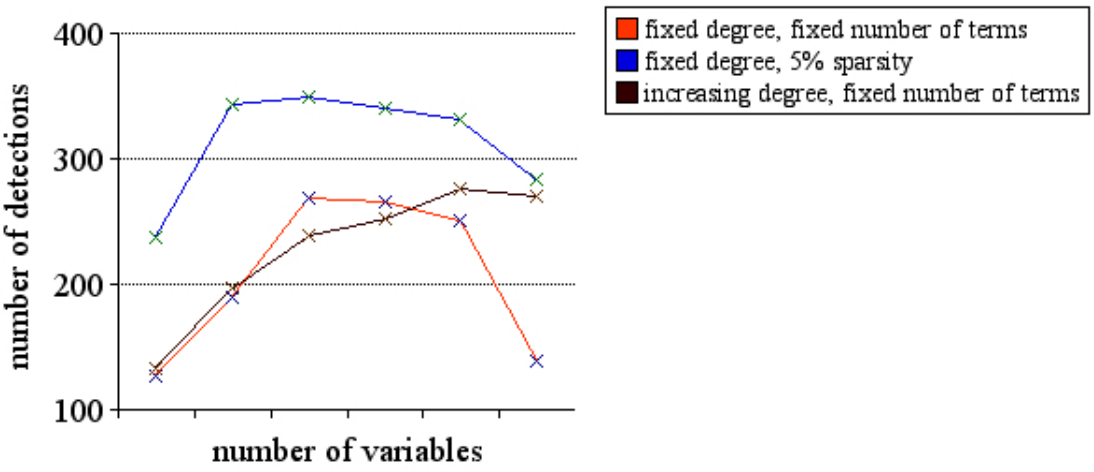


Figure 9.2: Summary of the number of detections of Gröbner bases for different cases of structured systems.

total degree, and the number of variables appears to keep the behavior fairly consistent; see figure 9.2.

A natural question to ask is, how does Gröbner basis *detection* compare to the Gröbner basis *computation?* Certainly, computing a Gröbner basis always terminates successfully with a Gröbner basis, whereas we will not always detect a Gröbner basis for given $f_1, \ldots, f_m$. Hence, there is a certain advantage to computing a Gröbner basis. On the other hand, we can find a term ordering for a Gröbner basis not infrequently; it would be useful to compare running times in these cases.

While running the experiments documented in tables 9.4, 9.5, and 9.6, we calculated the corresponding Gröbner basis for systems where we succeeded in detecting a Gröbner basis. We noted how many polynomials were in the final result, as well as the time needed to compute the basis. We used Maple's `gbasis()`

Table 9.7: Detection compared to computation: fixed number of terms and fixed total degree.

# vars	time to detect	time to compute	size of GB	avg size of GB
2	0.000418	.025260	2..9	2.8
3	0.010091	3.329418	2..21	5.2
4	0.023830	5.494907	2..40	5.9
5	0.048970	5.565019	2..48	6.0
6	0.100545	.612988	2..41	6.6
7	0.158870	.515607	2..28	5.9

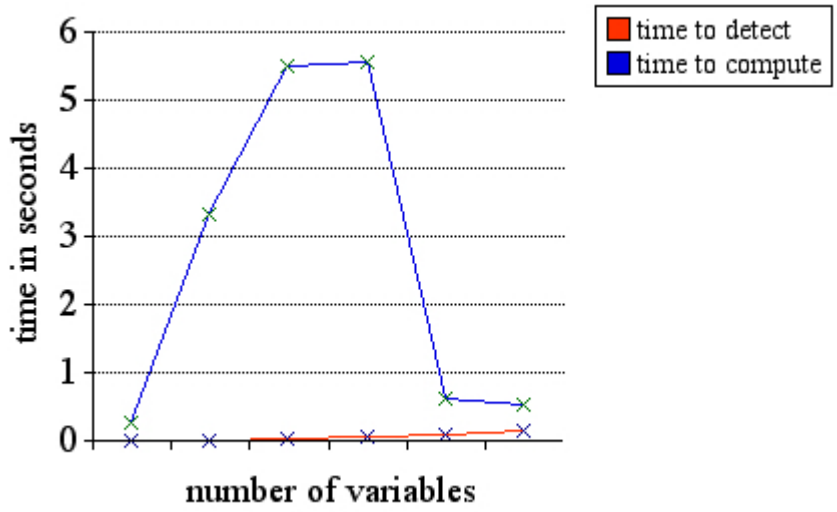


Figure 9.3: Detection compared to computation (chart of times): fixed number of terms and fixed total degree.

command to compute the basis with respect to the total degree term ordering; the general opinion of most researchers is that this ordering gives very good performance when computing a Gröbner basis (see also [**Tra05**]). We present the data in tables 9.7, 9.8, and 9.9. With only one exception, it always takes longer – and usually *much* longer – to compute the Gröbner basis than to detect it. The average

Table 9.8: Detection compared to computation: fixed sparsity of terms and fixed total degree.

# vars	time to detect	time to compute	size of GB	avg size of GB
2	0.028550	.024430	1..5	2.5
3	0.041150	.058634	2..14	3.8
4	0.050120	.105714	2..18	4.3
5	0.077490	.086529	2..23	4.7
6	0.071000	.134230	1..26	4.5
7	0.075450	.121625	2..23	4.5

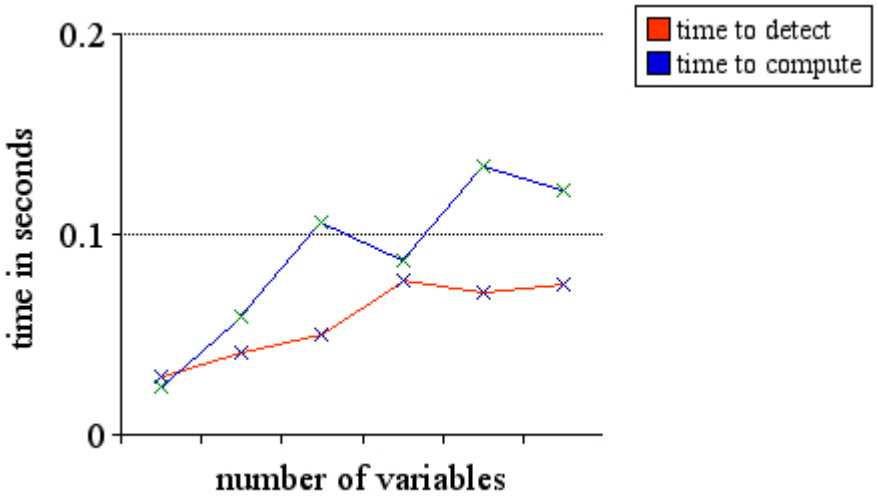


Figure 9.4: Detection compared to computation (chart of times): 5% sparsity of terms and fixed total degree.

Table 9.9: Detection compared to computation: fixed number of terms and increasing total degree.

# vars	time to detect	time to compute	size of GB	avg size of GB
2	0.017440	.186617	2..9	2.9
3	0.049060	15.701117	2..25	4.8
4	0.089670	20.773808	2..59	6.2
5	0.139160	1.420317	2..43	6.8
6	0.259470	31.433587	2..37	6.5
7	0.361990	16.906481	2..34	6.1

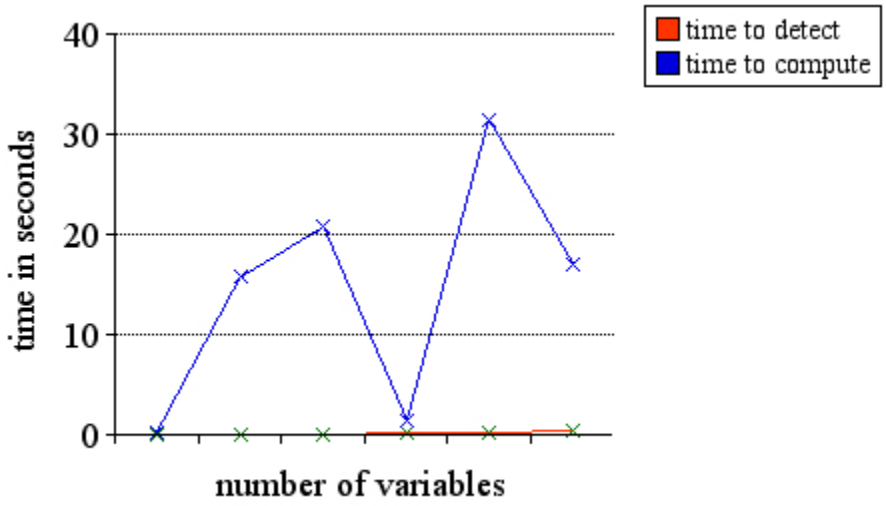


Figure 9.5: Detection compared to computation: fixed (chart of times): fixed number of terms and increasing total degree.

time for detection grows relatively consistently, whereas the average time for computation varies wildly, with the exception of table 9.8. This is possibly due to what one might call the occasional "unlucky" systems, whose Gröbner bases grow large out of proportion to most others. Moreover, there are always two polynomials in a detected basis, whereas the number of polynomials in a computed basis ranges from as few as two (if we're lucky) to as many as sixty-nine (if we're not).

We also computed Gröbner bases for the occasions when we did not detect a Gröbner basis, and compared the running times. The average time to compute a Gröbner basis was again much longer than the time to *fail* to detect one: again, this is possibly due to unlucky systems.

The data suggest that Gröbner basis detection could be a viable starting point for future optimization of Gröbner basis algorithms. Further research to generalize the algorithms to a larger number of polynomials could be worthwhile.

Conclusion

We have presented combinatorial criteria that allow us to skip:

- all S-polynomial reductions;
- all but one S-polynomial reductions;
- all but two S-polynomial reductions, for a set of three polynomials f_1, f_2, f_3.

We also presented a new method for Gröbner basis detection for a set of two polynomials f_1, f_2.

Directions for future research are clear. *First*, we have the opportunity to generalize the combinatorial criteria that allow us to skip all but two S-polynomial reductions. There are two possible paths:

- for $m > 3$, find criteria that allow us to skip all but two S-polynomial reductions;
- for $m > 3$, find criteria that allow us to skip exactly one S-polynomial reduction.

These two paths coincide when $m = 3$.

I have carried out some research on skipping all but two S-polynomial reductions for $m > 3$, but so far I cannot even hazard a guess as to what the solution might be.

Second, we have the opportunity to generalize the method of Gröbner basis reduction to $m > 2$ polynomials. Originally, I believed that this would be based on combinatorial criteria, just as theorem 9.1 on page 209 depends on Buchberger's first criterion. For a while, I believed that the solution embodied in theorem 6.3 on page 124 (the new combinatorial criterion) would help formulate a characterization of Gröbner bases consisting of three polynomials. Subsequent research has revealed that this is *not* the case, so we are back at square one.

Third, we have the opportunity to implement the method of Gritzmann and Sturmfels, and compare its performance on sets of two polynomials to the method we lay out in chapter 9. This will require the use of a computational package that can *efficiently* compute Minkowski sums of polytopes and their polyhedra, as well as pick representative weight vectors from the normal cones of the vertices of a polyhedron. The Convex package [**Fra04**] is a possible candidate; however, the documentation indicates that its implementation of Minkowski sums is "trivial, hence slow." I expect that I will have to spend some time researching ways to optimize this code and contribute to this project – or else, find a different package.

Bibliography

[BS87] Dave Bayer and Mike Stillman, *A criterion for detecting m-regularity*, Inventiones Mathematicae **87** (1987), no. 1, 1–11.

[Buc65] Bruno Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalem Polynomideal (an algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal)*, Ph.D. thesis, Mathematical Insitute, University of Innsbruck, Austria, 1965, English translation to appear in the Journal of Symbolic Computation.

[Buc79] ———, *A criterion for detecting unnecessary reductions in the construction of Gröbner bases*, Proceedings of the EUROSAM 79 Symposium on Symbolic and Algebraic Manipulation, Marseille, June 26-28, 1979 (Berlin - Heidelberg - New York) (E. W. Ng, ed.), Lecture Notes in Computer Science, vol. 72, Springer, 1979, pp. 3–21.

[BWK93] Thomas Becker, Volker Weispfenning, and Hans Kredel, *Gröbner bases: a computational approach to commutative algebra*, Springer-Verlag New York, Inc., New York, 1993.

[CKM97] Stéphane Collart, Michael Kalkbrenner, and Daniel Mall, *Converting bases with the Gröbner walk*, Journal of Symbolic Computation **24** (1997), no. 3–4, 465–469.

[CKR02] Massimo Caboara, Martin Kreuzer, and Lorenzo Robbiano, *Minimal sets of critical pairs*, Proceedings of the First Congress of Mathematical Software (B. Cohen, X. Gao, and N. Takayama, eds.), World Scientific, 2002, pp. 390–404.

[CLO97] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, second ed., Springer-Verlag New York, Inc., New York, 1997.

[CLO98] ———, *Using algebraic geometry*, Springer-Verlag New York, Inc., New York, 1998.

[Coh03] Joel Cohen, *Computer algebra and symbolic computation: Mathematical methods*, A K Peters, Ltd., Natick, MA, 2003.

[Eis95] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag New York, Inc., New York, 1995.

[Fau99] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*, Journal of Pure and Applied Algebra **139** (1999), no. 1-3, 61–88.

[Fau02] ———, *A new efficient algorithm for computing Gröbner bases without reduction to zero F5*, International Symposium on Symbolic and Algebraic Computation Symposium - ISSAC 2002, Villeneuve d'Ascq, France, Jul 2002.

[FGLM93] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, Journal of Symbolic Computation **16** (1993), no. 4, 329–344.

[Fra04] Matthias Franz, *Convex: a Maple package for convex geometry, version 1.1*, 2004, Maple worksheet available at `http://www-fourier.ujf-grenoble.fr/~franz/convex/`.

[GM88] Rudiger Gebauer and Hans Möller, *On an installation of Buchberger's algorithm*, Journal of Symbolic Computation **6** (1988), 275–286.

[GS93] Peter Gritzmann and Bernd Sturmfels, *Minkowski addition of polytopes: Computational complexity and applications to Gröbner bases*, SIAM J. Disc. Math **6** (1993), no. 2, 246–269.

[Hon98] Hoon Hong, *Gröbner basis under composition I*, Journal of Symbolic Computation **25** (1998), 643–663.

[HP04] Hoon Hong and John Perry, *Gröbner basis detection*, 2004, Maple worksheet available at `http://www4.ncsu.edu/~jeperry/Research/GBDetection.mw`.

[HW99] Hoon Hong and Volker Weispfenning, *Algorithmic theory of admissible term orders*, available at `http://www.math.ncsu.edu/~hong/`, 1999.

[KR00] Martin Kreuzer and Lorenzo Robbiano, *Computational commutative algebra I*, Springer-Verlag, Heidelberg, 2000.

[MR88] Teo Mora and Lorenzo Robbiano, *The Gröbner fan of an ideal*, Journal of Symbolic Computation **6** (1988), 183–208.

[Per94] John Perry, *GraphDQ*, 1994, binary code (AmigaOS) available at `http://wuarchive.wustl.edu/aminet/misc/math/graphdq.lha`.

[Rob86] Lorenzo Robbiano, *On the theory of graded structures*, Journal of Symbolic Computation **2** (1986), 139–170.

[SW97] Bernd Sturmfels and Markus Wiegelmann, *Structural Gröbner basis detection*, Applicable Algebra in Engineering, Communication and Computing **8** (1997), 257–263.

[Tra05] Quoc-Nam Tran, *Ideal-specified term orders for elimination and applications in implicitization*, Proceedings of the Tenth International Conference on Applications of Computer Algebra (Beaumont, TX), International Scientific Committee for Applications of Computer Algebra, 2005, Selected papers to appear in a forthcoming issue of the Journal of Symbolic Computation, pp. 15–24.

[vzGG99] Joachim von zur Gathen and Jurgen Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 1999.

[Wei87] Volker Weispfenning, *Admissible orderings and linear forms*, ACM SIGSAM Bulletin **21** (1987), no. 2, 16–18.

[Woo04] Chi Woo, *Planetmath.org*, 2004, online encyclopedia article available at `http://planetmath.org/encyclopedia/Indeterminate.html`.

Index

admissible matrix, 172
  equivalence, 187
  of $\succ$, 174
algorithms
  Can_Skip_All_But_One_SPolys, 110
  Can_Skip_All_SPolys, 90
  Can_Skip_Third_Spoly, 148
  Exists_Tord_with_given_leadterms, 215
  GB_Detection_by_Minkowski_Sums, 208
  Implied_GB, 58
  Is_GB, 35
  Tord_for_GB, 214

Buchberger's criteria
  allow us to skip S-polynomial reduction, 59
  first criterion, 59, 69
    term diagram, 74
  second criterion, 62, 69
    does not guarantee reduction to zero, 68
    term diagram, 75
  variablewise, 123

coefficient, 8
  leading coefficient, 12
combinatorial criterion, 58
  Buchberger's criteria, *see* Buchberger's criteria
  complete, 80
  existence of non-Buchberger criteria, 149

exponent vectors, 172

Gröbner basis, 19
  equivalent conditions, 34
Gröbner basis detection, 168

indeterminate, 8

leading coefficient, 12
leading monomial, 12
leading term, 12
lex term ordering, 11

Minkowski sum, 203
monomial, 8
  leading monomial, 12

Newton polyhedron, 202
Newton polytope, 201
normal cone, 204

reduction, 16
  implies representation, 30
  relationship with representation, 29–31
representation
  does not imply reduction, 31
  relationship with reduction, 29–31
representation of an S-polynomial, 28

S-polynomial
  parallel with Gaussian elimination, 24
Skipping S-polynomial reduction
  not equivalent to reduction to zero, 57
skipping S-polynomial reduction, 55
  allowed by Buchberger's criteria, 59
  experimental results, 117
  theorems, 87, 102, 124

tdeg term ordering, 14
term, 8
  leading term, 12
term diagrams, 71, 75
  Buchberger's first criterion, 74
  locating greatest common divisor and least common multiple, 73
  shading for divisible terms, 73
term ordering, 9
  admissible, 9
  as shorthand for admissible term ordering, 9
  equivalence, 206
  lexicographic, 11
  properties, 15
  total-degree, 14

variable, 8

weight, 174