REFERENCES

[1] T. Becker and V. Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra.* Graduate Texts in Mathematics. Springer-Verlag, New York, 1993.

[2] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[3] J. H. Davenport, Y. Siret, and E. Tournier. *Computer Algebra.* Academic Press, New York, 1988.

[4] T. W. Hungerford. *Algebra.* Graduate Texts in Mathematics. Springer-Verlag, New York, 1974.

[5] M. Mignotte. *Mathematics for Computer Algebra.* Springer-Verlag, New York, 1992.

[6] D. Pedoe. *Geometry: A Comprehensive Course.* Dover Publications, Inc, New York, 1970.

[7] V. Weispfenning. Comprehensive Gröbner bases. *Journal of Symbolic Computation*, 14:1–29, 1992.

of succession, each of these is a successor of γ) needed to determine k. So, for all $\beta \in \Delta$ either $\mathrm{HM}_\beta(k)$ is defined (and *red*) or all terms of k are *green*.

For each conditon β that gives k at least one *red* term, the algorithm replaces the current triple $(\delta, G, U) \in RD$ with $(\beta, \emptyset, G \cup U \cup \{\mathrm{col}^0_\beta(k)\})$. Hence, it replaces f by its "nonzero" remainder modulo $G - \{f\}$. Note that, by the ordering in 1.4,

$$\min(G \cup U' \cup \{\mathrm{col}^0_\beta(k)\}) < \min(U).$$

For each condition β that makes all terms of k *green*, the algorithm replaces the current triple (δ, G, U) with just $(\beta, G, U - \{f\})$. Under β, the remainder of f modulo G is zero. Hence, f is in the ideal generated by G. Therefore, it is not necessary to make f a generator. Note here also that $|U'| < |U|$.

The algorithm makes a finitely branching tree of triples. If the routine never terminated, there would at least one infinite branch $b = \{(\delta_i, G_i, U_i)\}$. But, by our observations above, if $(\delta_{i+1}, G_{i+1}, U_{i+1})$ follows (δ_i, G_i, U_i) in the tree, then either $|U_{i+1}| < |U_i|$ or $\min(U_{i+1}) < \min(U_i)$. Since both $<$ on the cardinal numbers $|A|$ and $<$ of section 1.4 are well-orderings, the branch b cannot be infinite. **End**

Once the algorithm to reduce one Groebner Pair is in place, it is a simple matter to write the algorithm to reduce all pairs of a given Groebner system $GS = \{(\gamma, G)\}$, see table B.2.

Table B.2, Algorithm **REDUCE SYSTEM**

Input: Groebner System $GS = \{(\gamma, G)\}$
Output: Groebner System with each Pair of GS reduced

$RD\_SYS := \bigcup_{(\gamma,G)\in GS}$ **REDUCE PAIR**(γ, G)
Return(RD_SYS)

Correctness and termination of this algorithm are clear.

In this case, replace **NORMALFORM** with **GCD-NORMALFORM**, replace **DET1** with **SAT DET1**, and replace $\mathrm{col}^0_\gamma(f)$ with $\mathrm{col}^1_\gamma(f)$ in **REDUCE PAIR**.

Analysis of REDUCE PAIR: Initialization step: set the flag

Finished_all_reductions

to false, and set RD to $\{(\gamma, \emptyset, G)\}$ using the input Groebner pair (γ, G). For reference, denote this input pair by (γ_0, G_0).

The algorithm stops when all triples of the form (δ, G, U) in RD have the set U empty. Given any triple (δ, G, U), it is a loop invariant that the sets G and U are both determined by δ, and that δ is a successor condition to γ_0. We may think of the set U as a list of generators for an unreduced Groebner Basis of G_0 and the set G as a holding place for the generators of a reduced Groebner Basis of G_0. The algorithm transfers "reduced" polynomials from U into G. We now describe how this works.

The algorithm first searches the list RD for a triple (δ, G, U) with U nonempty. It then takes f to be a minimal element of U, rebinds U to U' (without this f), and computes the normal form, k, of f with respect to divisors $G \cup U' = G \cup (U - \{f\})$ and conditon δ.

If the normal form $k = f$, then, by definition of normal form in section 1.4, this means that no monomial of f is divisible by *any* conditional head monomial $\mathrm{HM}_\delta(p)$, $p \in G \cup U - \{f\}$. We define (see also [2] pg. 91) an f with this property to be *reduced* for the divisor list. The algorithm then updates RD by replacing the current triple (δ, G, U) with $(\delta, G \cup \{f\}, U')$. Note that G now contains an element that is reduced for $G \cup U'$. Also note $|U'| < |U|$. The algorithm modifies G_0 so that all elements are reduced, but with the added feature that it keeps record of any and all extra conditions needed to do the reductions.

If $k \neq f$, the routine then determines if k has any *red* "nonzero" terms according to the condition δ. The set Δ will contain all successors to δ (and by transitivity

Table B.1, Algorithm **REDUCE PAIR**

Input: Groebner Pair (γ, G), with $\mathrm{HM}_\gamma(g)$ defined $\forall g \in G$
Output: List of pairs $\{(\delta, G')\}$ with stated properties

Finished_all_reductions:= false
$RD := \{(\gamma, \emptyset, G)\}$
WHILE Finished_all_reductions = false **DO**
  $RD1 := \{(\delta, G, U) \in RD \,|\, U \neq \emptyset\}$
  IF $RD1 = \emptyset$ **THEN**
    Finished_all_reductions:= true
  ELSE
    (δ, G, U):= first$(RD1)$
    $RD := RD - \{(\delta, G, U)\}$
  IF Finished_all_reductions = false **THEN**
    f:= some minimal element of U
    $U' := U - \{f\}$
    k:= **NORMALFORM**$(\delta, f, G \cup U')$
    IF $f = k$ **THEN**
      $RD := RD \cup \{(\delta, G \cup \{f\}, U')\}$
    ELSE
      Δ:= **DET1**(δ, k)
      $RD := RD$

$$\bigcup_{\{\beta \in \Delta \,|\, T_{red,\beta}(\mathrm{col}^0_\beta(k)) \neq \emptyset\}} \{(\beta, \emptyset, G \cup U' \cup \{\mathrm{col}^0_\beta\})\}$$

$$\bigcup_{\{\beta \in \Delta \,|\, T_{red,\beta}(\mathrm{col}^0_\beta(k)) = \emptyset\}} \{(\beta, G, U')\}$$

Return(RD)

APPENDIX B Reduction algorithm of Volker Weispfenning

For completeness of this dissertation, tables B.1 and B.2 of this section give the reduction algorithm of V. Weispfenning [7]. We implemented this algorithm without substantial changes. The input to the algorithm is a Groeber Pair (γ, G) as defined in section 1.5 of Chapter 1, with the additional property that

$$\mathrm{HM}_\gamma(g) \text{ is defined for all } g \in G.$$

The output is a list of pairs (δ, G') where

(i) δ is a successor to γ,

(ii) G' is determined by δ,

(iii) all elements g of G' have $\mathrm{HM}_\delta(g)$ defined,

(iv) G' gives a Groebner Basis for the ideal $\langle G \rangle$, and

(v) for all $p \in G'$, no monomial of p is in the monomial ideal

$$\langle \mathrm{HM}_\delta(G' - \{p\}) \rangle.$$

Consequently, for all specializations $\sigma \in \Sigma_\delta$, $\sigma(G')$ is a reduced Groebner Basis for the ideal $\langle \sigma(G') \rangle$ in $k[x_1, \ldots, x_n]$.

In the algorithm, we take a minimal element of a set of polynomials U in parameters. This minimum is taken with respect to the ordering described in section 1.4. Recall that this ordering examined sets of monomials of two given polynomials. A polynomial f was then declared to be greater than another polynomial g provided there was some monomial $a \cdot t$ of the set of monomials of f which was greater than the maximal of monomials in the set of monomials of g (after all monomial equalites are recursively removed).

For efficiency, one may restrict the computations to polynomials in

$$k[u_1, \ldots, u_m][x_1, \ldots, x_n].$$

To perform the colored arithmetic, we combine colors according to the coloring rules of chapter 1, e.g. $red + green = red$, etc. Coefficients a_α, a_β are added in the usual way for rational functions. Finally, like terms are collected by multindicies, and the coefficients are collected and colored accordingly. If two terms are multiplied together, the multiindicies are added vectorially.

APPENDIX A Representations of Colored Polynomials and Arithmetic

Given a polynomial $f = \sum a_\alpha x^\alpha$, in our MACSYMA implementation we first have a function called "internal form" which takes f and converts it to a list of the form:

$$f = [\ldots, [[color], [a_\alpha], [\alpha]], \ldots]$$

where *color* is one of the character strings *green, red, white*. This list is kept as an ordered list using some given monomial ordering on the multindicies α. When a polynomial is initially put into this form, all terms have their color set to *white* by default. Now, MACSYMA may be viewed as a Lisp interpreter. Hence, we wrote our prototype algorithms to operate on these ordered lists of polynomials. Professor Marek R. Rychlik then ported this code to Lisp for more speed and efficiency.

Now suppose that a condition γ has been given. To "color" the internal form of a polynomial f, we examine each a_α of each term

$$[[color], [a_\alpha], [\alpha]]$$

and assign it a color using either $\mathrm{col}^0_\gamma(a_\alpha)$ in chapter 1 or $\mathrm{col}^1_\gamma(a_\alpha)$ in chapter 2.

To create the conditional part of a polynomial colored by γ, we simply delete all terms from the internal form whose color entry is *green*.

To "recolor" a polynomial in internal form with respect to a successor condition, δ, of a condition γ, we just color the terms left *white* by γ. The other terms will have previously had their colors assigned by γ.

To obtain the conditional head term of a polynomial with a well-defind head term, we simply scan through the list of terms (past all the *green* terms) until we come to the first term whose color slot is *red*.

CLOSED:= CLOSED $\cup\{(\gamma, G)\}$

OPEN:= $\emptyset$.

The algorithm will then terminate the first time it generates a Groebner Pair (γ, G) such that dim $\mathbf{V}(\langle G\rangle)$ exceeds the bound.

Example 3.4.3 Let $I = \langle x + y, x + ty\rangle \subset k(t)[x, y]$ with $x > y$ from section 1.5. Take $B = \{\gamma\} = \{(\{\}, \{\})\}$, and set the dimension bound $D = 1$. The **PARTIAL GROEBNERSYSTEM** output is

$$\{((\{\}, \{1 - t\}), \{x + y, x + ty, (1 - t)y\}, 0), ((\{1 - t\}, \{\}), \{x + y, x + ty\})\}.$$

The first triple indicates that the dimension of $\mathbf{V}(I)$ is zero for all specializations of parameters with $t \neq 1$. The second pair indicates that the dimension of $\mathbf{V}(I)$ is greater than or equal to the bound D.

for γ to be such that some one of these will be a nonzero field constant. In any event, **DIMBOUND** will return the appropriate dimension d (see its analysis). If $d < D$, then we push the (γ, G), with d included, out to the CLOSED list. The algorithm returns a list of triples of the forms either (γ, G, d) or (γ, G). The pair (γ, G) will be a Groebner Pair and have the property that dim $\mathbf{V}(\langle G \rangle) \geq D$. Thus, one will be able to see at a glance those cases for which the dimension exceeds the bound D. The lists G in triples of the form (γ, G, d) where $d < D$ are generating sets for I but not necessarily Groebner Bases (since these may get pushed out of the algorithm at an early stage). The algorithm terminates for the same reasons as those of **GROBNERSYSTEM**. **End**

The **PARTIAL GROEBNERSYSTEM** algorithm is useful for solving the following type of problem: suppose that $I = \langle f_1, \ldots, f_n \rangle \subset S$ and one wants to know if dim $V = \mathbf{V}(I)$ is always smaller than some prescribed bound D under all specializations of the parameters in the coefficients of the f_i. If the output of our algorithm consists solely of the triples of the form (γ, G, d), then dim V is always smaller than D. If the output contains some Groebner pairs (γ, G), then we obtain information regarding those specializations of parameters $\sigma \in S_\gamma$ for which the dimension of V exceeds the bound. One can, and we did, modify the algorithm slightly so that it would stop once it calculated a triple (γ, G, P) for which the dimension of $\mathbf{V}(\langle G \rangle)$ exceeded the given bound. This is helpful if one does not wish to compute the entire partial Groebner system. The modification is to replace the lines

ELSE

CLOSED:= CLOSED $\cup\{(\gamma, G)\}$

with the lines

ELSE

Table 3.2, Algorithm **PARTIAL GROEBNERSYSTEM**

Input: Case Distinction B, list of polynomials $F = \{f_1, \ldots, f_n\}$, monomial order $\leq$, dimension bound D. Output: $GS = \{(\gamma, G)\}$ for F over B.
$SB := \{\mathbf{SAT\ CONDITION}(\gamma) \mid \gamma \in B\}$
$SB' := \{\beta \in SB \mid 1 \notin I_{\mathrm{gr}(\beta)}\}$
IF $SB' = \emptyset$ **THEN** Return($\emptyset$)
$\Gamma := \bigcup_{\beta \in SB} \{\mathbf{SAT\ DET}(\beta, F)\}$
OPEN:= $\bigcup_{\gamma \in \Gamma} \{(\gamma, \mathrm{NG}(\mathrm{col}^1_\gamma(F)))\}$
OPEN:= $\{(\gamma, G) \in \mathrm{OPEN} \mid G \neq \emptyset\}$
IF OPEN $= \emptyset$ **THEN** Return($\emptyset$)
OPEN:= $\{(\gamma, G, \mathrm{P}(|G|)) \mid (\gamma, G) \in \mathrm{OPEN}\}$
CLOSED:= $\emptyset$
WHILE OPEN $\neq \emptyset$ **DO** found:=false, (γ, G, P):=pop(OPEN)
  d:= **DIMBOUND**($\{\mathrm{monom1}(\mathrm{col}^0_\gamma(g)) \mid g \in G\}$) of triple (γ, G, P)
  IF $d < D$ **THEN**
    CLOSED:= CLOSED $\cup\{(\gamma, G, d)\}$
  ELSE
    WHILE $P \neq \emptyset$ **and** found =false **DO**
      pair:= pop(P) $(=\{i_0, j_0\})$ $i := i_0, j := j_0$
      IF $\mathrm{HM}_\gamma(g_i)$ **and** $\mathrm{HM}_\gamma(g_j)$ are defined **THEN**
        found:= (**LCM TEST**(g_i, g_j)) **and**
        ($\sim$**CRITERION**(i, j, G, P))
    IF found = true **THEN**
      h:=**GCD-SPOLY**$_\gamma(g_i, g_j)$
      k:=**GCD-NORMALFORM**(γ, h, G)
      Δ:= **SAT DET1**(γ, k)
      Δ':= $\{\delta \in \Delta \mid T_{red,\delta}(k) = \{a \cdot t \in T(k) \mid \mathrm{col}^1_\delta(a) = red\} \neq \emptyset\}$
      OPEN:= OPEN
      $\bigcup_{\delta \in \Delta'} \{(\delta, G \cup \{\mathrm{col}^0_\delta(k)\}, P \cup \{\{i, n+1\} \mid 1 \leq i \leq n\})\}$
      $\bigcup_{\delta \in \Delta/\Delta'} \{(\delta, G, P)\}$
    ELSE
      CLOSED:= CLOSED $\cup\{(\gamma, G)\}$
Return(CLOSED)

convention, we set the dimension of this variety to -1. So now suppose that all M_j are nonempty. The algorithm then finds the set $\mathcal{M}$ of all subsets of subscripts of main variables such that, by setting these variables to zero, all monomials m_j will vanish. We then set r to be the minimal cardinality of such subsets in $\mathcal{M}$, and set $d = n - r$, the number of variables free. Claim: [2] this d is the dimension of $\mathbf{V}(I)$. If not, then there exists a set of subscripts of main variables, $J' = \{i_1, \ldots, i_s\}$, with $s < r$, such that the variety $W' = \mathbf{V}(x_{i_1}, \ldots, x_{i_s})$ is contained in $\mathbf{V}(I)$. We need to show $J' \in \mathcal{M}$ to get a contradiction that r is minimal. So, let M_j be one of the sets constructed by the routine. Since, m_j is zero on $\mathbf{V}(I)$, it is also zero on W'. This means that m_j must be of the form $m_j = x^{\beta} x_{i_j}$ for at least one $i_j \in J'$. Since, M_j was arbitrary, we have $J' \in \mathcal{M}$. This proves the claim. **End**

Example 3.4.2 Let $I = \langle m_1, m_2 \rangle \subset k[x, y, z]$ with $m_1 = xy^2, m_2 = xz$ as in the above example. Then $M_1 = \{1, 2\}, M_2 = \{1, 3\}$, and

$$\mathcal{M} = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}\}.$$

Thus, dim $\mathbf{V}(I) = 3 - 1 = 2$ as before.

Table 3.2 gives our algorithm **PARTIAL GROEBNERSYSTEM**. Assumming k is an algebraically closed field, and making use of the main estimate in equation 3.5, the algorithm computes a Groebner System for an ideal over a case distinction with the added feature that it checks to see if the upper bound on the dimension of an intermediate generating set is strictly smaller than some prescribed, positive integer, bound D. As in section 1.2, let monom1(f) be the monomial of the first, not necessarily the head, term of f.

Analysis of PARTIAL GROEBNERSYSTEM: For each triple (γ, G, P) in OPEN, the algorithm checks the dimension of the variety of the monomial ideal generated by the first monomials of polynomials in G after being directly colored by γ. It is possible for γ to be such that all of these will be zero. It is also possible

Table 3.1, Algorithm **DIMBOUND**

Input: List $I = \{m_1, \ldots, m_t\}$ where each m_i may be zero, or a monomial $m_i = x^{\alpha_i}$ in the main variables $\{x_1, \ldots, x_n\}$
Output: Dimension d of the variety of the monomial ideal $I = \langle m_1, \ldots, m_t \rangle$

$I' := \emptyset$
bigideal:= false
WHILE $I \neq \emptyset$ **DO**
  $m_i := \text{pop}(I)$
  IF $m_i \neq 0$ **THEN**
    $I' := I' \cup \{m_i\}$
IF $I' = \emptyset$ **THEN**
  $d := n$
ELSE
  FOR $j := 1$ **WHILE** ($j \leq t$ **and** bigideal = false) **DO**
    $M_j := \{k \in \{1, \ldots, n\} \mid x_k | m_j\}$
    IF $M_j = \emptyset$ **THEN**
      bigideal:= true
  IF bigideal:= true **THEN**
    $d := -1$
  ELSE
    $\mathcal{M}$:= $\{J \subset \{1, \ldots, n\} \mid J \cap M_j \neq \emptyset, 1 \leq j \leq t\}$
    r:= $\min(|J| : J \in \mathcal{M})$
    $d := n - r$
Return(d)

$V = \mathbf{V}(I)$ its variety. Elementary set theory gives

$$\begin{aligned}
\mathbf{V}(I) &= \mathbf{V}(xy^2) \cap \mathbf{V}(xz) \\
&= (H_x \cup H_y) \cap (H_x \cup H_z) \\
&= (H_x \cap (H_x \cup H_z)) \cup (H_y \cap (H_x \cup H_z)) \\
&= (H_x \cup H_{xz}) \cup (H_{yx} \cup H_{yz}) \\
&= H_{xz} \cup H_{yx} \cup H_{yz} \cup H_x.
\end{aligned}$$

We readily see that $\dim V = 2 = \dim H_x$, the largest dimension of the coordinate subspaces.

Suppose now that V is as in equation 3.6 above, and that we have a set $S = \{x_{i_1}, \ldots, x_{i_r}\}$ of distinct main variables such that each one divides every monomial m_j. Let W be the variety $W = \mathbf{V}(x_{i_1}, \ldots, x_{i_r})$. Clearly, W is contained in V. Thus we have a lower bound on the dimension of V:

$$\dim V \geq \dim W = n - r. \tag{3.7}$$

As in linear algebra, the difference $n - r$ is interpreted as "number of variables" - "number set to zero" = "number of main variables left unspecified (i.e. free)." The dimension algorithm in table 3.1 follows Theorem 3 pg. 411 of [2] with some additional checking of the trivial cases. The main idea of the algorithm is to find a minimal set of main variables that divide *all* the monomials m_j of I.

Analysis of DIMBOUND: In the **WHILE** loop, we let I' be the ideal generated by all nonzero m_i of input list I. If $I' = \emptyset$, then $\mathbf{V}(I) = \mathbf{V}(0) = k^n$, so the dimension d is set to n. If $I' \neq \emptyset$, then for each monomial m_j, set M_j to be the set of subscripts of all main variables that divide m_j. Note that if $M_j = \{x_{i_1}, \ldots, x_{i_r}\}$, then the variety $W' = \mathbf{V}(x_{i_1}, \ldots, x_{i_r}) \subset \mathbf{V}(m_j)$. If it happens that an M_j is empty, then we have the monomial $m_j \in k - \{0\}$. In this case, we have a constant in the list I, so $\langle I \rangle = k[x_1, \ldots, x_n]$, and $\mathbf{V}(I) = \emptyset$. Following

Combining equations 3.3 and 3.4 gives us the desired estimate:

$$\dim V \leq \dim \mathbf{V}(\langle \mathrm{HM}(f_1), \ldots, \mathrm{HM}(f_s) \rangle). \tag{3.5}$$

Since $\langle \mathrm{HM}(f_1), \ldots, \mathrm{HM}(f_s) \rangle$ is a monomial ideal, there is a nice algorithm, shown in table 3.1 and based on Theorem 3 pg. 117 of [2], to compute the dimension of the variety of any monomial ideal. For completeness, we summarize this next and then give the algorithm.

So let $I = \langle m_1, \ldots, m_t \rangle$ be a monomial ideal, and $V = \mathbf{V}(I)$ its variety. We may write I as $I = \langle m_1 \rangle + \cdots + \langle m_t \rangle$. From chapter 4 of [2] we have that the variety of a sum of ideals equals the intersection of the varieties of each ideal:

$$\mathbf{V}(I) = \mathbf{V}\left(\sum_{i=1}^{t} \langle m_i \rangle\right) = \bigcap_{i=1}^{t} \mathbf{V}(m_i). \tag{3.6}$$

For any nonempty collection A of main variables, the variety $\mathbf{V}(A)$, obtained by setting each main variable to zero, is called a **coordinate subspace** of k^n (it is also clearly a vector subspace). It turns out [2] that $\mathbf{V}(m_i)$ is a then a union of such coordinate subspaces. Thus, V is a finite union of intersections of such coordinate subspaces. If a subspace is contained in another in this union we may omit it and then write

$$V = V_1 \cup \ldots \cup V_p.$$

This decomposition is unique [2].

Definition 3.4.1 *Let I be a monomial ideal and V be the variety of I written as the above union of vector coordinate subspaces. Then the dimension of V,* **dim** *V, is the largest of the dimensions of these subspaces.*

Example 3.4.1 For main variables x_i, x_j, let $H_{x_i} = \mathbf{V}(x_i) \subset k^n$, and $H_{x_i x_j} = \mathbf{V}(x_i, x_j) \subset k^n$, etc. Let $I = \langle xy^2, xz \rangle \subset k[x, y, z]$ be a monomial ideal with

form the ideal $I = \langle f_1, \ldots, f_n \rangle$, and set V to be the variety

$$V = \mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_n) \subset k^n.$$

The problem then is to determine conditions on the parameters such that the dimension of V is less or equal to some given integer $D \geq 0$ (see Chap 9 of [2], and also see [7]). Indeed, as we choose different specializations of the parameters then I will change, so will V, and thus the dimension also. In [7] is a discussion of this problem and a solution given in terms of eliminating quantifier blocks. We refer the interested reader to this. For our purposes, we constructed an algorithm based on our **GROEBNERSYSTEM** which provides a somewhat more direct approach to the problem. The algorithm has its basis in the estimate shown in equation 3.5 below.

Let $F = \{f_1, \ldots, f_s\}$ be a basis (not necessarily a Groebner Basis) for an ideal $I \subset k[x_1, \ldots, x_n]$, and let $V = \mathbf{V}(I)$. Then we always have

$$\langle \mathrm{HM}(f_1), \ldots, \mathrm{HM}(f_s) \rangle \subseteq \langle \mathrm{HM}(I) \rangle. \tag{3.1}$$

Let $G = \{g_1, \ldots, g_t\}$ be a Groebner Basis for I computed with respect to a [2] graded monomial order $>$ on $k[x_1, \ldots, x_n]$, e.g. graded lex, etc. It is a general fact that for a pair of ideals I,J with $I \subseteq J$, then $\mathbf{V}(J) \subseteq \mathbf{V}(I)$. Hence, by the above,

$$\mathbf{V}(\langle \mathrm{HM}(I) \rangle) \subseteq \mathbf{V}(\langle \mathrm{HM}(f_1), \ldots, \mathrm{HM}(f_s) \rangle), \tag{3.2}$$

and so,

$$\mathrm{dim}\mathbf{V}(\langle \mathrm{HM}(I) \rangle) \leq \mathrm{dim}\mathbf{V}(\langle \mathrm{HM}(f_1), \ldots, \mathrm{HM}(f_s) \rangle). \tag{3.3}$$

If we now assume that k is an algebraically closed field, then the Dimension Theorem (pg. 431-2 of [2]) states that

$$\mathrm{dim}V = \mathrm{dim}\mathbf{V}(\langle \mathrm{HM}(I) \rangle). \tag{3.4}$$

This may be fierce looking output, yet it is actually less nasty looking than that to be found in [7]. Now, we apply the simplifications of section 2.4.2. The output is strikingly simpler. It is as follows:

$$\begin{aligned}
(\gamma_1, G_1) &= (\{\}, \{a_2 - a_4\}), \\
&\quad \{-{x_3}^3 + (-a_4 - a_3 - a_1)\, {x_3}^2 + ((-a_3 - a_1)\, a_4 - a_1\, a_3)\, x_3 + a_1\, a_3\, a_4, \\
&\quad x_4 - a_4 + a_2, \\
&\quad -{x_3}^2 + (-2\, a_4 - a_3 + a_2 - a_1)\, x_3 + (a_2 - a_4)\, x_2 - 2\, {a_4}^2 + \\
&\quad (-2\, a_3 + 3\, a_2 - 2\, a_1)\, a_4 + (a_2 - a_1)\, a_3 - {a_2}^2 + a_1\, a_2, \\
&\quad {x_3}^2 + (a_4 + a_3 + a_1)\, x_3 + (a_2 - a_4)\, x_1 + (a_3 + a_1)\, a_4 + a_1\, a_3\}), \\
(\gamma_2, G_2) &= (\{\{a_1\, a_2\, a_3, a_2 - a_4\}, \{\}), \\
&\quad \{-{x_3}^2 + (-a_3 - a_2 - a_1)\, x_3 + (-a_2 - a_1)\, a_3 - a_1\, a_2, \\
&\quad x_4, \\
&\quad x_3 + x_2 + x_1 + a_3 + a_2 + a_1\}), \\
(\gamma_3, G_3) &= (\{\{a_2 - a_4\}, \{a_1\, a_2\, a_3\}\}, \{a_1\, a_2\, a_3\}).
\end{aligned}$$

In the first case, we may solve the system for each variable x_1, x_2, x_3, x_4. So the dimension of $\mathbf{V}(F)$ is zero in this case. In the second case, $x_4 = 0$. So, we may solve the cubic for x_3, and then solve the remaining equation for x_2 as a function of x_1. Therefore, x_1 is unspecified, and the dimension of $\mathbf{V}(F)$ is 1 in this case. In the last case, since the product $a_1 a_2 a_3$ is in the red list of the condition, it is nonzero. Hence $\langle F \rangle$ contains a constant. Thus, $\mathbf{V}(F)$ is empty (assign it dimension -1).

3.4 Partial Comprehensive Groebner Bases

In this section we consider the following problem: let

$$f_1, \ldots, f_n \in S = k[u_1, \ldots, u_m][x_1, \ldots, x_n],$$

Example 3.3.1 Let $F = \{f_1, f_2, f_3, f_4\} \subset k[a_1, a_2, a_3, a_4][x_1, x_2, x_3, x_4]$, where

$$\begin{aligned} f_1 &= x_4 - (a_4 - a_2), \\ f_2 &= x_1 + x_2 + x_3 + x_4 + (a_1 + a_3 + a_4), \\ f_3 &= x_1x_3 + x_1x_4 + x_2x_3 + x_3x_4 - (a_1a_4 + a_1a_3 + a_3a_4), \\ f_4 &= x_1x_3x_4 - a_1a_3a_4. \end{aligned}$$

Taking $B = \{\gamma\}$ with γ as the empty condition, **REDGS2**$(B, F, [x_1, x_2, x_3, x_4])$ gives the following three case output:

$$\begin{aligned} (\gamma_1, G_1) &= ((\{\}, \{a_2 - a_4\}), \\ &\quad \{-{x_3}^3 + (-a_4 - a_3 - a_1)\,{x_3}^2 + (-(a_3 + a_1)\,a_4 - a_1\,a_3)\,x_3 + a_1\,a_3\,a_4, \\ &\quad x_4 - a_4 + a_2, \\ &\quad -{x_3}^2 + (-2\,a_4 - a_3 + a_2 - a_1)\,x_3 + (a_2 - a_4)\,x_2 - 2\,{a_4}^2 + \\ &\quad (-2\,a_3 + 3\,a_2 - 2\,a_1)\,a_4 + a_2\,(a_3 + a_1) - a_1\,a_3 - {a_2}^2, \\ &\quad {x_3}^2 + (a_4 + a_3 + a_1)\,x_3 + (a_2 - a_4)\,x_1 + (a_3 + a_1)\,a_4 + a_1\,a_3\}), \\ (\gamma_2, G_2) &= ((\{a_1\,a_2\,a_3, a_2 - a_4\}, \{\}), \\ &\quad \{-{x_3}^2 + (-2\,a_4 - a_3 + a_2 - a_1)\,x_3 - 2\,{a_4}^2 + \\ &\quad (-2\,a_3 + 3\,a_2 - 2\,a_1)\,a_4 + a_2\,(a_3 + a_1) - a_1\,a_3 - {a_2}^2, \\ &\quad x_4 - a_4 + a_2, \\ &\quad x_3 + x_2 + x_1 + 2\,a_4 + a_3 - a_2 + a_1\}), \\ (\gamma_3, G_3) &= ((\{a_2 - a_4\}, \{-2\,{a_4}^3 + (-2\,a_3 + 5\,a_2 - 2\,a_1)\,{a_4}^2 + \\ &\quad (a_2\,(3\,a_3 + 3\,a_1) - 4\,{a_2}^2)\,a_4 + a_1\,a_2\,a_3 + {a_2}^2\,(-a_3 - a_1) + {a_2}^3\}), \\ &\quad \{-2\,{a_4}^3 + (-2\,a_3 + 5\,a_2 - 2\,a_1)\,{a_4}^2 + \\ &\quad (a_2\,(3\,a_3 + 3\,a_1) - 4\,{a_2}^2)\,a_4 + a_1\,a_2\,a_3 + {a_2}^2\,(-a_3 - a_1) + {a_2}^3\}). \end{aligned}$$

(Time: 11.6 sec)

$$
\begin{aligned}
(\gamma_1, G_1) &= \{(\{\}, \{2\,a, 24\,b\,c + 2\,a^2\,b, -1024\,a\,c^4 + \\
&\quad 512\,a^3\,c^3 + (-576\,a^2\,b^2 - 64\,a^5)\,c^2 + \\
&\quad (108\,a\,b^4 + 16\,a^4\,b^2)\,c\}), \\
&\quad \{-256\,a\,c^4 + 128\,a^3\,c^3 + (-144\,a^2\,b^2 - 16\,a^5)\,c^2 + \\
&\quad (27\,a\,b^4 + 4\,a^4\,b^2)\,c\}, \\
(\gamma_2, G_2) &= \{(\{a\}, \{b, -256\,c^3 - 72\,a\,b^2\,c + 27\,b^4\}), \\
&\quad \{-256\,c^3 - 72\,a\,b^2\,c + 27\,b^4\}\}, \\
(\gamma_3, G_3) &= \{(\{b, a\}, \{c\}), \{c\}\}, \\
(\gamma_4, G_4) &= \{(\{-c\}, \{a, a^2\,b, -27\,a\,b^4 - 4\,a^4\,b^2\}), \\
&\quad \{-27\,a\,b^4 - 4\,a^4\,b^2\}\}, \\
(\gamma_5, G_5) &= \{(\{-c, -b\}, \{a, a^3\}), \{a^3\,x\}\}, \\
(\gamma_6, G_6) &= \{(\{c, b, a\}, \{\}), \{x^3\}\}, \\
(\gamma_7, G_7) &= \{(\{-8\,a\,c + 9\,b^2 + 2\,a^3, -27\,b^3 - 8\,a^3\,b, \\
&\quad 16\,c^2 - 3\,a\,b^2 - a^4, 12\,b\,c + a^2\,b\}, \{a\}), \{a\,x^2 + b\,x + c\}\}, \\
(\gamma_8, G_8) &= \{(\{12\,b\,c + a^2\,b\}, \{a, 32\,c^2 - 8\,a^2\,c + 3\,a\,b^2\}), \\
&\quad \{32\,c^2 - 8\,a^2\,c + 3\,a\,b^2\}\}, \\
(\gamma_9, G_9) &= \{(\{27\,b^4 - 256\,c^3, a\}, \{b\}), \{b\,x + c\}\}, \\
(\gamma_{10}, G_{10}) &= \{(\{-256\,c^3 + 128\,a^2\,c^2 + (-144\,a\,b^2 - 16\,a^4)\,c + 27\,b^4 + 4\,a^3\,b^2\}, \\
&\quad \{a, 12\,b\,c + a^2\,b\}), \{(12\,b\,c + a^2\,b)\,x + 32\,c^2 - 8\,a^2\,c + 3\,a\,b^2\}\}.
\end{aligned}
$$

3.3 An example from V. Weispfenning

In this section we give another example using the two optimizations described in section 2.4.2. This example is taken from the paper of Weispfenning [7] (it is supposed to describe a chemical equilibrium).

$$
\begin{aligned}
& (144\,a^2\,b^2 + 16\,a^5)\,c - 27\,a\,b^4 - 4\,a^4\,b^2\}), \\
& \{256\,a\,c^3 - 128\,a^3\,c^2 + (144\,a^2\,b^2 + 16\,a^5)\,c - 27\,a\,b^4 - 4\,a^4\,b^2\}), \\
(\gamma_5, G_5) &= (((\{-c, -b\}, \{2\,a, -8\,a\,c + 9\,b^2 + 2\,a^3\}), \{(-8\,a\,c + 9\,b^2 + 2\,a^3)\,x\}), \\
(\gamma_6, G_6) &= (((\{c, b, a\}, \{\}), \{4\,x^3\}), \\
(\gamma_7, G_7) &= (((\{-8\,a\,c + 9\,b^2 + 2\,a^3, -27\,b^3 - 8\,a^3\,b, \\
& 16\,c^2 - 3\,a\,b^2 - a^4, 12\,b\,c + a^2\,b\}, \{2\,a\}), \{2\,a\,x^2 + 3\,b\,x + 4\,c\}), \\
(\gamma_8, G_8) &= (((\{12\,b\,c + a^2\,b\}, \{2\,a, 32\,c^2 - 8\,a^2\,c + 3\,a\,b^2\}), \\
& \{32\,c^2 - 8\,a^2\,c + 3\,a\,b^2\}), \\
(\gamma_9, G_9) &= (((\{27\,b^4 - 256\,c^3, a\}, \{3\,b\}), \{3\,b\,x + 4\,c\}), \\
(\gamma_{10}, G_{10}) &= (\{\{-256\,c^3 + 128\,a^2\,c^2 + (-144\,a\,b^2 - 16\,a^4)\,c + 27\,b^4 + 4\,a^3\,b^2\}, \\
& \{2\,a, 24\,b\,c + 2\,a^2\,b\}\}, \{(24\,b\,c + 2\,a^2\,b)\,x + 32\,c^2 - 8\,a^2\,c + 3\,a\,b^2\}).
\end{aligned}
$$

MACSYMA will compute the Z matrix and the resultant of f and f'. For the reader's patience, note that the various cases above show the common factors (or lack thereof) depending on the vanishing (or nonvanishing) of the resultant. For reference, the Z matrix is

$$
\begin{vmatrix}
b & -4c & ab & b^2 - 2ac \\
2a & -3b & 2a^2 - 4c & ab \\
0 & -2a & -3b & -4c \\
4 & 0 & 2a & b
\end{vmatrix}.
$$

So our algorithm examines all the possible cases for the determinant of Z and its consequences. (Time: 30.4 sec)

To further simplify the above ten pairs, we apply the procedures of section 2.4.2. Recall that this meant we replace each element of the red list of a condition γ and each coefficient of each polynomial in the basis G with their remainders modulo the ideal generated by the green list of γ. The output from these procedures is shown below. Note the simplifications in the red lists and the basis polynomials. We have:

A second classical result (again see Mignotte) is that the resultant R may be computed via the formula

$$R = (-1)^{m(m-1)/2}\det(Z),$$

where Z is the matrix whose entries form the coefficients of the bezoutian,

$$\begin{vmatrix} af - cd & bf - ce \\ ae - bd & af - cd \end{vmatrix}.$$

So we see again that our algorithm calculates all possible ways for this determinant to vanish or not.

Example 3.2.2 Consider now the case of the quartic polynomial $f = x^4 + ax^2 + bx + c$ and its derivative $g = f' = 4x^3 + 2ax + b$. Take the inital case distinction to be $B = \{\gamma\}$ with $\gamma = (\{\}, \{\})$. We can choose the empty condition since f, g do not have parameters a, b, c in their greatest terms. Setting $I = \langle f, g\rangle$ we have the following output from **REDGS2**$(B, I, [x])$ (we are now essentially analyzing the *discriminant* of the polynomials (the resultant of f and f' up to a constant [5])). There are 10 distinct Groebner pairs:

$$\begin{aligned}
(\gamma_1, G_1) &= (\{\}, \{2\,a, 24\,b\,c + 2\,a^2\,b, -1024\,a\,c^4 + \\
&\quad 512\,a^3\,c^3 + (-576\,a^2\,b^2 - 64\,a^5)\,c^2 + \\
&\quad (108\,a\,b^4 + 16\,a^4\,b^2)\,c\}), \\
&\quad \{-1024\,a\,c^4 + 512\,a^3\,c^3 + (-576\,a^2\,b^2 - 64\,a^5)\,c^2 + \\
&\quad (108\,a\,b^4 + 16\,a^4\,b^2)\,c\}), \\
(\gamma_2, G_2) &= (\{\{a\}, \{3\,b, -256\,c^3 - 72\,a\,b^2\,c + 27\,b^4\}), \\
&\quad \{-256\,c^3 - 72\,a\,b^2\,c + 27\,b^4\}), \\
(\gamma_3, G_3) &= (\{\{b, a\}, \{4\,c\}), \{4\,c\}), \\
(\gamma_4, G_4) &= (\{\{-c\}, \{2\,a, 24\,b\,c + 2\,a^2\,b, 256\,a\,c^3 - 128\,a^3\,c^2 +
\end{aligned}$$

where R is the resultant of f_1, f_2:

$$R = (af - cd)^2 - (ae - bd)(bf - ce).$$

It is a classical fact (chapter 3 of [2]) that for two polynomials f, g of positive degree in $k[x]$, there exist polynomials $A, B \in k[x]$ for which $Af + Bg = R$. Furthermore, A, B, and R are integer polynomials in the coefficients of f and g. We may thus interpret the GS above as follows. For all specializations of the parameters a, b, c, d, e, f that make the resultant R nonzero, the ideal $I = \langle f_1, f_2 \rangle = \langle R \rangle$. In the second case, R is still nonzero under all specializations making the factors $bd - ae = 0$ and $af - cd \neq 0$. Hence $I = \langle R \rangle$ here as well. In the third case, R will be zero, and one can see that the coefficients of f_1, f_2 are porportional. Hence, I just consists of the one generator f_2. Lastly, under all specializations where $R = 0$ but $bd - ae$ is nonzero, the two polynomials must have a common factor. The polynomial $p(x) = (bd - ae)x - (af - cd)$ is this common factor. Note that it is indeed of degree one under the given condition. Since $k[x]$ is a principal ideal domain, we have found the generator for I, i.e. $I = \langle p(x) \rangle$. (Time: 10.9 sec)

The example shows how the algorithm essentially computes all possible cases for the resultant to be zero or nonzero and lets the generators of I be the results. On pgs. 112-14 of the book by Mignotte [5] is a discussion of the *bezoutian* of two polynomials $F(x), G(x)$ of positive degree $n = \deg(G) \leq \deg(F) = m$. It is defined as

$$B(X, Y) = \frac{F(X)G(Y) - F(Y)G(X)}{X - Y}.$$

It turns out that this is a symmetric polynomial in X, Y [5]. In our case, with $F = f_1$ and $G = f_2$, the bezoutian is

$$B(X, Y) = (ae - bd)xy + (af - cd)x + (af - cd)y + (bf - ce).$$

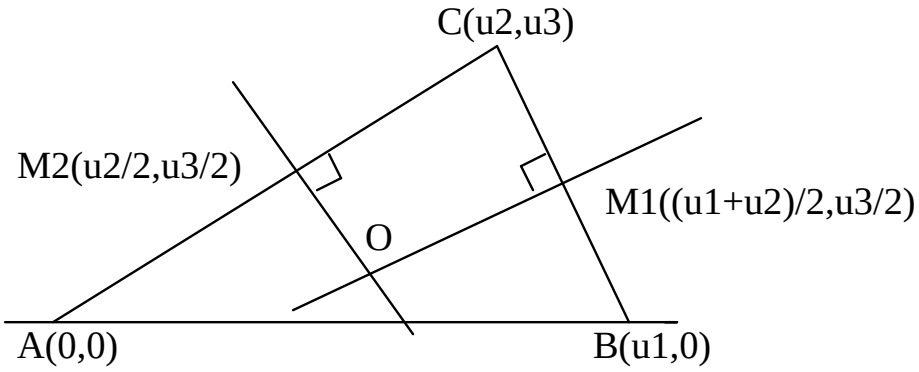

Figure 3.7, Circumcenter Theorem

We sum up this section with the Euler Line theorem. By the above three examples, one may easily compute from their coordinates that that M, H, and O are collinear, i.e. Collinear$(M, H, O) = 0$ in both the case of ABC a right triangle or otherwise.

3.2 Computations involving Resultants

In this section we present two examples that illustrate how the pairs in a Groebner System capture information about the resultant for a pair of polynomials in a single variable.

Example 3.2.1 Let $f_1 = ax^2 + bx + c, f_2 = dx^2 + ex + f \in k[a, b, c, d, e, f][x]$ be two quadratic polynomials. The generic case is for a, d nonzero. So we let $B = \{\gamma\}$, with $\gamma = (\{\}, \{a, d\})$. Then, with $I = \langle f_1, f_2 \rangle$, **REDGS2**$(B, I, [x])$ gives the Groebner System GS with four Groebner pairs:

$$\begin{aligned}
(\gamma_1, G_1) &= ((\{\}, \{R\}), \{R\}), \\
(\gamma_2, G_2) &= ((\{bd - ae\}, \{a, d, af - cd\}), \{af - cd\}), \\
(\gamma_3, G_3) &= ((\{bf - ce, cd - af, bd - ae\}, \{a, d\}), \{dx^2 + ex + f\}), \\
(\gamma_4, G_4) &= ((\{R\}, \{a, d, bd - ae\}), \{(bd - ae)x - (af - cd)\}),
\end{aligned}$$

The conclusion is that the line segments $\overline{OA}$, $\overline{OB}$ and $\overline{OC}$ all have the same length. This length is then the radius of the circumscribing circle with center at O. We encode the conclusion with two polynomials using the square of the Euclidean distance formula between two points:

$$\begin{aligned} g_1 &= (x_1^2 + x_2^2)^2 - ((u_1 - x_1)^2 + x_2^2)^2, \\ g_2 &= (x_1^2 + x_2^2)^2 - ((u_2 - x_1)^2 + (u_3 - x_2)^2)^2. \end{aligned}$$

The first equation gives the difference of the lengths of $\overline{OA}$ and $\overline{OB}$. The second equation gives the difference of the lengths of $\overline{OA}$ and $\overline{OC}$. If both the equations $g_1 = 0$ and $g_2 = 0$ are satisfied from the hypotheses, this will then prove the result. We may take the initial case distinction as in the previous example.

The output from **REDGS2**$(B, I, [x_1, x_2])$ is $GS = \{(\gamma_1, G_1), (\gamma_2, G_2)\}$ where

$$\begin{aligned} (\gamma_1, G_1) &= ((\{\}, \\ &\quad \{u_1, u_2, u_3, u_1^2 + u_2^2, u_1^2 + u_3^2, u_2^2 + u_3^2, (u_1 - u_2)^2 + u_3^2, u_2 - u_1\}), \\ &\quad \{u_1 u_2 (x_1 - \frac{u_1}{2}), u_1 (u_3 x_2 - \frac{u_2^2 + u_3^2 - u_1 u_2}{2})\}), \\ (\gamma_2, G_2) &= ((\{u_2 - u_1\}, \\ &\quad \{u_1, u_2, u_3, u_1^2 + u_2^2, u_1^2 + u_3^2, u_2^2 + u_3^2, (u_1 - u_2)^2 + u_3^2\}), \\ &\quad \{u_2 x_1 - \frac{u_1^2}{2}, u_3 x_2 - \frac{u_2^2 + u_3^2 - u_1^2}{2}\}). \end{aligned}$$

We again obtain two cases depending on whether triangle ABC is right or not. Setting the polynomials in G_1 (G_2) to zero, we may solve for x_1 and x_2. The solution will satisfy both conclusion equations and give coordinates for the circumcenter. From G_1 we have

$$x_1 = \frac{u_1}{2}, \text{ and } x_2 = \frac{u_2^2 + u_3^2 - u_1 u_2}{2u_3},$$

and from G_2 we have (remembering that $u_1 = u_2$ in this case)

$$x_1 = \frac{u_1}{2}, \text{ and } x_2 = \frac{u_3}{2}.$$

(Time: 10.03 sec)

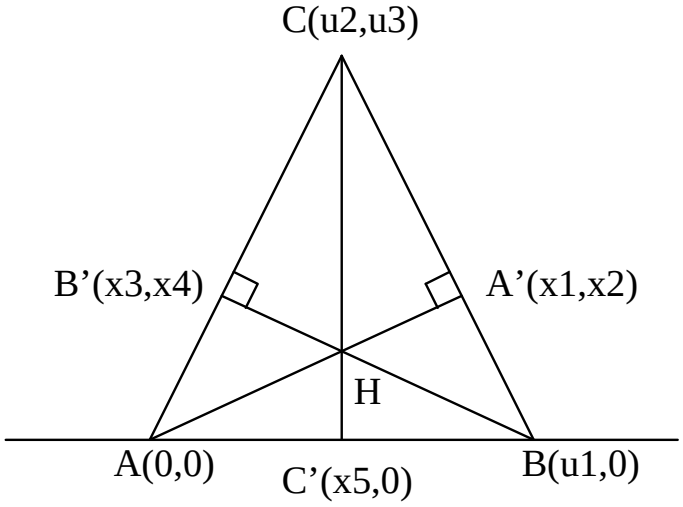

Figure 3.6, Orthocenter Theorem

In the second pair, $x_5 = u_2$ and so $C' = C$, and $x_7 = u_1, x_8 = 0$. We see that the orthocenter $H = B$ as it should. In the first pair, $x_5 = u_2$ again (corresponding to the perpendicular dropped from C onto the x-axis), and we have the coordinates of $H(x_7, x_8)$ as

$$x_7 = u_2, \text{ and } x_8 = \frac{u_2(u_1 - u_2)}{u_3}.$$

Note that both x_7 and x_8 are nonzero by the condition γ_1. In both cases, the conclusion equation $g = 0$ is satisfied. (Time: 25.23 sec)

Example 3.1.8 Result: The three perpendicular bisectors of each side of a triangle meet in a single point; the *circumcenter* of the triangle (the center of the circle that circumscribes the triangle). Let $M_1((u_1 + u_2)/2, u_3/2)$ and $M_2(u_2/2, u_3/2)$ be midpoints of the sides $\overline{BC}$ and $\overline{CA}$ respectively of the triangle. Let $O(x_1, x_2)$ be the point of intersection of the perpendicular bisectors of $\overline{BC}$ and $\overline{CA}$ (see figure 3.7). We may encode the geometric hypotheses as the polynomials

$$\begin{aligned} h_1 &= \text{dotp}(M_1 - O, C - B), \\ h_2 &= \text{dotp}(M_2 - O, C - A). \end{aligned}$$

where

$$
\begin{aligned}
(\gamma_1, G_1) \;=\; & ((\{\}, \\
& \{u_1, u_2, u_3, u_1^2+u_2^2, u_1^2+u_3^2, u_2^2+u_3^2, (u_1-u_2)^2+u_3^2, u_2-u_1\}), \\
& \{(u_2-u_1)(((u_2-u_1)^2+u_3^2)x_1 - u_1u_3^2), \\
& ((u_2-u_1)^2+u_3^2)x_2 + (u_2-u_1)u_1u_3, \\
& u_3((u_2^2+u_3^2)x_3 - u_1u_2^2), \\
& (u_2^2+u_3^2)x_4 - u_1u_2u_3, \\
& u_1(x_5-u_2), \\
& ((u_2-u_1)^2u_1^3u_3^3u_2)(x_7-u_2), \\
& ((u_2-u_1)u_1^3u_2u_3^2)(u_3x_8 + u_2(u_2-u_1))\}), \\
(\gamma_2, G_2) \;=\; & ((\{u_2-u_1\}, \\
& \{u_1, u_2, u_3, u_1^2+u_2^2, u_1^2+u_3^2, u_2^2+u_3^2, (u_1-u_2)^2+u_3^2\}), \\
& \{u_3(x_1-u_1), \\
& u_3x_2, \\
& u_2((u_2^2+u_3^2)x_3 - u_1u_2), \\
& (u_2^2u_3^2)x_4 - u_1u_2u_3, \\
& u_1(x_5-u_2), \\
& (u_1u_2^2u_3)(x_7-u_1), \\
& u_1u_3x_8\}).
\end{aligned}
$$

In the second pair, $u_2 = u_1$ since $u_2 - u_1$ is in the green list of the condition. This corresponds geometrically to B and C having the same x coordinate, and hence, the triangle ABC is a right triangle. In the first pair, $u_2 - u_1$ is in the red list of the condition and so triangle ABC is not a right triangle. By setting all the equations of G_1 (G_2) to zero, we may solve for x_i accordingly.

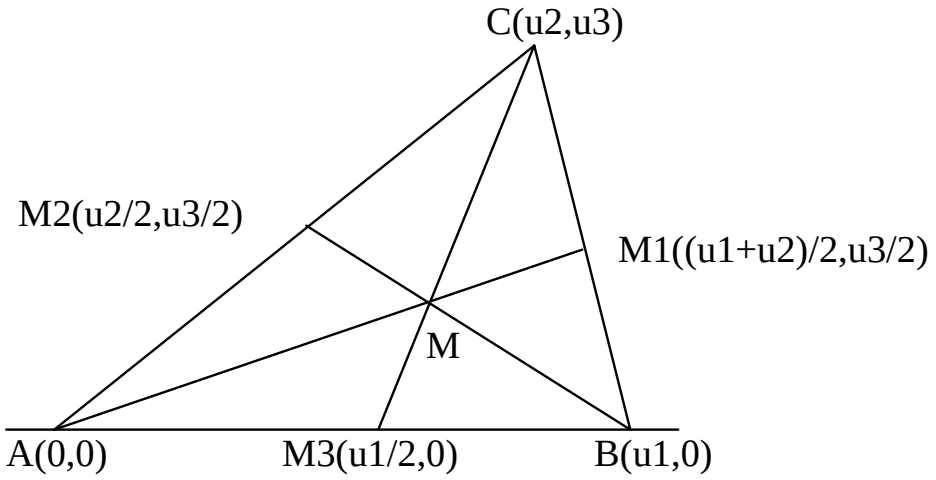

Figure 3.5, Centroid Theorem

$$\begin{aligned} h_3 &= \text{Collinear}(A, B', C), \\ h_4 &= \text{dotp}(B' - B, C - A), \\ h_5 &= \text{Collinear}(A, C', B), \\ h_6 &= \text{dotp}(C' - C, B - A), \\ h_7 &= \text{Collinear}(A, H, A'), \\ h_8 &= \text{Collinear}(B, H, B'). \end{aligned}$$

The equations $h_1 = 0$ and $h_2 = 0$ encode that A' is on the side $\overline{BC}$ of the triangle and that the line segment $\overline{AA'}$ is the altitude dropped from vertex A. The other two altitudes are similarly encoded. The last two hypotheses indicate H as the point of intersection of two of the altitudes. Set the conclusion polynomial as

$$g = \text{Collinear}(C, H, C') = u_3x_5 - u_3x_7 + (u_2 - x_5)x_8.$$

Then, $g = 0$ means that H is on the third altitude of the triangle as well. We may take the initial case distinction B as in the previous example.

The output from **REDGS2**$(B, I, [x_1, x_2, x_3, x_4, x_5, x_7, x_8])$ is

$$GS = \{(\gamma_1, G_1), (\gamma_2, G_2)\},$$

the conclusion as

$$g = \text{Collinear}(C, M, M_1) = u_3 x_1 + \left(\frac{u_1}{2} - u_2\right) x_2 - \frac{u_1 u_3}{2}.$$

The generic case condition is

$$\gamma = (\{\}, \{u_1, u_2, u_3, u_1^2 + u_2^2, u_1^2 + u_3^2, u_2^2 + u_3^2, (u_1 - u_2)^2 + u_3^2\}).$$

As in the previous example, putting the sums of squares in the red list tells the algorithm to not consider those specializations that could make them zero.

The output from **REDGS2**$(B, I, [x_1, x_2])$ is $GS = \{(\gamma_1, G_1)\}$ where

$$\begin{aligned}(\gamma_1, G_1) \;=\; & (\{\}, \{u_1, u_2, u_3, u_1^2 + u_2^2, u_1^2 + u_3^2, u_2^2 + u_3^2, (u_1 - u_2)^2 + u_3^2\}), \\ & \{\tfrac{u_1 u_3}{2}(3x_1 - (u_1 + u_2)), \tfrac{u_1}{2}(3x_2 - u_3)\}).\end{aligned}$$

Setting the two polynomials in G_1 to zero and easily solving for x_1 and x_2 gives the coordinates of the centriod:

$$x_1 = \frac{u_1 + u_2}{3}, \text{ and } x_2 = \frac{u_3}{3}.$$

Clearly, this solution satisfies the conclusion equation $g = 0$. Hence, g vanishes on the variety of G_1 under the given condition γ_1. (Time: 4.25 sec)

Example 3.1.7 Result: The three altitudes of a triangle (line segments from each vertex that meet the side opposite the vertex in a right angle) meet in a single point; the *orthocenter* of the triangle. Let $A'(x_1, x_2)$, $B'(x_3, x_4)$ and $C'(x_5, 0)$ be where the altitudes from vertices A, B and C respectively meet the opposite side (see figure 3.6). Let $H(x_7, x_8)$ be the point of intersection of the altitudes $\overline{AA'}$ and $\overline{BB'}$. We encode the geometric hypotheses as the polynomials

$$\begin{aligned} h_1 &= \text{Collinear}(B, A', C), \\ h_2 &= \text{dotp}(A' - A, C - B), \end{aligned}$$

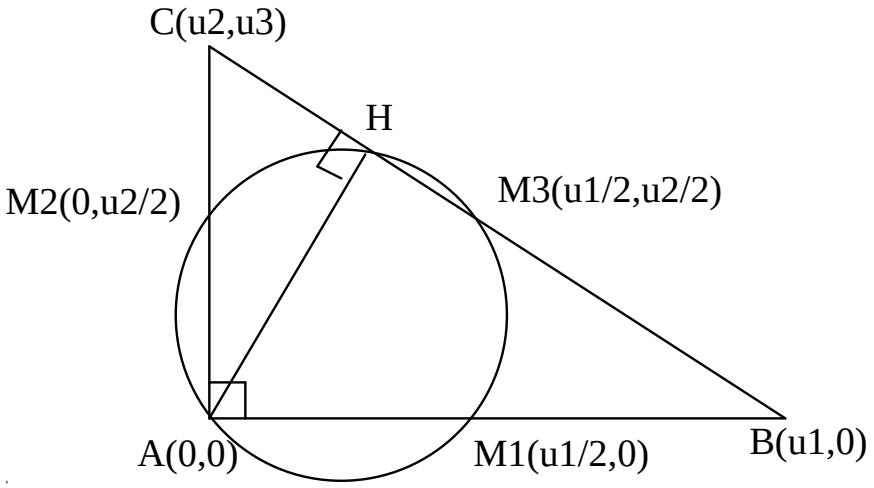

Figure 3.4, Appolonius Circle result

defined head monomials for the basis polynomials. This will be a recurring theme. (Time: 1.5 sec)

The next three examples are based on exercises 5-7 pg. 293 of [2]. They collectively lead up to the *Euler line* of a triangle in the plane. In each example, we let $A(0,0)$, $B(u_1,0)$, and $C(u_2,u_3)$ be the vertices of a triangle. Also, $B = \{\gamma\}$ will be the initial case distinction in each example, where γ will be the condition specified in the centroid example. The ideal I of each will be the ideal generated by the presented hypotheses h_i.

Example 3.1.6 Result: The line segments from each vertex of a triangle to the midpoint of side opposite the vertex meet in a single point; the *centroid* (center of mass) of the triangle. Let $M_1((u_1+u_2)/2, u_3/2)$, $M_2(u_2/2, u_3/2)$ and $M_3(u_1/2, 0)$ be the midpoints of the sides $\overline{BC}$, $\overline{CA}$, and $\overline{AB}$ respectively (see figure 3.5). Let $M(x_1,x_2)$ be the point of intersection of the line segments $\overline{AM_1}$ and $\overline{BM_2}$. Set the hypotheses as $h_1 = \text{Collinear}(A,M,M_1)$ and $h_2 = \text{Collinear}(B,M,M_2)$, and set

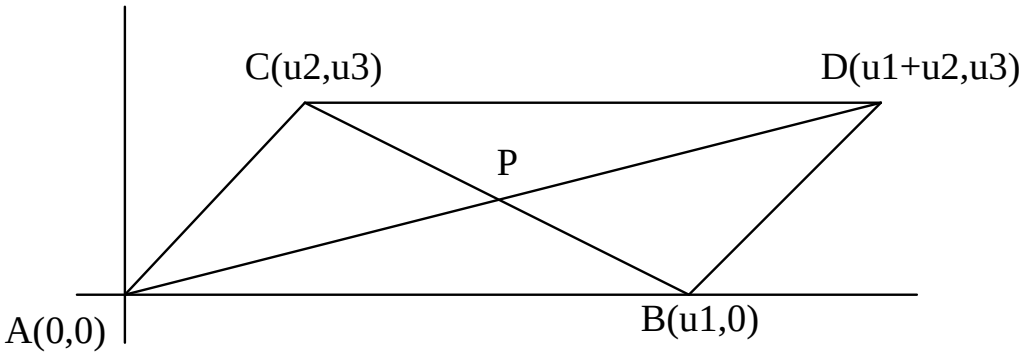

Figure 3.3, Parallelogram result

The equation $g = 0$ says that H must lie on the circle with center being determined from the midpoints of the two legs of the triangle and radius the distance from the center to the origin. The initial condition is $\gamma = (\{\}, \{u_1, u_2, u_1^2 + u_2^2\})$ for the generic case; $B = \{\gamma\}$. Setting u_1,u_2 not equal to zero ensures that the triangle does not collapse. The computer does not know that we are working over the reals. By putting $u_1^2 + u_2^2$ in the red list, we do not consider those specializations, say $u_1 = i$, $u_2 = 1$, that could make $u_1^2 + u_2^2$ zero. Doing this also tells the Comprehensive Groebner Basis algorithms not to consider the case of making $u_1^2+u_2^2$ *green*. Set $I = \langle h_1, h_2 \rangle$. The output from **REDGS2**$(B, I, [x_1, x_2])$ consists of just one Groebner Pair:

$$(\gamma_1, G_1) = ((\{\}, \{u_1, u_2, u_1^2 + u_2^2\}), \{u_1((u_1^2 + u_2^2)x_1 - u_1u_2^2), (u_1^2 + u_2^2)x_2 - u_1^2u_2\}).$$

Setting the two polynomials in G_1 to zero and solving for x_1, x_2 in terms of the generically set u_i gives

$$x_1 = \frac{u_1u_2^2}{u_1^2 + u_2^2}, \text{ and } x_2 = \frac{u_1^2u_2}{u_1^2 + u_2^2}.$$

This solution will then satisfy the conclusion equation $g = 0$. We see that g indeed vanishes where the two equations of G_1 vanish. The form of the Groebner system output shows our initial case distinction was just what was needed to have well-

of vectors $\vec{v}, \vec{w}$. Then, the statement "the lines AB and CD are perpendicular" may be encoded as dotp$(B-A, D-C)$ = dotp$(\vec{b}-\vec{a}, \vec{d}-\vec{c}) = 0$ (where $\vec{a}$ is the vector from the origin to A, etc).

Example 3.1.4 Result: The diagonals of a parallelogram bisect each other. Let $A(0,0), B(u_1,0), C(u_2,u_3), D(u_1+u_2,u_3)$ be the vertices of the parallelogram $ABDC$ (see figure 3.3) and let $P(x_1,x_2)$ be the point where the diagonals meet. Let $h_1 =$ Collinear$(A,P,D), h_2 =$ Collinear(B,P,C) be the hypotheses and $I = \langle h_1, h_2 \rangle$. Let $g_1 = 2x_1 - (u_1+u_2)$, and $g_2 = 2x_2 - u_3$. be the conclusion polynomials. The equations $g_1 = 0$ and $g_2 = 0$ mean that P bisects both diagonals. Now, the degenerate cases correspond to when, say, $u_1 = 0$, or $u_3 = 0$, for then the parallelogram collapses. So set $\gamma = (\{\}, \{u_1, u_2, u_3\})$ and $B = \{\gamma\}$. This puts u_1, u_2, and u_3 in the red list. The effect is to tell the algorithm to assume that $u_1 \neq 0$,$u_2 \neq 0$, and $u_3 \neq 0$ throughout the course of the computations. The output from **REDGS2**$(B, I, [x_1, x_2])$ is $GS = \{(\gamma_1, G_1)\}$ where

$$(\gamma_1, G_1) = ((\{\}, \{u_1, u_2, u_3\}), \{u_1(2x_2 - u3), u_1u_3(2x_1 - (u_2+u_1))\}).$$

Clearly both conclusions follow from the hypotheseses; they form a Groebner Basis of I! The output gives a Groebner Basis for all specializations of the parameters for which u_i are nonzero. This is the generic case. (Time: 0.66 sec)

Example 3.1.5 Result: the Circle Theorem of Appollonius.
Let $A(0,0), B(u_1,0), C(0,u_2)$ be a right triangle in the plane (see figure 3.4) with right angle at A. Let $H(x_1,x_2)$ be the foot of the altitude drawn from A to the hypotenuse. The result is that the midpoints of all three sides and H all lie on one circle, the Appollonius Circle. By the diagram, we can set the hypotheses to be $h_1 =$ Collinear(B,H,C) and $h_2 =$ dotp$(C-B, H-A)$. This sets H as the foot of the altitude. We may write the conclusion as

$$g = \left(x_1 - \frac{u_1}{4}\right)^2 + \left(x_2 - \frac{u_2}{4}\right)^2 - \frac{u_1^2+u_2^2}{16}.$$

if $g \in \mathbf{I}(V)$ *where* $V = \mathbf{V}(h_1, \ldots, h_n)$.

Unfortunately, it often turns out that, in translating the geometric hypotheses to multivariable polynomials, these polynomials often allow for more solutions than are desired, i.e. there may exist some solutions to the hypotheses corresponding to degenerate geometric configurations. Furthermore, it may be the case that there exists some nonzero polynomials in just the parameters u_i alone inside I_h. In such cases, the conclusion g may not satisfy the above definiton (see section 4 of chapter 6 of [2]).

Definition 3.1.2 *Let* W *be an irreducible variety of* k^{m+n} *with coordinates* $u_1, \ldots, u_m, x_1, \ldots, x_n$. *We say that the functions* $u_1, \ldots, u_m$ *are* **algebraically independent on** W *if no nonzero polynomial in the* u_i *alone vanishes identically on* W.

The variety $V = \mathbf{V}(I_h)$ may be decomposed into its irreducible components. These may be grouped in two sets: ones for which the u_i are algebraically independent and those for which this is not the case. We will illustrate how the red list of a condition can be used to specify nonzero polynomial inequalities of the u_i alone.

To aid in translating geometric statments to polynomials, we wrote two functions "collinear" and "dotp." Collinear takes the coordinates of three points, $P(x_1, x_2)$, $Q(x_3, x_4)$, $Q(x_5, x_6)$ and returns the determinant

$$\text{Collinear}((x_1, x_2), (x_3, x_4), (x_5, x_6)) = \begin{vmatrix} x_1 & x_2 & 1 \\ x_3 & x_4 & 1 \\ x_5 & x_6 & 1 \end{vmatrix}.$$

Thus, the statment "the points P, Q, R are collinear" may be encoded as setting Collinear(P, Q, R) equal to zero (pg. 45 [6]).

Let $A(a_1, a_2)$, $B(b_1, b_2)$ be endpoints of the directed line segment $\overline{AB}$, and let $C(c_1, c_2)$, $D(d_1, d_2)$ be endpoints of $\overline{CD}$. Define dotp to be the usual dot product

We now give some examples from Automatic Geometric Theorem Proving and demonstrate how Comprehensive Groebner Bases may be used to eliminate unnecessary cases.

In general, suppose we have some constructive result from Euclidean Geometry. Typically, such results will be of the form: given some arbitrarily specified points in the plane, construct various other points by the intersections of lines, circles, perpendicular bisectors, etc. Then some conclusion is asserted regarding the constructed points.

For example, consider the result "the diagonals of a parallelogram must bisect each other." That is, for four given points $A(u_1, u_2)$, $B(u_2, u_3)$, $C(u_4, u_5)$, and $D(u_7, u_8)$ such that the convex polygon $ABDC$ is a parallelogram, let $P(x_1, x_2)$ be the constructed intersection point of the diagonals of the parallelogram. The result is that the line segments $\overline{AP} = \overline{PD}$, and $\overline{BP} = \overline{PC}$ (see the first example to follow).

It turns out [2] that the statement $ABDC$ is a parallelogram and the like have relatively simple translations into polynomials in $k[u_1, \ldots, u_m][x_1, \ldots, x_n]$. We will assume throughout that k is the field of real numbers.

So suppose $u_1, \ldots, u_m$ refer to the coordinates used to specify some arbitrary points in the plane, and $x_1, \ldots, x_n$ refer to coordinates used to specify the constructed points of some result. Let $h_1, \ldots, h_n \in S = k[u_1, \ldots, u_m][x_1, \ldots, x_n]$ be the polynomials corresponding to the hypotheses and set $g \in S$ as the conclusion. Let $I_h = \langle h_1, \ldots, h_n \rangle$ be the ideal generated by the hypotheses, and consider the corresponding variety $V = \mathbf{V}(I_h) = \mathbf{V}(h_1, \ldots, h_n)$. Note that I_h consists of all possible linear combinations of h_i with coefficients in S. So, we may think of I_h as containing all "polynomial consequences" of the h_i.

Definition 3.1.1 *The conclusion* g **follows strictly** *from the hypotheses*

$$h_1, \ldots, h_n$$

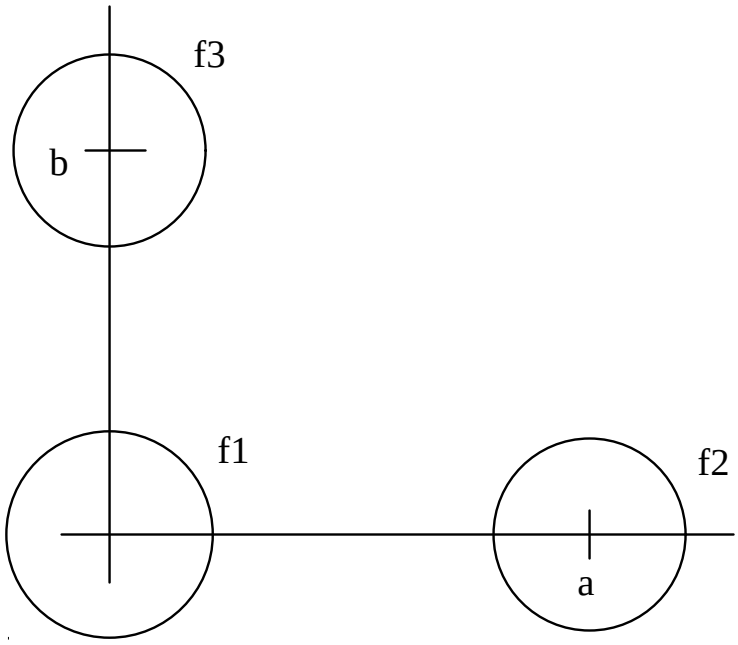

Figure 3.2, Three Circles

The second and the third cases are symmetric in a and b. Looking carefully at the second case we see that, since a is zero, the two circles f_1, f_2 coincide. The third circle intersects them both at either the one point $(0, \pm 1)$ for $b = \pm 2$, or at the points $(\pm\sqrt{4-b^2}/2, b/2)$ for $0 < b < 2$, (similarly, for $0 > b > 2$).

Finally, in the first case, V is empty, since the generator $ab(a^2+b^2-4)$ of G_1 is in the red list of γ_1. So under all specializations $\sigma \in \Sigma_{\gamma_1}$, we have $\sigma(a^2+b^2-4) \neq 0$. Thus this case tells us that, under all such specializations, we will have a nonzero field constant in $\sigma(G_1)$, and so the variety must be empty. In the case of k equal to the real numbers, we see geometrically that with (a, b) off the circle $a^2 + b^2 - 4$, if one circle (f_2 or f_3) gets close to $x^2 + y^2 = 1$, then the other must move away. Hence V is empty. It should be further noted that the problem of arbitrary radi of the circles increases the complexity significantly. (Time = 11.733 sec)

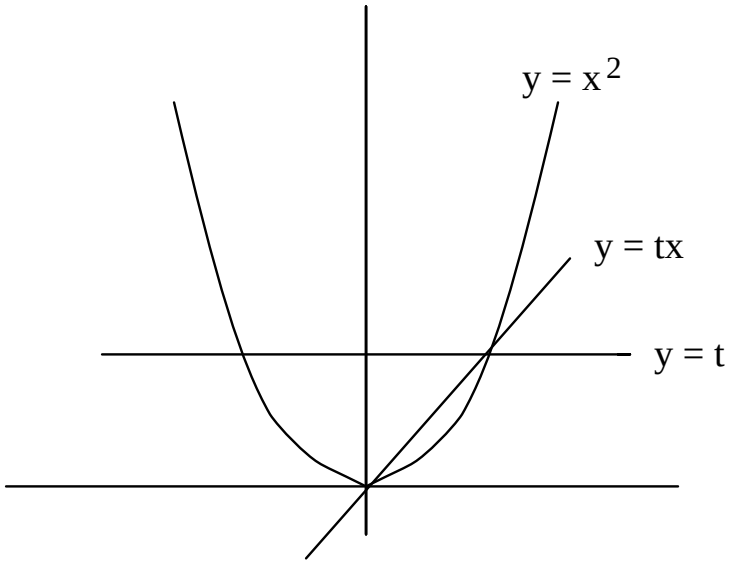

Figure 3.1, Parabola example

seem! The output from **REDGS2**$(B, I, [x, y])$ is a GS consisting of five reduced pairs. They are (after factoring):

$$\begin{aligned}
(\gamma_1, G_1) &= (((\{\}, \{2a, 2b, ab(a^2+b^2-4)\}), \{ab(a^2+b^2-4)\}),\\
(\gamma_2, G_2) &= (((\{a\}, \{2b\}), \{b(2y-b), b(4x^2+b^2-4)\}),\\
(\gamma_3, G_3) &= (((\{b\}, \{2a\}), \{a(2y-a), a(4y^2+a^2-4)\}),\\
(\gamma_4, G_4) &= (((\{a, b\}, \{\}), \{x^2+y^2+b^2-1\}),\\
(\gamma_5, G_5) &= (((\{a^2+b^2-4\}, \{2a, 2b\}), \{a(2x-a), b(2y-b)\}).
\end{aligned}$$

The fourth case is the easiest to interpret. In this case, all three circles coincide with the unit circle at the origin.

In the last case, $a^2+b^2=4$ since a^2+b^2-4 is in the green list of the condition γ_5. Further, a and b are nonzero since $2a$ and $2b$ are in the red list of γ_5. By G_5 we see that there is a unique solution, $(x, y) = (a/2, b/2)$. The reader will notice that this solution is in V. The symmetric solution is to take $a = \sqrt{2}$, $b = \sqrt{2}$, and then all three circles meet at $(\sqrt{2}/2, \sqrt{2}/2)$.

One sees how the algorithm has distinguished the two cases by the vanishing or nonvanishing of the determinant $ad - bc$. (Time = 1.583 sec)

Example 3.1.2 Let $I = \langle f_1, f_2 \rangle$ where $f_1 = x^2 - y, f_2 = (y - t)(y - tx)$ are in $k[t][x, y]$. Clearly, the variety $V = \mathbf{V}(I) = \mathbf{V}(f_1, f_2)$ changes for specializations of t and choice of field k. See figure 3.1 for a picture over the reals. Let $B = \{\gamma\}$, where $\gamma = (\{\}, \{\})$. Then **REDGS2**$(B, I, [x, y])$ gives $GS = \{(\gamma_1, G_1), (\gamma_2, G_2)\}$, where

$$\begin{aligned}(\gamma_1, G_1) &= ((\{\}, \{-t\}), \{x^2 - y, (y - t)(y - tx), y(y - t)(y - t^2)\}),\\ (\gamma_2, G_2) &= ((\{-t\}, \{\}), \{x^2 - y, y^2\}).\end{aligned}$$

The first pair gives a reduced Groebner Basis for all specializations of t to a nonzero constant in k, the second pair for when $t = 0$. For the first pair, we see that $\mathbf{V}(I)$ consists of (x, y), where (x, y) are in the set

$$\{(0, 0), (\pm\sqrt{t}, t), (\pm t, t^2)\}.$$

The actual number of solutions depends on the chosen field k to compute $\sqrt{t}$. The second pair gives a reduced Groebner Basis for $t = 0$. The only point in $\mathbf{V}(I)$ in this case is $(0, 0)$. (Time = 1.2 sec)

Example 3.1.3 Let $I = \langle f_1, f_2, f_3 \rangle$ with f_i in $k[a, b][x, y]$ given by,

$$\begin{aligned}f_1 &= x^2 + y^2 - 1,\\ f_2 &= (x - a)^2 + y^2 - 1,\\ f_3 &= x^2 + (y - b)^2 - 1.\end{aligned}$$

See figure 3.2 for a picture of three circles for x, y real. Take $B = \{\gamma\}$, with $\gamma = (\{\}, \{\})$. The problem again is to find all $(x, y) \in V = \mathbf{V}(I)$ for various specializations of the parameters a, b. The problem is not as obvious as it may

The main thrust of all the examples is to show how the initial case distinction and our other optimizations cut down on the sheer number of unnecessary cases. The idea is that the red list of a condition allows for the specification of polynomial inequalites in the parameters that are to hold throughout the course of the entire computation.

Our plan for this chapter is thus: we first show some nice examples of solving systems of equations in parameters, followed by examples from Automatic Geometric Theorem Proving. Next are examples showing how information concerning the resultant of two polynomials in a single variable becomes captured by the Groebner pairs. We also review an example in the paper of Weispfenning [7]. Lastly, we give our algorithm for computing a partial Groebner system. This algorithm has potential for obtaining information on the dimensions of parametric varieties for various specializations of the parameters. Our discussion of this algorithm uses the algorithm in chapter 9 of [2] for determining the dimension of the variety of a monomial ideal in the main variables.

3.1 Applications to Geometric Theorem Proving

Almost all the examples in this section were inspired by exercises in Chapter 6 of Cox, Little, and O'Shea [2]. These problems provided us with much good material to test the code and gauge its effectiveness in the course of the development. We first give some examples of solving systems of polynomial equations in parameters.

Example 3.1.1 Consider $I = \langle ax + by, cx + dy \rangle \subset k[a,b,c,d][x,y]$. The generic case is for a,b,c,d to be all nonzero. With $B = \{\gamma\}$, where $\gamma = (\{\}, \{a,b,c,d\})$, we encode this generic case to the algorithm. Then **REDGS2**$(B, I, [x,y])$ gives exactly two cases for solution with the determinant: $(\gamma_1, G_1), (\gamma_2, G_2)$ where

$$\begin{aligned} (\gamma_1, G_1) &= ((\{\}, \{a,b,c,d,ad-bc\}), \{(ad-bc)x, (ad-bc)y\}), \\ (\gamma_2, G_2) &= ((\{ad-bc\}, \{a,b,c,d\}), \{cx+dy\}). \end{aligned}$$

3 APPLICATIONS OF THE CONSTRUCTION

In this chapter we present a feast of examples of our Comprehensive Groebner Bases package in action. All examples (except where specifically noted) were run using our MACSYMA implementation of all the algorithms described in Chapter 2 on a Sun Sparc 10 workstation under Unix. Timing marks are those of MACSYMA by setting the internal variable SHOWTIME to true.

The examples of this chapter were chosen not so much for the computational complexity of the results, but rather for illustrative clarity of the method. We combined the **GROEBNERSYSTEM2** algorithm with the reduction algorithm **REDUCE SYSTEM** of appendix B together into one function call

REDUCED_GROEBNERSYSTEM2,

which we will abbreviate by **REDGS2**. The input to **REDGS2** is as in **GROEBNERSYSTEM2**:

(i) a case distinction $B = \{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ of initial conditions,

(ii) a list of polynomials

$$F = \{f_1, \ldots, f_n\} \subset S = k[u_1, \ldots, u_m][x_1, \ldots, x_n]$$

which are generators of the ideal $I = \langle F \rangle$, and

(iii) a list of main variables $[x_1, \ldots, x_n]$.

Unless specifically noted otherwise, the examples assumed LEX order on the main variables with $x_1 > x_2 > \ldots > x_n$. The **REDGS2** algorithm first calls **GROEBNERSYSTEM2** to get a $GS = \{(\gamma, G)\}$ and then calls the reduction algorithm on each pair of (γ, G). We will always give our examples by first listing the input, then showing the resulting reduced Groebner system, and then discussing the output.

where δ is the condition $\delta = (g, r')$, and r' consists of all elements of $r_i \equiv \tilde{r}_i \, I_{\mathrm{gr}(\gamma)}$, $r_i \in \mathrm{rd}(\gamma)$. The simplification of γ to δ may allow for simplier presentation of polynomial inequalities in the parameters.

By the same reasoning, if $f = \sum a_\alpha(U) x^\alpha \in G$, where $a_\alpha(U)$ is a polynomial in the parameters U, we may replace $a_\alpha(U)$ by its remainder modulo $I_{\mathrm{gr}(\gamma)}$. This again may allow for a simplier presentation of the Groebner Basis output polynomials in G (see the next chapter for examples).

its ID_CONTRACT command. Professor Marek R. Rychlik of the University of Arizona solved this problem by implementing the entire new construction in Lisp and was thus able to utilize other elimination orders.

Earlier in our researches for implementing these algorithms, we wrote a post-processor that would sweep out all contradictory cases from the Groebner system, AFTER, it had performed all computations. This lead to much unnecessary computations of S-polynomials and normals forms computed along branches that would be deleted anyway. Our new approach with **SAT DET** prunes the tree by not starting any branch with a contradictory condition as its starting node. Therefore, this new construction does not carry along *any* "virtual" Buchberger algorithms as discussed in the appendix of Becker and Weispfenning [1].

2.4.2 Two further Simplifications

In this section we describe two additional simplifications that may be performed on each Groebner Pair (γ, G) of a Grobner System GS. These simplifications lead to some nicer looking output.

First, suppose $r_i \in \mathrm{rd}(\gamma)$. By the division algorithm, we may write r_i in the form

$$r_i = \sum_{i=1}^{s} q_i g_i + \tilde{r_i}$$

where $\langle g_1, \ldots, g_s \rangle = I_{\mathrm{gr}(\gamma)}$. Thus r_i is **congruent modulo** $I_{\mathrm{gr}(\gamma)}$ to $\tilde{r_i}$. For any specialization, $\sigma \in \Sigma_\gamma$, we have

$$\sigma(r_i) = 0 + \sigma(\tilde{r_i}).$$

We see that replacing all the elements in the red list of γ by their remainders modulo the ideal generated by the green list of γ does not change the set Σ_γ. In other notations, for the sets of specializations of symbolic parameters Σ_γ and Σ_δ, we have

$$\Sigma_\gamma = \Sigma_\delta$$

of $\sigma(G)$ by our theorem 2.3.3. Again, because successor conditions preserve head terms, $\sigma(S_{ij}^{\delta})$ may still be deleted from the basis of syzygies of $\sigma(G)$ for all $\sigma \in \Sigma_{\delta}$, where $\delta \supset \gamma$. Therefore, there is no need to work with this pair of polynomials.

At the end of the routine, all triples (γ, G, P) will have $P = \emptyset$. All polynomial pairs $g_i, g_j \in G$ will, by construction, have the property that

$$\text{Spoly}_{\gamma}(g_i, g_j) \stackrel{G}{\Longrightarrow} k[\gamma].$$

Thus, as before in section 1.5,

$$\sigma(\text{Spoly}_{\gamma}(g_i, g_j)) = \text{Spoly}(\sigma(g_i), \sigma(g_j)) \stackrel{\sigma(G)}{\Longrightarrow} \sigma(k) = 0.$$

By lemma 2.3.1, $\text{Spoly}(\sigma(g_i), \sigma(g_j)) \rightarrow_{\sigma(G)} 0$. Therefore, all pairs in CLOSED are Groebner Pairs. **End**

2.4.1 Further Remarks on Implementations

Definition 2.4.1 *Given an ideal* $I = \langle f_1, \ldots, f_l \rangle \subset k[x_1, \ldots, x_n]$, *the* $k-th$ **elimination ideal** *of* I, *denoted by* I_k, *is the ideal of* $k[x_{k+1}, \ldots, x_n]$ *defined by*

$$I_k = I \cap k[x_{k+1}, \ldots, x_n].$$

Thus the proposition 2.1.2 shows that $I : r_1^{\infty} : \ldots : r_t^{\infty}$ is the $(t+1)$-st elimination ideal of I. By the **Elimination Theorem** [2], if G is a Groebner Basis for an ideal $I \subset k[x_1, \ldots, x_n]$ computed with respect to lex order with $x_1 > \cdots > x_n$, then for every $0 \leq k \leq n$, the set $G_k = G \cap k[x_{k+1}, \ldots, x_n]$ is a Groebner Basis of the k-th elimination ideal I_k of I. Thus we may compute a Groebner Basis for $I : r_1^{\infty} : \ldots : r_t^{\infty}$. Unfortunately, lex order can lead to some VERY large (in the sense of numbers of polynomials in the basis, their total degrees, and sheer number of terms for each polynomial) Groebner Bases. Other orders have been studied which allow one to eliminate only certain variables and not others. We refer the reader to the literature listed in [2]. MACSYMA always assumes the lex order in

g_i,g_j. Recall that the main idea was to first, compute k, the conditional normal form of this pairs' conditional S-polynomial; second, to determine k with respect to the current γ; and lastly, to form new triples for OPEN (replacing the current triple) depending on if k is to be put in G or not.

The new idea here is *not* to compute with the pair g_i, g_j if

LCM_TEST(γ, g_i, g_j) is FALSE and **CRITERION**(γ, i, j, G, P) is TRUE.

Our aim is to prove that all pairs (γ, G) of CLOSED have the property that, for all specializations $\sigma \in \Sigma_\gamma$, $\sigma(G)$ is a Groebner Basis of $\langle \sigma(G) \rangle$. By theorem 2.3.1 of the previous section, we need to show that all homogeneous syzygies S in a basis of syzygies for $S(\sigma(G))$ have the property that

$$S \cdot \sigma(G) \rightarrow_{\sigma(G)} 0. \tag{2.4}$$

If **LCM_TEST**(γ, g_i, g_j) is FALSE, then by our proposition 2.3.1, for all $\sigma \in \Sigma_\gamma$,

$$\sigma(\text{Spoly}_\gamma(g_i, g_j)) \rightarrow_G 0.$$

Hence,

$$S(\sigma(g_i), \sigma(g_j)) \rightarrow_{\sigma(G)} 0.$$

Since successor conditions δ to γ preserve conditional head terms, once **LCM_TEST**(γ, g_i, g_j) is FALSE for γ, it will stay false for all successors. Therefore, there is no need to work with this pair of polynomials.

If $\text{HM}_\gamma(g_i)$ and $\text{HM}_\gamma(g_j)$ are not relatively prime, the routine checks if **CRITERION**(γ, i, j, G, P) is TRUE. If this is the case, then S_{ij}^γ may be written as a linear combination of S_{ik}^γ and S_{jk}^γ. Having $[i,k] \notin P$ and $[j,k] \notin P$ means that the routine has, at some prior step, examined the S_{ik}^γ, and S_{jk}^γ (or with subscripts ik, jk reversed as appropriate). So, S_{ij}^γ may be deleted from a basis of homogeneous syzygies. Therefore, $\sigma(S_{ij}^\gamma)$ may be deleted from a basis of homogeneous syzygies

Analysis of GROEBNERSYSTEM2: Initialization step: We first saturate all conditions in the input case distinction B. Next, we eliminate all the contradictory ones after saturation. If there are none left, we exit the routine, i.e. if all conditions in B are contradictory at the start, then the routine quits. All conditions left in SB' are in saturated form and so may be passed to the saturated determine algorithm.

We now set Γ to the union of all covers of conditions in SB' necessary to determine the input list F. Next, after some intermediate checking, we have OPEN as the set of all triples (γ, G, P) where

(i) γ determines G,

(ii) $\mathrm{HM}_\gamma(g)$ is well-defined for all $g \in G$,

(iii) G is nonempty, and

(iv) P is the set of distinct pairs $\{i, j\}$ indexing polynomials in G.

It is a loop invariant that all triples in OPEN have the above properties. Again, P is to be viewed as pairs of polynomials in G whose conditional S-polynomial is yet to be examined by the routine. Lastly, we initialize the set CLOSED to be empty. The algorithm returns the Groebner System in this set. It is significant also to note that we only adjoin to any intermediate G a polynomial k with at least one *red* term. Consequently, all pairs (γ, G) in CLOSED will have $\mathrm{HM}_\gamma(g)$ defined for every $g \in G$.

After initialization, the routine searches OPEN for the first triple (γ, G, P) for which

(i) $P \neq \emptyset$, and

(ii) there exists a pair of subscripts $\{i, j\} \in P$ so that $\mathrm{HM}_\gamma(g_i)$ and $\mathrm{HM}_\gamma(g_j)$ are defined for $g_i, g_j \in G$.

In the previous **GROEBNERSYSTEM** algorithm, these two criteria were enough to set the flag "found" to true, and then perform arithmetic with the pair

Table 2.3, Algorithm **GROEBNERSYSTEM2**

Input: Case Distinction $B = \{\gamma\}$, list of distinct polynomials
$F = \{f_1, \ldots, f_n\}$, monomial order $\leq$
Output: A Groebner system $GS = \{(\gamma, G)\}$ for F over B

$SB := \{\mathbf{SAT\ CONDITION}(\gamma) \mid \gamma \in B\}$
$SB' := \{\beta \in SB \mid 1 \notin I_{\mathrm{gr}(\beta)}\}$
IF $SB' = \emptyset$ **THEN** Return($\emptyset$)
$\Gamma := \bigcup_{\beta \in SB} \{\mathbf{SAT\ DET}(\beta, F)\}$
OPEN:= $\bigcup_{\gamma \in \Gamma} \{(\gamma, \mathrm{NG}(\mathrm{col}^1_\gamma(F)))\}$
OPEN:= $\{(\gamma, G) \in \mathrm{OPEN} \mid G \neq \emptyset\}$
IF OPEN = $\emptyset$ **THEN** Return($\emptyset$)
OPEN:= $\{(\gamma, G, \mathrm{P}(|G|)) \mid (\gamma, G) \in \mathrm{OPEN}\}$
CLOSED:= $\emptyset$
WHILE OPEN $\neq \emptyset$ **DO**
found:=false
WHILE OPEN $\neq \emptyset$ **and** found = false**DO**
(γ, G, P):= pop(OPEN)
WHILE $P \neq \emptyset$ **and** found =false **DO**
pair:= pop(P) (=$\{i_0, j_0\}$)
$i := i_0, j := j_0$
IF $\mathrm{HM}_\gamma(g_i)$ **and** $\mathrm{HM}_\gamma(g_j)$ are defined **THEN**
found:= (**LCM TEST**(γ, g_i, g_j)) **and**
(∼**CRITERION**(γ, i, j, G, P))
IF found = false **THEN**
CLOSED:=CLOSED $\cup\{(\gamma, G)\}$
IF found = true **THEN**
h:=**GCD-SPOLY**$_\gamma(g_i, g_j)$
k:=**GCD-NORMALFORM**(γ, h, G)
Δ:= **SAT DET1**(γ, k)
$\Delta' := \{\delta \in \Delta \mid T_{red,\delta}(k) = \{a \cdot t \in T(k) \mid \mathrm{col}^1_\delta(a) = red\} \neq \emptyset\}$
OPEN:= OPEN
$\bigcup_{\delta \in \Delta'} \{(\delta, G \cup \{\mathrm{col}^1_\delta(k)\}, P \cup \{\{i, n+1\} \mid 1 \leq i \leq n\})\}$
$\bigcup_{\delta \in \Delta / \Delta'} \{(\delta, G, P)\}$
Return(CLOSED)

For **CRITERION**: Input:

(i) Condition γ,

(ii) pair i, j such that polynomials g_i,g_j in a set

$G = \{g_1, \ldots, g_t\}$ with $\mathrm{HM}_\gamma(g_i)$,$\mathrm{HM}_\gamma(g_j)$ defined,

(iii) the set G,

(iv) and P a set of distinct pairs $\{n, m\}$,

where $1 \leq n, m \leq |G|$.

Output: TRUE if there exist a $1 \leq k \leq |G|$, $k \neq i$, $k \neq j$, such that

(i) $[i, k] \notin P$, and $[j, k] \notin P$, and

(iii)$\mathrm{HM}_\gamma(g_k)$ divides $\mathrm{LCM}(\mathrm{HM}_\gamma(g_i), \mathrm{HM}(g_j))$,

(where $[i, j] = (i, j)$ if $i < j$ else (j, i))

FALSE otherwise.

Let G be a set of polynomials determined with respect to some γ. Denote by $\mathrm{NG}(G)$ (read: "not *green* of G") the function sending G to the set

$$\mathrm{NG}(G) = \{g \in G \,|\, \text{not all terms of } g \text{ are } \textit{green}\}.$$

So all polynomials in $\mathrm{NG}(G)$ are not totally *green*, and they all have well-defined $\mathrm{HM}_\gamma(g)$, for all $g \in \mathrm{NG}(G)$. Lastly, define the function, $\mathrm{P}(n)$, for n a positive integer, by

$$\mathrm{P}(n) = \begin{cases} \emptyset & \text{if } n = 1 \\ \{\{i, j\} \,|\, 1 \leq i < j \leq n\} & \text{otherwise.} \end{cases}$$

The algorithm of Table 2.3 uses all of the above functions. In the remainder of this section we explain how all the optimizations work in this algorithm. As in section 1.5, one can easily construct Comprehensive Groebner Bases from the output. Furthermore, this output may be then used as input to the reduction algorithm in appendix B.

- Saturated conditions,
- Conditional syzygies, and
- Gcd use in S-poly and Normal Form computations.

Recall from section 2.1 that input conditions

$$\gamma = (g, r) = (\{g_1, \ldots, g_s\}, \{r_1, \ldots, r_t\})$$

to **SAT DET1** and **SAT DET** had to be in saturated form. Thus, we wrote a simple function **SAT CONDITION** that takes a given condition γ and returns a new condition $\gamma' = (g', r)$ where $g' = I_g : r_1^\infty : \ldots : r_t^\infty$. With MACSYMA, this was accomplished by the command

$$g' = \text{ID\_CONTRACT}([g_1, \ldots, g_s, 1 - y_1 r_1, \ldots, 1 - y_t r_t], [u_1, \ldots, u_m]).$$

This computes a reduced (hence minimal) Groebner Basis for

$$\tilde{I} \cap k[u_1, \ldots, u_m] = I_g : r_1^\infty : \ldots : r_t^\infty$$

where $\tilde{I} = \langle g_1, \ldots, g_s, 1 - y_1 r_1, \ldots, 1 - y_t r_t \rangle$. To utilize the reductions in the previous section we also wrote two algorithms **LCM TEST** and **CRITERION**. We now describe their inputs and outputs.

For **LCM TEST**:

Input: Condition γ, polynomials g_i,g_j with $\text{HM}_\gamma(g_i)$,$\text{HM}_\gamma(g_j)$ defined.

Output: TRUE if

$$\text{LCM}(\text{HM}_\gamma(g_i), \text{HM}_\gamma(g_j)) \neq \text{HM}_\gamma(g_i)\text{HM}_\gamma(g_j),$$

FALSE otherwise.

Thus the algorithm returns FALSE if the conditional head monomials are relatively prime.

By hypothesis, $\mathrm{HM}(g_i), \mathrm{HM}(g_j)$ and $\mathrm{HM}(g_k)$ divide t_{ij}. So, the fractions $\frac{t_{ij}}{t_{ik}}, \frac{t_{ij}}{t_{jk}}$ are indeed monomials. Computation gives

$$S_{ij} = \frac{t_{ij}}{t_{ik}} S_{ik} - \frac{t_{ij}}{t_{jk}} S_{jk}$$

and ends the proof.

The main point of the theorem is that S_{ij} is linearly dependent on the two syzygies S_{ik} and S_{jk}.

We use this theorem to prove our result.

Theorem 2.3.3 *Let γ be a condition, and $G = (g_1, \ldots, g_t) \subset S$ be such that $\mathrm{HM}_\gamma(g_i)$ are all defined. Suppose also that we have a subset $\mathcal{S} \subset \{S_{ij}^\gamma \,|\, 1 \leq i < j \leq t\}$ which is a basis of $S(G)$. Suppose also that there exist distinct elements $g_i, g_j, g_k \in G$ such that*

$$\mathrm{HM}_\gamma(g_k) \text{ divides } \mathrm{LCM}(\mathrm{HM}_\gamma(g_i), \mathrm{HM}_\gamma(g_j)).$$

Then if $S_{ik}^\gamma, S_{jk}^\gamma \in \mathcal{S}$, then for every $\sigma \in \Sigma_\gamma$, $\sigma(\mathcal{S}) - \{\sigma(S_{ij}^\gamma)\}$ is a basis of $S(\sigma(G))$.

Proof: By the previous proof, we have S_{ij}^γ as a linear combination of S_{ik}^γ and S_{jk}^γ. So for any $\sigma \in \Sigma_\gamma$, we have $\sigma(S_{ij}^\gamma)$ as a linear combination of the specializations of S_{ik}^γ and S_{jk}^γ. Hence, this $\sigma(S_{ij}^\gamma)$ may be excluded from the basis $\sigma(\mathcal{S})$ of syzygies of $\sigma(G)$. End of proof.

2.4 The New Construction

In this section we present our new main algorithm **GROEBNERSYSTEM2** in table 2.3 that constructs a Groebner System, as defined in section 1.5. This algorithm uses the optimizations and theory of

- New Coloring Criteria,

form a finite basis of $S(F)$. The same is true in the conditional case. It also turns out that the Buchberger criterion may be recast using the language of syzygies. The main result is [2]

Theorem 2.3.1 *A basis $G = (g_1, \ldots, g_t)$ for an ideal $I \subset R$ is a Groebner Basis if and only if for every element $S = (h_1, \ldots, h_t)$ in a homogeneous basis for the syzygies $S(G)$, we have*

$$S \cdot G := \sum_{i=1}^{t} h_i g_i \rightarrow_G 0.$$

Proposition 4 pg. 103 of [2] (of which our proposition 2.3.1 is the generalization), shows that if g_i, $g_j \in R$ have relatively prime head monomials, then

$$S_{ij} \cdot G = S(g_i, g_j) \rightarrow_G 0.$$

Thus it is not necessary to check that $S_{ij} \cdot G$ reduces to zero modulo G in such a case. It also turns out that, under the condition of the next theorem, some basis elements of a homogeneous basis of syzygies for $S(G)$ need not be examined (see Proposition 10 of [2]).

Theorem 2.3.2 *Given $G = (g_1, \ldots, g_t)$, suppose that we have a subset $\mathcal{S} \subset \{S_{ij} \,|\, 1 \leq i < j \leq t\}$ which is a basis of $S(G)$. Suppose also that there exist distinct elements $g_i, g_j, g_k \in G$ such that*

$$\mathrm{HM}(g_k) \textit{ divides } \mathrm{LCM}(\mathrm{HM}(g_i),\mathrm{HM}(g_j)).$$

If $S_{ik}, S_{jk} \in \mathcal{S}$, then $\mathcal{S} - \{S_{ij}\}$ is still a basis of $S(G)$. (Note: if $i > j$, set $S_{ij} = S_{ji}$).

Proof: Let

$$\begin{aligned} t_{ij} &= \mathrm{LCM}(\mathrm{HM}(g_i), \mathrm{HM}(g_j)), \\ t_{ik} &= \mathrm{LCM}(\mathrm{HM}(g_i), \mathrm{HM}(g_k)), \text{and} \\ t_{jk} &= \mathrm{LCM}(\mathrm{HM}(g_j), \mathrm{HM}(g_k)). \end{aligned}$$

The analogous definition of a **conditional homogenous syzygy of multidegree** α is clear.

Definition 2.3.5 *Let γ be a condition and $F = (f_1, \ldots, f_s)$ be an s-tuple of polynomials, $f_i \in S$ such that $HM_\gamma(f_i)$ are all defined. Then, for any pair $i < j$, let t_0 = LCM(HM$_\gamma(f_i)$,HM$_\gamma(f_j)$), and*

$$s_i = \mathrm{HM}_\gamma(f_i), s_j = \mathrm{HM}_\gamma(f_j),$$

and set

$$S_{ij}^\gamma = \mathrm{HM}_\gamma(f_j) \cdot s_i \, \boldsymbol{e}_i - \mathrm{HM}_\gamma(f_i) \cdot s_j \, \boldsymbol{e}_j.$$

Then $S_{i,j}^\gamma$ is a **homogeneous syzygy** *of* multidegree(t_0) *of the pair f_i,f_j.*

We see that each S_{ij}^γ corresponds to the conditional S-polynomial on leading monomials of f_i, f_j.

Lemma 2.3.2 *If $S = (h_1, \ldots, h_s)$ is any conditional syzygy of $F = (f_1, \ldots, f_s)$, then for all $\sigma \in \Sigma_\gamma$, we have that $\sigma(S) = (\sigma(h_1), \ldots, \sigma(h_s))$, with $\sigma(h_i) \in R$, is a syzygy on the head monomials of $\sigma(F) = (\sigma(f_1), \ldots, \sigma(f_s))$.*

Proof: Let γ be a condition and $f \in S$ with HM$_\gamma(f)$ defined. For every $\sigma \in \Sigma_\gamma$, we have HM$_\gamma(f)$ = HM$(\sigma(f))$. Since,

$$\sum_{i=1}^{s} h_i \mathrm{HM}_\gamma(f_i) = 0,$$

upon specialization by σ we have,

$$\sum_{i=1}^{s} \sigma(h_i) \mathrm{HM}(f_i) = 0.$$

End of proof.

In particular, S_{ij}^γ corresponds under specialization to a syzygy of form S_{ij}.

Now, it turns out (see lemma 7 pg. 105 of [2]) that every element of $S(F)$ may be written uniquely as a sum of homogeneous syzygies, and that the syzygies S_{ij}

Definition 2.3.3 *A syzygy $S \in S(F)$ is* **homogeneous of multidegree** $\alpha \in Z^n_{\geq 0}$ *if*

$$S = (c_1 x^{\alpha_1}, \ldots, c_s x^{\alpha_s})$$

where $c_i \in k$ and for all nonzero c_i, $\alpha_i + multidegree(f_i) = \alpha$.

A homogeneous syzygy is then just a syzygy so that all terms, $c_i x^{\alpha_i} \mathrm{HM}(f_i)$, in linear combination with the head monomials of f_i have multidegree α. Note that, by our defintion of syzygy, the cancellation to zero must come from the sum $\sum_{i=1}^{s} c_i$.

Let (f_i, f_j) be a pair of distinct polynomials of $F = \{f_1, \ldots, f_s\} \subset R$, with $i < j$. Let $t_0 = \mathrm{LCM}(\mathrm{HM}(f_i), \mathrm{HM}(f_j))$, and

$$s_i = t_0/\mathrm{HM}(f_i), s_j = t_0/\mathrm{HM}(f_j).$$

Then we define the homogeneous syzygy

$$\begin{aligned} S_{ij} &= \mathrm{HC}(f_j) \cdot s_i \, \mathbf{e}_i - \mathrm{HC}(f_i) \cdot s_j \, \mathbf{e}_j \\ &= (0, \ldots, \mathrm{HC}(f_j) \cdot s_i \, , 0, \ldots, 0, \mathrm{HC}(f_i) \cdot s_j \, , 0, \ldots, 0). \end{aligned}$$

It is easy to see that S_{ij} has multidegree(t_0). This syzygy corresponds to the S-polynomial between f_i and f_j.

We may readily define conditional versions of the above as follows:

Definition 2.3.4 *Let γ be a condition and $F = (f_1, \ldots, f_s)$ be an s-tuple of polynomials, $f_i \in S$, such that $HM_\gamma(f_i)$ are all defined. A* **conditional syzygy** *on the conditional head monomials of each f_i of F is an s-tuple of polynomials*

$$S = (h_1, \ldots, h_s),$$

$h_i \in S$ such that

$$\sum_{i=1}^{s} h_i \mathrm{HM}_\gamma(f_i) = 0.$$

(it is not necessarily the conditional head monomial of q). This equation then implies

$$\text{monom1}(\sigma(q))\text{HM}_\gamma(f) = \text{monom1}(\sigma(p))\text{HM}_\gamma(g).$$

Thus $\text{HM}_\gamma(f)$ would divide $\text{monom1}(\sigma(p)) \leq \text{HM}_\gamma(f)$ since $\text{HM}_\gamma(f)$ and $\text{HM}_\gamma(g)$ are relatively prime. This is a contradiction. Hence, in all cases, equation 2.3 holds. Therefore, we have written $\sigma(\text{Spoly}_\gamma(f,g)) \in R$ in the desired form. End of proof.

This result says that if we know in advance that the conditional head monomials of two polynomials are relatively prime, then their specialized S-polynomial is gauranteed to reduce to zero modulo the specialized set G. We will use this result in the next section.

We also want to make use of results on bases of syzygy polynomials. Our definition below uses leading monomials only (see [2]).

Definition 2.3.2 *Let $F = (f_1, \ldots, f_s)$ be a s-tuple of polynomials in R. A* **syzygy** *on the leading monomials of each f_i of F is an s-tuple of polynomials*

$$S = (h_1, \ldots, h_s),$$

$h_i \in R$, such that

$$\sum_{i=1}^{s} h_i \text{HM}(f_i) = 0.$$

So we see that a syzygy provides the coefficient polynomials needed to make the above linear combination of leading monomials zero. That is, a syzygy provides the necessary "alignment" to make the sum of leading monomials zero. Let $S(F)$ be the vector space of all syzygies of F (under vector addition and scalar multiplication by a polynomial). Let $\mathbf{e}_i$ be the s-tuple of polynomials in R with the polynomial 1 in the i-th place. We can write $S \in S(F)$ as $S = \sum_{i=1}^{s} h_i \, \mathbf{e}_i$.

Proof: Let $f = \mathrm{HC}_\gamma(f)\mathrm{HM}_\gamma(f) + p$, and $g = \mathrm{HC}_\gamma(g)\mathrm{HM}_\gamma(g) + q$. Since the conditional head monomials are relatively prime, we have

$$\begin{aligned}
\mathrm{Spoly}_\gamma(f,g) &= \mathrm{HC}_\gamma(g)\cdot\mathrm{HM}_\gamma(g)f - \mathrm{HC}_\gamma(f)\cdot\mathrm{HM}_\gamma(f)g \\
&= \mathrm{HC}_\gamma(g)\left(\frac{g-q}{\mathrm{HC}_\gamma(g)}\right)f - \mathrm{HC}_\gamma(f)\left(\frac{f-p}{\mathrm{HC}_\gamma(f)}\right)g \\
&= (-q)f + (p)g.
\end{aligned}$$

Let $\sigma \in \Sigma_\gamma$. As in lemma 1.3.1,

$$\begin{aligned}
\mathrm{HM}_\gamma(f) &= \mathrm{HM}(\sigma(f)), and \\
\mathrm{HM}_\gamma(g) &= \mathrm{HM}(\sigma(g)).
\end{aligned}$$

We claim that

$$\mathrm{multidegree}(\sigma(\mathrm{Spoly}_\gamma(f,g))) = \max(\mathrm{multidegree}(\sigma(qf)), \mathrm{multidegree}(\sigma(pg))). \tag{2.3}$$

Now, $\sigma(q)$, $\sigma(p)$ are either zero or not in R. If they are both zero, then so is $\sigma(\mathrm{Spoly}_\gamma(f,g))$, and equation 2.3 holds. If one is zero, and the other is nonzero, equation 2.3 still holds. Finally, if both $\sigma(q)$, $\sigma(p)$ are nonzero, then

$$\sigma(\mathrm{Spoly}_\gamma(f,g)) = -\sigma(q)\sigma(f) + \sigma(p)\sigma(g).$$

The leading monomials of the products $\sigma(q)\sigma(f)$ and $\sigma(p)\sigma(g)$ are distinct (hence, they do not cancel in the sum above). To see this, note that if the leading monoomials were the same, we would have

$$\mathrm{monom1}(\sigma(q))\mathrm{HM}(\sigma(f)) = \mathrm{monom1}(\sigma(p))\mathrm{HM}(\sigma(g))$$

where $\mathrm{monom1}(\sigma(q))$ ($\mathrm{monom1}(\sigma(p))$) is the first (greatest) monomial of

$$\sigma(q)\ (\sigma(p)) \in R$$

For the rest of this section, we discuss how we implemented the two optimizations in section 9 of chapter 2 of [2] in the algorithm **GROEBNERSYSTEM2**. The idea of these optimizations is to reduce the number of critical pairs of S-polynomials the algorithm must examine. We outline the main ideas and formulate conditional versions of defintions and theorems. Recall that we set $R = k[x_1, \ldots, x_n]$.

Definition 2.3.1 *Fix a monomial order and let $G = \{g_1, \ldots, g_t\} \subset R$. Given $f \in R$, we say that f* **reduces to zero modulo** *G, written $f \rightarrow_G 0$, if f may be written in the form $f = \sum_{i=1}^{t} a_i g_i$, such that whenever $a_i g_i \neq 0$, we have* multidegree$(f) \geq$ multidegree$(a_i g_i)$.

By the usual division algorithm, the nonzero quotient terms $a_i g_i$, obtained when dividing some $f \in R$ by a list $g_1, \ldots, g_t$, satisfy the multidegree inequality of this definition. Hence we have the following easy lemma.

Lemma 2.3.1 *Let $G = (g_1, \ldots, g_s)$ be an ordered set of elements of R, and fix $f \in R$. Then, if the normal form of f modulo G is zero, then $f \rightarrow_G 0$.*

The next proposition is ours and is a conditional version of Prop. 4 pg. 103 of [2].

Proposition 2.3.1 *Let γ be a condition, and $f, g \in S$ be two distinct polynomials in a finite set $G \subset S$ such that $\mathrm{HM}_\gamma(f)$ and $\mathrm{HM}_\gamma(g)$ are well-defined. Suppose further that*

$$\mathrm{LCM}(\mathrm{HT}_\gamma(f), \mathrm{HT}_\gamma(g)) = \mathrm{HT}_\gamma(f)\mathrm{HT}_\gamma(g).$$

Then, for all $\sigma \in \Sigma_\gamma$, we have

$$\sigma(\mathrm{Spoly}_\gamma(f, g)) \rightarrow_{\sigma(G)} 0.$$

the length of the computations in **GROEBNERSYSTEM**. For efficiency, we made use of $d = \mathrm{GCD}(\mathrm{HC}_\gamma(f), \mathrm{HC}_\gamma(g))$. Using the notation above, define

$$\text{GCD-Spoly}_\gamma(f,g) = \left(\frac{\mathrm{HC}_\gamma(g)}{d}\right) \cdot s \cdot f - \left(\frac{\mathrm{HC}_\gamma(f)}{d}\right) \cdot t \cdot g.$$

This difference cancels (at least) the common term

$$\frac{\mathrm{HC}_\gamma(f)\mathrm{HC}_\gamma(g)}{d} \cdot t_0 = \mathrm{LCM}(\mathrm{HC}_\gamma(f), \mathrm{HC}_\gamma(g)) \cdot t_0$$

and is less costly since we are multiplying f (g) by smaller polynomials. We will refer to the algorithm that uses this construction as **GCD-SPOLY**$_\gamma(f,g)$.

Recall next that the conditional normal form of a given polynomial f, with respect to a set of polynomials P, relative to a condition γ, was a polynomial obtained by a chain of iterated reductions of the form $f \xrightarrow{p} g[\gamma]$. This meant that $\mathrm{HT}_\gamma(p)$ is defined and

$$g = \mathrm{HC}_\gamma(p) \cdot f - a \cdot s \cdot p \tag{2.2}$$

where, $a \cdot t$ is a term of f with $t \in T_{red}(f) \cup T_{white}(f)$, $\mathrm{HM}_\gamma(p)$ divides t, and $s = t/\mathrm{HM}_\gamma(p)$. This difference cancels (at least) the common term

$$a \cdot \mathrm{HC}_\gamma(p) \cdot t$$

but, again, at the high, computational, cost of multiplying all terms of f by $\mathrm{HC}_\gamma(p)$ and all terms of p by a. So, let $d = \mathrm{GCD}(a, \mathrm{HC}_\gamma(p))$. Using the notation above, we now redefine the subtraction step in equation 2.2 as

$$g = \left(\frac{\mathrm{HC}_\gamma(p)}{d}\right) \cdot f - \left(\frac{a}{d}\right) \cdot s \cdot p.$$

This difference cancels (at least) the common term

$$\frac{a\mathrm{HC}_\gamma(p)}{d} \cdot t = \mathrm{LCM}(a, \mathrm{HC}_\gamma(p)) \cdot t$$

and is again less costly. We will refer to the algorithm that uses iterated reductions of this form as **GCD-NORMALFORM**(γ, f, P).

Finally then, we have that $S_\gamma = \emptyset$ implies $1 \in I_g : r_1^\infty : \ldots : r_t^\infty$. Thus, γ is contradictory. Again, this is not true of γ. Therefore, S_γ cannot be empty. This ends the proof.

Remark 3 The proof shows much more. If γ is contradictory, we clearly have $\Sigma_\gamma = \emptyset$. Since any prime ideal π is also radical, we have that if γ is contradictory, then S_γ is empty also. Therefore, over an algebraically closed field, γ is contradictory if and only if Σ_γ and S_γ are empty!

In closing we further remark that our saturated representation of γ is then the optimal choice in the sense that we eliminate all possibilities for problems to occur with specializations of parameters. Thus we continue to carry a lot of information in the green and red lists of any given condition.

2.3 Further Optimizations

In this section we describe some optimizations we implemented for use in our main algorithm **GROEBNERSYSTEM2** of the next section. First, recall the pseudo-division definitions for the Conditional S-polynomial. Let γ be a condition, and let $f, g \in S = P[x_1, \ldots, x_n] = k[u_1, \ldots, u_m][x_1, \ldots, x_n]$ with $\mathrm{HT}_\gamma(f)$, $\mathrm{HT}_\gamma(g)$ defined. Then $\mathrm{Spoly}_\gamma(f, g)$ was defined by

$$\mathrm{Spoly}_\gamma(f, g) = \mathrm{HC}_\gamma(g) \cdot s \cdot f - \mathrm{HC}_\gamma(f) \cdot t \cdot g$$

where $s = t_0/\mathrm{HM}_\gamma(f)$, $t = t_0/\mathrm{HM}_\gamma(g)$, and $t_0 = \mathrm{LCM}(\mathrm{HM}_\gamma(f), \mathrm{HM}_\gamma(g))$. This difference subtracts (at least) the common term

$$\mathrm{HC}_\gamma(f) \cdot \mathrm{HC}_\gamma(g) \cdot t_0$$

but at a cost of multiplying *all* terms of f (g) by $\mathrm{HC}_\gamma(g)$ $(\mathrm{HC}_\gamma(g))$. Thus the coefficients of the resulting difference can bceome VERY large VERY quickly over

Thus, $\Sigma_\gamma = \emptyset$ implies γ is contradictory. But this is not true of γ. Therefore, Σ_γ cannot be empty.

We now argue, again by contradiction, that S_γ cannot be empty. First note, by definition, that $S_\gamma = \emptyset$ if and only if for all prime ideals π either

(1) there exists an $f \in I_g - \pi$, or

(2) there exists an $r_i \in r \cap \pi$.

By the Lasker-Noether theorem, we may write

$$I_g = \cap_{i=1}^{r} Q_i$$

where Q_i are primary ideals and the decomposition is minimal. Set $P_i = \sqrt{Q_i}$. Each P_i is then the smallest prime ideal (hence also radical and primary) containing Q_i. Suppose alternative (1) above holds, and there exist some $f \in I_g - P_i$ for some $1 \leq i \leq r$. Then, since $f \in I_g$, f is also in every Q_i of the decomposition, and we have

$$f \in Q_i \subseteq \sqrt{Q_i} = P_i.$$

But this contradicts (1) since each P_i is a prime ideal in $\mathrm{Spec}(P)$. Therefore, $S_\gamma = \emptyset$ if and only if alternative (2) above holds, i.e. for any prime ideal π, there always exists some $r_i \in r \cap \pi$. So, pick an $r_i \in r \cap P_i$ for each Q_i in the decomposition of I_g. By definition of P_i, there exists an integer $n_i > 0$ so that $r_i^{n_i} \in Q_i$, for each $i = 1, \ldots, t$. Since each Q_i is primary, and $r_i^{n_i}$ is in it, we have that

$$Q_i : r_i^{n_i} = \{f \in P \mid f r_i^{n_i} \in Q_i\} = \langle 1 \rangle.$$

Doing some arithmetic with the quotients, gives

$$\begin{aligned} I_g : r_1^\infty : \ldots : r_t^\infty &\supseteq I_g : r_1^{n_1} : \ldots : r_t^{n_t} \\ &= \left(\cap_{i=1}^{t} Q_i\right) : r_1^{n_1} : \ldots : r_t^{n_t} \\ &= \cap_{i=1}^{t} (Q_i : r_i^{n_i}) \\ &\supseteq \langle 1 \rangle. \end{aligned}$$

Definition 2.2.1 *An ideal I in P is* **primary** *if $fg \in I$ implies either $f \in I$ or some power $g^m \in I$ (for some $m > 0$).*

Definition 2.2.2 *A* **primary decomposition** *of an ideal is an expression of I as an intersection of primary ideals: $I = \cap_{i=1}^{r} Q_i$. It is called* **minimal** *or* **irredundant** *if the radicals $\sqrt{Q_i}$ are all distinct and $Q_i \not\supset \cap_{j \neq i} Q_j$.*

Also relevant to us here is the fact that (see pgs. 208-210 of [2]) if I is primary, then its radical is prime, and is the smallest prime ideal containing I.

Theorem 2.2.2 (Lasker-Noether) *Every ideal $I \subset P$ has a minimal primary decomposition.*

We now give the proof of our Theorem 2.2.1.

Proof: Let

$$\gamma = (g, r) = (\{g_1, \ldots, g_s\}, \{r_1, \ldots, r_t\}),$$

be a condition in saturated form. As noted, by proposition 2.1.3 and corrollary 2.1.1, γ is not contradictory.

We now argue that $\Sigma_\gamma \neq \emptyset$. We may think of each $\sigma \in \Sigma_\gamma$ as mapping the symbolic parameter m-tuple $(u_1, \ldots, u_m)$ to a point $(a_1, \ldots, a_m)$ of the subset $S \subset k^m$ (not necessarily a variety), where

$$S = \mathbf{V}(I_g) - \bigcup_{i=1}^{t} \mathbf{V}(r_i).$$

Assuming k algebraically closed, we have the equivalences:

$$\begin{aligned}
\Sigma_\gamma = \emptyset \quad &\leftrightarrow \quad \mathbf{V}(I_g) = \bigcup_{i=1}^{t} \mathbf{V}(r_i) \\
&\leftrightarrow \quad \mathbf{I}(\mathbf{V}(I_g)) = \mathbf{I}\left(\bigcup_{i=1}^{t} \mathbf{V}(r_i)\right) = \mathbf{I}(\mathbf{V}(r_i r_j : 1 \leq i, j \leq t)) \\
&\leftrightarrow \quad \sqrt{I_g} = \mathbf{I}(\mathbf{V}(r_i r_j : 1 \leq i, j \leq t)) \supset \{r_i r_j \mid 1 \leq i, j \leq t\}.
\end{aligned}$$

(iii) $\sigma_\pi(f) = \Psi(f + \pi)$ where Ψ is the canonical ring isomorphism $\Psi : P/\pi \to \sigma_\pi(P)$.

Thus, $\sigma_\pi = \Psi \circ \Phi$ where Φ is the natural map taking f to its coset $f + \pi \in P/\pi$. If $g_i \in g \subset \pi$, then $\sigma_\pi(g_i) = 0$. If $r_i \in r$, then since $r \cap \pi = \emptyset$, $r_i \notin \ker(\sigma_\pi)$. So, $\sigma_\pi(r_i) \neq 0$. Therefore, $\sigma_\pi \in \Sigma_\gamma$.

The declaration, $\sigma_\pi(f) = 0$ for all $f \in \pi$, essentially imposes a set of polynomial constraints on the symbolic parameters u_i; i.e. the parameters must satisfy the polynomial equations $\sigma_\pi(f) = 0$. We may see this more explicitly in the case k is algebraically closed. For then, let I be a maximal ideal (hence, prime and radical) so that $I \supseteq I_{\mathrm{gr}(\gamma)}$. Such ideals do exist for any I_g (see [4]). By Theorem 11, pg. 200 of [2], I has the form

$$I = \langle u_1 - a_1, \ldots, u_m - a_m \rangle$$

for some point $a = (a_1, \ldots, a_m) \in k^m$. We see that the declaration $\sigma_I(f) = 0$, for all $f \in I$, amounts to setting each parameter $u_i = a_i$. Furthermore, $\Phi(f) = f + I = r + I$, where r is the remainder of f when divided by the generators $\{u_1 - a_1, \ldots, u_m - a_m\}$ of I, i.e. $f = \sum q_i(u_i - a_i) + r$. Since, $\mathrm{gr}(\gamma) \subset I$, we have $\sigma_I(g) = \Psi(\Phi(g)) = \Psi(I) = 0$, for all $g \in \mathrm{gr}(\gamma)$. Since, $\mathrm{rd}(\gamma) \cap I = \emptyset$, for all $r_i \in \mathrm{rd}(\gamma)$ we have $\sigma_I(r_i) = \Psi(r_i + I) = \Psi(\tilde{r_i} + I) = \tilde{r_i}(a) \neq 0$, where $\tilde{r_i}$ is the remainder upon division of r_i by generators of I. Thus we see that $\sigma_I \in \Sigma_\gamma$.

We now state our main result signifying the importance of the saturated form of a condition.

Theorem 2.2.1 *Let γ be a condition in saturated form. Then if k is algebraically closed, both Σ_γ and S_γ are nonempty.*

Our proof will require use of the Lasker-Noether Theorem [2]. We need some preliminary definitions.

Table 2.2, Algorithm **SAT DET**

Input: Condition γ in saturated form, list of polynomials F
Output: Cover Γ of consisting solely of non-contradictory successors δ to γ, in saturated form, that determines F

IF $F = \emptyset$ **THEN**
$\Gamma := \{\gamma\}$
ELSE
$\Gamma := \bigcup_{\delta \in \mathbf{SAT\ DET1}_{(\gamma, f_1)}} \mathbf{SAT\ DET}(\delta, F - \{f_1\})$
Return(Γ)

---

in this form, we ensure that no output Groebner pair from the **GROEBNER-SYSTEM2** algorithm will have Σ_γ empty. In this section, we also show some relationships between this representation of a condition and the ideal theoretic viewpoint of specializations given in the paper by Weisspfenning [7].

As in that paper, let $\mathrm{Spec}(P) = \{\text{all prime ideals } \pi \subset P\}$. Then, the **spectrum of a condition** $\gamma = (g, r)$ is defined to be

$$\mathrm{S}_\gamma = \{\pi \in \mathrm{Spec}(P) \,|\, g \subset \pi, \text{ and } r \cap \pi = \emptyset\}.$$

We observe that if $g \subset \pi$, then $I_g \subset \pi$ also. Recall from chapter 1,

$$\Sigma_\gamma = \{\sigma \in \Sigma \,|\, \sigma(g) = 0, \forall g \in \mathrm{gr}(\gamma), \text{ and } \sigma(r) \neq 0, \forall r \in \mathrm{rd}(\gamma)\}.$$

So, given any $\sigma \in \Sigma_\gamma$, one sees that $\ker(\sigma) \in \mathrm{Spec}(P)$, $\mathrm{gr}(\gamma) \subset \ker(\sigma)$, and $\mathrm{rd}(\gamma) \cap \ker(\sigma) = \emptyset$. Hence, $\ker(\sigma) \in \mathrm{S}_\gamma$. Therefore, any specialization $\sigma \in \Sigma_\gamma$ corresponds to a prime ideal of S_γ.

Conversely, for any prime ideal $\pi \in \mathrm{S}_\gamma$, we may define a specialization $\sigma_\pi \in \Sigma_\gamma$ as follows: declare

(i) $\sigma_\pi =$ identity on k,

(ii) $\sigma_\pi(f) = 0$ for all $f \in \pi$, (so $\ker(\sigma_\pi) = \pi$), and

Then **SAT DET1**(γ, f) gives the cover $\Gamma = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5\}$ where

$$\begin{aligned}
\gamma_1 &= (\{\}, \{a^2b\}),\\
\gamma_2 &= (\{a^2b\}, \{c\}),\\
\gamma_3 &= (\{b, c\}, \{a^3\}),\\
\gamma_4 &= (\{a^2, c\}, \{5b\}), \text{and}\\
\gamma_5 &= (\{a^3, b, c\}, \{\}).
\end{aligned}$$

Note again that no condition is contradictory. Furthermore,

$$\begin{aligned}
\mathrm{HT}_{\gamma_1}(f) &= (a^2b)x^2y,\\
\mathrm{HT}_{\gamma_2}(f) &= cx^2,\\
\mathrm{HT}_{\gamma_3}(f) &= a^3y^2, \text{and}\\
\mathrm{HT}_{\gamma_4}(f) &= (5b)y.
\end{aligned}$$

All terms of f are colored *green* by γ_5.

Finally, we use **SAT DET1** to write the algorithm **SAT DET** in table 2.2 to generate a cover of a condition to determine the head terms of a finite set of polynomials $F = \{f_1, \ldots, f_n\} \subset S$. Patial correctness and termination of this algorithm are clear.

2.2 Algebraic Study of Specializations

In section 2.1, we defined the notion of a contradictory condition (see subsection 2.1.4). The prevailing idea was that we wanted to disallow having powers of products of polynomials in the red list of a condition γ in the ideal of the green list of γ. If γ is contradictory, then it is easy to see that $\Sigma_\gamma = \emptyset$. The aim of this section is to show, over algebraically closed fields, that by keeping our conditions in saturated form, we thereby rule out all possible cases where the set of specializations Σ_γ may become empty. That is to say, by always keeping our conditions

Example 2.1.3 In example 2.1.1, $\gamma = (\{uv^2 + 2v^2, u^4 - 2u^2 + 1\}, \{\})$, and

$$f = (-u^2 + v + 1)xy + 5y \in k[u, v][x, y].$$

Using lex order $x > y$, **SAT DET1**(γ, f), gives just $\Gamma = \{\gamma\}$, since the first term of f is *green* by γ (it is in the radical of $I_{\mathrm{gr}(\gamma)}$). In this case $\mathrm{HT}_\gamma(f) = 5y$.

Example 2.1.4 As written, the condition $\gamma = \Big(\{u^4 + 1\}, \{u^2 + \sqrt{2}u + 1\}\Big)$ of example 2.1.2 is not a valid input to **SAT DET1**. One easily sees, however, that

$$\langle u^4 + 1\rangle : (u^2 + \sqrt{2}u + 1)^\infty = \langle u^2 - \sqrt{2}u + 1\rangle.$$

The appropriate input condition then is $\gamma' = \Big(\{u^2 - \sqrt{2}u + 1\}, \{u^2 + \sqrt{2}u + 1\}\Big)$. So, with $f = (u^2 - \sqrt{2}u + 1)x^5 + 3xy$, the output cover from **SAT DET1**(γ', f) is then simply $\Gamma = \{\gamma'\}$. We see that the head term of f with respect to γ' is then $3xy$.

Example 2.1.5 Compare the previous example to this one. Let $\gamma = (\{\}, \{\})$, and let $g = (u^4 + 1)x^5 + (u^2 - \sqrt{2}u + 1)x^3 + (u^2 + \sqrt{2}u + 1) \in k[u][x]$. Then **SAT DET1**$(\gamma, g)$ yields $\Gamma = \{\gamma_1, \gamma_2, \gamma_3\}$, where

$$\begin{aligned}
\gamma_1 &= (\{\}, \{u^4 + 1\}) \\
\gamma_2 &= \Big(\{u^2 - \sqrt{2}u + 1\}, \{u^2 + \sqrt{2}u + 1\}\Big) \\
\gamma_3 &= \Big(\{u^2 + \sqrt{2}u + 1\}, \{u^2 - \sqrt{2}u + 1\}\Big).
\end{aligned}$$

Note that the case $\delta = (g, r) = \Big(\{u^2 + \sqrt{2}u + 1, u^2 - \sqrt{2}u + 1\}, \{\}\Big)$ never occurs. If it did, then then reduced Groebner Basis of I_g would be $\{1\}$. Hence, $\mathbf{V}(I_g)$ would be empty. There are no common roots of the two polynomials in g.

Example 2.1.6 Let $\gamma = (\{\}, \{\})$, and

$$f = (a^2b)x^2y + cx^2 + a^3y^2 + (5b)y \in k[a, b, c][x, y].$$

Therefore, in either case, the algorithm just returns the condition $\delta = (sg, r')$, where $sg = I_g : (\text{coef1}(g))^\infty$ and $r' = \text{rd}(\gamma) \cup \{\text{coef1}(g)\}$, and stops.

We now show that this $\delta = (sg, r')$ is a valid output. First note the following five facts.

- The condition δ determines f.
- Since $I_g \subset I_{sg} = I_g : \text{coef1}(g)^\infty$ and $r' \supset r$, δ is a successor to γ.
- By our implementation, sg is a reduced Groebner Basis for I_{sg}. Making use of proposition 2.1.1, we have

$$\begin{aligned} I_{sg} : \text{coef1}(g)^\infty : r_1^\infty : \ldots : r_t^\infty = & \\ & ((I_g : \text{coef1}(g)^\infty) : \text{coef1}(g)^\infty) : r_1^\infty : \ldots : r_t^\infty \\ = \quad & (I_g : \text{coef1}(g)^\infty) : r_1^\infty : \ldots : r_t^\infty \\ = \quad & (I_g : r_1^\infty : \ldots : r_t^\infty) : \text{coef1}(g)^\infty \\ = \quad & I_g : \text{coef1}(g)^\infty \\ = \quad & I_{sg}. \end{aligned}$$

- I_{sg} is a proper ideal since coef1(g) is not in $\sqrt{I_g}$.
- δ is non-contradictory since

  (i) no $r_i \in \text{rd}(\gamma)$ nor coef1(g) are in $\sqrt{I_{sg}}$ by proposition 2.1.1, and
  (ii) I_{sg} would be improper if property (ii) of definition 2.1.4 were true.

Therefore, δ is a valid output, and it is in saturated form. Lastly, if $1 \notin I_{g'}$, the routine calls itself with inputs $\delta = (g', \text{rd}(\gamma))$ and $g - \text{term1}(g)$. By construction, $I_{g'}$ is proper and pre-saturated by the redlist of δ. Termination of the algorithm is clear. **End**

We now present some examples of the algorithm.

The output from the algorithm is a cover Γ of γ consisting solely of non-contradictory successor conditions of γ, each in saturated form, that determines f.

Analysis of SAT DET1: Upon entering the algorithm, we first set $g = f$. If $g = 0$, we are done, and the output cover is simply $\Gamma = \{\gamma\}$. As noted, γ determines f (indeed $0 \in \sqrt{I_g}$) and is non-contradictory by our input assumptions. If $g \neq 0$, then starting from the first (greatest) term of g, we sequentially discard terms $a \cdot t$ of g for which $1 \in I_g : a^\infty$, i.e. for which $a \in \sqrt{I_g}$ and are thus *green*, until the first (greatest) term of g is *nongreen* or g becomes zero.

If $g = 0$ here, we are done. The routine returns $\Gamma = \{\gamma\}$. We are also done if $\mathrm{col}^1_\gamma(\mathrm{coef1}(g)) = red$. For then, $\mathrm{HT}_\gamma(f) = \mathrm{coef1}(g) \cdot \mathrm{monom1}(g)$. If neither of these are true then the first nongreen term has $\mathrm{coef1}(g)$ *white*. In the **DET1** algorithm of chapter one, we would now branch γ into two distinct successor conditions by pushing $\mathrm{coef1}(g)$ into first the red list r of γ (thereby making it the head term of f) and then into the green list of γ (thereby continuing the search for the head term of f among the following terms).

In this new algorithm, we first compute

$$g' = \langle g_1, \ldots, g_s, \mathrm{coef1}(g) \rangle : r_1^\infty : \ldots : r_t^\infty,$$

$r_i \in \mathrm{rd}(\gamma)$, and then test if $1 \in I_{g'}$. Note: the notation "g' = an ideal" in the above is taken to mean that g' is a Groebner basis of the ideal. If $1 \in I_{g'}$ and on input $\mathrm{rd}(\gamma) = \emptyset$, then the reduced Groebner Basis of $I_{g'}$ will be $\{1\}$. In this case, regardless if k is algebraically closed, $\mathbf{V}(I_{g'}) = \mathbf{V}(g') = \emptyset$. If $1 \in I_{g'}$ and $\mathrm{rd}(\gamma) \neq \emptyset$, then there exist integers $m_i > 0$ for which the product $\prod_{i=1}^t (r_i)^{m_i} \in I_{g'}$. Thus, if we formed the condition $\delta = (g', r)$, it would be either

(a) not useful; in the sense that $\mathbf{V}(g') = \emptyset$, in which case the set of specializations $\Sigma_\delta = \emptyset$, or

(b) contradictory; in which case Σ_δ is again empty.

Table 2.1, Algorithm **SAT DET1**

Input: Condition γ in saturated form, and a polynomial $f \in P$
Output: Cover Γ of γ consisting solely of non-contradictory, successors δ to γ, in saturated form, that determines f

$g := f$
IF $g = 0$ **THEN** Return($\Gamma := \{\gamma\}$)
WHILE $g \neq 0$ **and** $1 \in sg := I_g : (\mathrm{coef1}(g))^\infty$ **DO**
    $g := g - \mathrm{term1}(g)$
IF $g = 0$ **or** $\mathrm{col}^0_\gamma(\mathrm{coef1}(g)) = red$ **THEN**
    $\Gamma := \{\gamma\}$
ELSE
    $g' := \langle g_1, \ldots, g_s, \mathrm{coef1}(g)\rangle : r_1^\infty : \ldots : r_t^\infty$
    IF $1 \in I_{g'}$ **THEN**
        $\Gamma := \{(sg, \mathrm{rd}(\gamma) \cup \{\mathrm{coef1}(g)\})\}$
    ELSE
        $\Gamma := \{(sg, \mathrm{rd}(\gamma) \cup \{\mathrm{coef1}(g)\})\} \cup$
            SAT DET1$((g', \mathrm{rd}(\gamma)), g - \mathrm{term1}(g))$
Return(Γ)

This command returns a reduced (hence also minimal) Groebner Basis for the intersection $\tilde{I} \cap k[u_1, \ldots, u_m]$ (see the next section for a further discussion of this).

Motivated by our examples 2.1.1 and 2.1.2, we make the following definition.

Definition 2.1.7 *A condition* $\gamma = (g, r) = (\{g_1, \ldots, g_s\}, \{r_1, \ldots, r_t\})$ *is called* **contradictory** *if one (or both) of the following is true:*

(i) *there exists some* $r_i \in r$ *such that* $r_i \in \sqrt{I_g}$ *or,*
(ii) *there exist a nonempty subset* $\{r_{i_1}, \ldots, r_{i_l}\} \subseteq r$ *and positive integers* $m_{i_1}, \ldots, m_{i_l}$ *for which* $\prod_{k=i_1}^{i_l} (r_k)^{m_k} \in I_g$.

It is clear that if γ is contradictory, then Σ_γ must be empty.

Definition 2.1.8 *A condition* $\gamma = (g, r) = (\{g_1, \ldots, g_s\}, \{r_1, \ldots, r_t\})$ *is in* **saturated form** *if*

(i) g *is a minimal Groebner Basis for* I_g, *and*
(ii) $1 \notin I_g$ (*so* I_g *is a proper ideal*), *and*
(iii) $I_g : r_1^\infty : \ldots : r_t^\infty = I_g$.

We next give our algorithm **SAT DET1** in table 2.1 below. As in section 1.2, given any polynomial $f = \sum a_i \cdot t_i \in S$, let $\text{term1}(f) = a \cdot t$ denote the first (greatest) term in the summation with respect to the chosen monomial ordering on the main variables. So again we have $\text{coef1}(f) = a$, and $\text{monom1}(f) = t$.

The input to this algorithm consists of a polynomial $f \in P$ and a condition γ in saturated form.

Remark 2 From proposition 2.1.3 and corrollary 2.1.1, it is clear that if γ is in saturated form, then γ is not contradictory!

In other words, if $I : r_1^\infty : \ldots : r_t^\infty = I$, then no polynomial of G contains *any* powers of the irreducible factors of the r_i. We will use both of these results in the next section.

2.1.4 The Saturated Determine Algorithm

In this section we now formulate working criteria to implement our new coloring definition col_γ^1 of subsection 2.1.2. For a given condition

$$\gamma = (g, r) = (\{g_1, \ldots, g_s\}, \{r_1, \ldots, r_t\}),$$

let $I_g = \langle g_1, \ldots, g_s \rangle \subset P$. Observe that for any $a \in P$

$$\begin{aligned} \mathrm{col}_\gamma^1(a) = green &\leftrightarrow a \in \sqrt{I_g} \\ &\leftrightarrow 1 \in I_g : a^\infty \\ &\leftrightarrow 1 \in \langle g_1, \ldots, g_s, 1 - ya \rangle \cap k[u_1, \ldots, u_m], \end{aligned}$$

and

$$\begin{aligned} \mathrm{col}_\gamma^1(a) = red(\text{by (iv)}) &\leftrightarrow a \Big| \left(\prod_{i=1}^{t} (r_i)^{m_i} \right) \text{for some } m_i > 0 \\ &\leftrightarrow 1 \in \langle a \rangle : r_1^\infty : \ldots : r_t^\infty \\ &\leftrightarrow 1 \in \langle a, 1 - y_1 r_1, \ldots, 1 - y_t r_t \rangle \cap k[u_1, \ldots, u_m]. \end{aligned}$$

In our MACSYMA implementation, we made use of its command ID_CONTRACT to compute Groebner bases for the intersection of ideals of the form

$$\tilde{I} = \langle f_1, \ldots, f_m, 1 - y_1 g_1, \ldots, 1 - y_n g_n \rangle \subset k[u_1, \ldots, u_m, y_1 \ldots, y_n],$$

where $f_i, g_j \in k[u_1, \ldots, u_m]$, with the subring $k[u_1, \ldots, u_m]$ of

$$k[u_1, \ldots, u_m, y_1, \ldots, y_n].$$

$g_1 = h_1 f^m$ for some $h_1 \in P$. Since $h_1 f^m = g_1 \in I = I : f^\infty$, we have by definition that $h_1 \in I$. Hence,

$$\mathrm{HM}(h_1) \in \langle \mathrm{HM}(I) \rangle = \langle \mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_s) \rangle.$$

Thus, $\mathrm{HM}(h_1)$ is divisible by some $\mathrm{HM}(g_i)$, and we may write

$$\mathrm{HM}(h_1) = x^\gamma \cdot \mathrm{HM}(g_i).$$

Now,

$$\mathrm{HM}(g_1) = \mathrm{HM}(h_1 f^m) = \mathrm{HM}(h_1)\mathrm{HM}(f^m) = x^\gamma \mathrm{HM}(f^m)\mathrm{HM}(g_i).$$

If $i = 1$ in this equation, we have the contradiction that $\mathrm{HM}(f^m)$ divides 1 (f is nonconstant). If $i \neq 1$, we contradict that G is a minimal Groebner Basis of I. This proves part (i).

If $f \in \sqrt{I}$ then there exists an $n > 0$ for which $f^n \in I$. This implies for any polynomial $h \in P$, that $hf^n \in I$. So $P \subset I : f^\infty = I$ which contradicts that I is proper. This proves part (ii) and ends the proof.

In other words, if $I : f^\infty = I$, then no polynomial of G contains *any* powers of the irreducible factors of f. The following corrollary is proved similarly.

Corollary 2.1.1 *Let $I = \langle g_1, \ldots, g_s \rangle \subset P$ be a proper, nontrivial ideal, where $G = \{g_1, \ldots, g_s\}$ is a minimal Groebner Basis of I. Let $r_1, \ldots, r_t \in P - I$ be nonconstant polynomials. If $I : r_1^\infty : \ldots : r_t^\infty = I$, then*

(i) *for all $g_i \in G$, g_i is not divisible by any power product $\prod_{i=1}^t (r_i)^{m_i}$, $m_i > 0$, and*
(ii) *$r_i \notin \sqrt{I}$, and*
(iii) *for any subset $\{r_{i_1}, \ldots, r_{i_l}\} \subset \{r_1, \ldots, r_t\}$ and any positive integers $m_{i_1}, \ldots, m_{i_l}$, $\prod_{k=i_1}^{i_l} (r_k)^{m_k} \notin I$.*

We also have $1 - y_j r_j \in \tilde{I}$ for all j. Hence, we may write

$$f = \left(\prod_{j=1}^{t} (y_j r_j)^{m_j} \right) f - \left(1 - \prod_{j=1}^{t} (y_j r_j)^{m_j} \right) f.$$

It remains to show that $\left(1 - \prod_{j=1}^{t} (y_j r_j)^{m_j}\right) \in \tilde{I}$. By some factoring,

$$\begin{aligned} 1 - \prod_{j=1}^{t} (y_j r_j)^{m_j} &= (1 - (y_1 r_1)^{m_1}) + (y_1 r_1)^{m_1} \left[1 - \prod_{j=2}^{t} (y_j r_j)^{m_j} \right] \\ &= h_1 (1 - y_1 r_1) \\ &+ (y_1 r_1)^{m_1} \left[(1 - (y_2 r_2)^{m_2}) + (y_2 r_2)^{m_2} \left[1 - \prod_{j=3}^{t} (y_j r_j)^{m_j} \right] \right] \\ &= \sum_{j=1}^{t} h_j \left(\prod_{i=1}^{j-1} (y_i r_i)^{m_i} \right) (1 - y_j r_j) \in \tilde{I}, \end{aligned}$$

where $h_j = \sum_{k=1}^{m_j - 1} (y_j r_j)^k \in k[y_1, \ldots, y_r, u_1, \ldots, u_m]$. We tacitly assume that

$$\prod_{i=1}^{0} (y_i r_i)^{m_i} = 1.$$

Therefore, $f \in \tilde{I} \cap k[u_1, \ldots, u_m]$. This ends this nice proof.

Note by this proof that we have $1 \in I : r_1^{\infty} : \ldots : r_t^{\infty}$ if and only if there exist integers $m_1, \ldots, m_t > 0$ such that the product $\prod_{k=1}^{t} (r_i)^{m_i} \in I$.

Proposition 2.1.3 *Let $I = \langle g_1, \ldots, g_s \rangle \subset P$ be a proper, nontrivial ideal, where $G = \{g_1, \ldots, g_s\}$ is a minimal Groebner Basis of I. Let $f \in P - I$ be a nonconstant polynomial. If $I : f^{\infty} = I$, then*

(i) *for all $g_i \in G$, g_i is not divisible by any power f^m, $m > 0$, and*
(ii) $f \notin \sqrt{I}$.

Proof: Part (i): Suppose the contrary, and let $g_1 \in G$ (relabeling the elements of G as necessary) be such that there exists an $m > 0$ for which f^m divides g_1. Then

Proposition 2.1.2 *Let $I = \langle g_1, \ldots, g_s \rangle$ be an ideal in $k[u_1, \ldots, u_m]$, and $r_1, \ldots, r_t$ be a polynomials in $k[u_1, \ldots, u_m]$. Form the ideal*

$$\tilde{I} = \langle g_1, \ldots, g_s, 1 - y_1 r_1, \ldots, 1 - y_r r_t \rangle$$

in $k[y_1, \ldots, y_t, u_1, \ldots, u_m]$. Then

$$I : r_1^\infty : \ldots : r_t^\infty = \tilde{I} \cap k[u_1, \ldots, u_m].$$

Proof. The proof is a generalization of the proof for the Radical Membership test. First, let $f \in \tilde{I} \cap k[u_1, \ldots, u_m] \subset \tilde{I} \cap k[y_1, \ldots, y_t, u_1, \ldots, u_m]$. Then f may be written

$$f = \sum_{i=1}^{s} a_i(y_1, \ldots, y_t, u_1, \ldots, u_m) g_i + \sum_{j=1}^{t} b_j(y_1, \ldots, y_t, u_1, \ldots, u_m)(1 - y_j r_j)$$

where $a_i, b_j \in k[y_1, \ldots, y_t, u_1, \ldots, u_m]$. Setting $y_i = 1/r_i$ for each $j = 1, \ldots, t$ gives

$$f = \sum_{i=1}^{s} a_i(1/r_i, \ldots, 1/r_t, u_1, \ldots, u_m) g_i. \tag{2.1}$$

For each $j = 1, \ldots, t$, choose an integer $m_j > 0$ such that

$$((r_j)^{m_j})\, a_i(1/r_i, \ldots, 1/r_t, u_1, \ldots, u_m) \in k[u_1, \ldots, u_m]$$

for every $i = 1, \ldots, s$. Then we may clear all denominators of all rational functions a_i on the right hand side of equation 2.1 to get

$$\left(\prod_{j=1}^{t} (r_j)^{m_j} \right) f = \sum_{i=1}^{s} A_i g_i \in I$$

for some polynomials $A_j \in k[u_1, \ldots, u_m]$. Therefore, $f \in I : r_1^\infty : \ldots : r_t^\infty$.

For the reverse inclusion, let $f \in I : r_1^\infty : \ldots : r_t^\infty$. By definition there exist positive integers $m_1, \ldots, m_t$ such that $\left(\prod_{j=1}^{t} (r_j)^{m_j} \right) f \in I$. Since $I \subset \tilde{I}$ and $\tilde{I}$ is an ideal, we have

$$\left(\prod_{j=1}^{t} (y_j r_j)^{m_j} \right) f = \left(\prod_{j=1}^{t} (y_j)^{m_j} \right) \left(\prod_{j=1}^{t} (r_j)^{m_j} \right) f \in \tilde{I}.$$

Definition 2.1.6 *Let $I \subset k[u_1, \ldots, u_m]$ be an ideal, and fix $f \in k[u_1, \ldots, u_m]$. Then the* **saturation of I with respect to f** *is the set*

$$I : f^\infty = \{g \in k[u_1, \ldots, u_m] \mid gf^m \in I \text{ for some } m > 0\}.$$

One shows that $I : f^\infty$ is an ideal containing I. Further, for any $r_1, r_2 \in P$ and an ideal I, we have $(I : r_1^\infty) : r_2^\infty = (I : r_2^\infty) : r_1^\infty$. Thus, for a given ideal I and a list of polynomials $r_1, \ldots, r_t \in P$, it makes sense to define the ideal

$$I : r_1^\infty : \ldots : r_t^\infty = \left\{ g \in P \;\middle|\; g\left(\prod_{i=1}^{t}(r_i)^{m_i}\right) \in I \text{ for some } m_1, \ldots, m_t > 0 \right\}.$$

We will refer to this ideal as I **saturated** with the list $r_1, \ldots, r_t$. Note that for any nonzero f, $\langle 0\rangle : f^\infty = \langle 0\rangle$, and I saturated with an empty list (no polynomials r_i) is just I. We next prove a set of relevant facts for computing with saturations of ideals. We will use these results in the algorithm **SAT DET1** in table 2.1 below.

Proposition 2.1.1 *Let I be an ideal, $r_1, \ldots, r_t \in P$. If J is the ideal*

$$J = I : r_1^\infty : \ldots : r_t^\infty,$$

then

$$J : r_1^\infty : \ldots : r_t^\infty = J.$$

Proof: Let $h \in J : r_1^\infty \ldots r_t^\infty$. Then there exist $m_i > 0$ such that

$$h(\prod_{i=1}^{t}(r_i)^{m_i}) \in J.$$

Again, there exist $n_i > 0$ such that

$$h\left(\prod_{i=1}^{t}(r_i)^{m_i n_i}\right) = h\left(\prod_{i=1}^{t}(r_i)^{m_i}\right)\left(\prod_{i=1}^{t}(r_i)^{n_i}\right) \in I.$$

Therefore, $h \in J$. The opposite inclusion is clear. This ends the proof.

In words, once an ideal I is fully saturated with a list of polynomials, it does not change if saturated again by this same list. In particular, $(I : f^\infty) : f^\infty = I : f^\infty$.

Definition 2.1.4 *Let f be a polynomial in S, and let γ be a condition. Then we say*

> (i) *a term $a \cdot t \in T(f)$ is the* **conditional head term of f relative to γ**, *denoted* $\mathrm{HT}_\gamma(f)$, *if* $\mathrm{col}^1_\gamma(a) =$ *red and all greater terms $b \cdot t' \in T(f)$, where $t' \geq t$, have* $\mathrm{col}^1_\gamma(b) =$ *green, and*
> (ii) *if* $\mathrm{HT}_\gamma(f) = a \cdot t$, *then a is the* **conditional head coefficient of f relative to γ**, *denoted* $\mathrm{HC}_\gamma(f)$, *and t is the* **conditional head monomial of f relative to γ**.

Thus the conditional head term of f is simply the first *red*, i.e. "nonzero" term one comes to in scanning the terms of f past the *green*, i.e. "zero" terms of f. Note that $\mathrm{HT}_\gamma(f)$ is again undefined for a polynomial with a *white* term before its first *red*, or if all its terms are colored *green*. We next update the definition of "successor" to a condition.

Definition 2.1.5 *A* **successor to a condition** $\gamma = (g, r)$, *is another condition, $\delta = (g', r')$, such that one (or both) of the following is true:*

> *(i) the ideal I_g is contained in the ideal $I_{g'}$,*
> *(ii) the set r is a subset of the set r'*

Notation: $\delta \supseteq \gamma$.

With this definition, we may now carry over intact the definitions of determine and cover from section 1.2.

2.1.3 Computations with Saturated Ideals

To implement the new definitions in the previous section, we found it helpful to make use of the notion of the *saturation* of an ideal with respect to a given polynomial.

$\mathrm{col}^1_\gamma(a) = \textit{green, if } a \in \sqrt{I_g}$,

$\mathrm{col}^1_\gamma(a) = \textit{red, if either}$

(i) a *is invertible in* k, *or if*

(ii) $a \in \mathrm{rd}(\gamma)$, *or if*

(iii) $a = ca'$ *for some nonzero* $c \in k$

and some $a' \in \mathrm{rd}(\gamma)$, *or if*

(iv) a *divides a product of the form:* $\prod(r_i)^{m_i}$, *where* $r_i \in r$

and m_i *are nonnegative integers.*

In all other cases, $\mathrm{col}^1_\gamma(a) = \textit{white}$.

The "or" in the choice of declaring a polynomial *red* is the nonexclusive "or." By defining a polynomial to be *green* if it is in the radical of the ideal generated by the green list of γ, we thus ensure that it is in $\mathbf{I}(\mathbf{V}(I_g))$. Hence, it will be specialized to zero by any $\sigma \in \Sigma_\gamma$. Statements (i-iii) above are precisely those from the previous definition of $\mathrm{col}^0_\gamma(a) = \textit{red}$ in section 1.1. The motivation behind statement (iv) is that we want to declare a polynomial $a \in P$ to be *red* if it's irreducible factors are powers of some collection of the irreducible factors of the $r_i \in \mathrm{rd}(\gamma)$. Thus, any $\sigma \in \Sigma_\gamma$ that makes all the r_i nonzero (and so must also make all their irreducible factors nonzero) will also make a nonzero. The coloring decsions are thus no longer based solely on memebership (up to a constant nonzero scaler multiple) in the green and red lists of γ. Rather, the purpose is to reduce the number of *white* cases. That is, with this new methodology, more decisions for declaring polynomials in P as *green* or *red* can be made. Essentially then, by not putting such a strict membership interpretation upon color assignments, we allow any given condition to "carry" more color information in its finite green and red lists than its individual members may show.

With this new coloring scheme we next redefine the conditional head term of a polynomial.

Assuming lex order with $x > y$, **DET1**(γ, f) gives the cover $\Gamma = \{\gamma_1, \gamma_2\}$ where

$$\begin{aligned} \gamma_1 &= (\{uv^2 + 2v^2, u^4 - 2u^2 + 1\}, \{-u^2 + v + 1\}) \\ \gamma_2 &= (\{uv^2 + 2v^2, u^4 - 2u^2 + 1, -u^2 + v + 1\}, \{\}). \end{aligned}$$

The trouble here is with condition γ_1. For, if $\sigma \in \Sigma_{\gamma_1}$, then this σ is supposed to make every polynomial in $\mathrm{gr}(\gamma_1)$ zero and those in $\mathrm{rd}(\gamma_1)$ nonzero. But it can be shown that $(-u^2 + v + 1) \in \sqrt{I_g}$ by the radical membership test (in fact, $(-u^2+v+1)^3 \in I_g$ [but no lower power]). Therefore, when σ makes all polynomials in I_g zero, it must also make $-u^2 + v + 1$ zero. Thus we have a contradiction.

Example 2.1.2 Let $\gamma = \Big(\{u^4 + 1\}, \{u^2 + \sqrt{2}u + 1\}\Big)$, and

$$f = (u^2 - \sqrt{2}u + 1)x^5 + 3xy \in k[u][x, y].$$

Again using lex order $x > y$, the output from **DET1**(γ, f) will be $\Gamma = \{\gamma_1, \gamma_2\}$ with

$$\begin{aligned} \gamma_1 &= \Big(\{u^4 + 1\}, \{u^2 + \sqrt{2}u + 1, u^2 - \sqrt{2}u + 1\}\Big) \\ \gamma_2 &= \Big(\{u^4 + 1, u^2 - \sqrt{2}u + 1\}, \{u^2 + \sqrt{2}u + 1\}\Big). \end{aligned}$$

The trouble here is that the product of the two polynomials in $\mathrm{rd}(\gamma_1)$ is $u^4+1 \in I_g$. Thus, it is again impossible for a specialization $\sigma \in \Sigma_{\gamma_1}$ to make all polynomials in $\mathrm{rd}(\gamma_1)$ nonzero and make all those in $\mathrm{gr}(\gamma_1)$ nonzero.

In light of these examples, we now refine the notion of coloring P with respect to a given condition γ. We will denote this new coloring scheme by col^1_γ to distinguish it from col^0_γ of chapter one.

Definition 2.1.3 *Let $\gamma = (g, r) = (\{g_1, \ldots, g_s\}, \{r_1, \ldots, r_t\})$ be a given condition. Then a* **coloring of P with respect to γ** *is a mapping,*

$$\mathrm{col}^1_\gamma : P \to \{green, red, white\},$$

defined as follows:

Lemma 2.1.1 *For any monomial ordering, the only reduced Groebner Basis of the ideal* $I = \langle 1 \rangle$ *is* $G = \{1\}$.

Proof: Let $G = \{g_1, \ldots, g_s\}$ be a Groebner Basis of I. Then, since

$$1 \in \langle \mathrm{HM}(I) \rangle = \langle \mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_s) \rangle$$

there exists an $1 \leq i_0 \leq s$ such that $\mathrm{HM}(g_{i_0})$ divides 1. Thus, this g_{i_0} must be a nonzero constant. Since all other $\mathrm{HM}(g_j)$ for $g_j \in G$ are divisible by 1, they may all be removed from G and the resulting set $\tilde{G} = \{1\}$ is still a Groebner Basis for I (see section 1.5). This ends the lemma.

Thus we see that if $I = \langle f_1, \ldots, f_n \rangle$ has a reduced Groebner Basis $G = \{1\}$ then $V = \mathbf{V}(f_1, \ldots, f_n) = \mathbf{V}(I) = \mathbf{V}(1) = \emptyset$. The converse is not true if k is not algebraically closed. If k is algebraically closed then $V = \mathbf{V}(I) = \emptyset$ implies $I = \langle 1 \rangle = P$. This result is the **Weak Nullstellensatz**. Therefore, over an algebraically closed field, any given system of polynomial equations $f_1 = 0, \ldots, f_n = 0$ has a solution if and only if the reduced Groebner Basis of $I = \langle f_1, \ldots, f_n \rangle$ is not $G = \{1\}$.

2.1.2 Refined Definitions of Colorings

Now, the **DET1** and **DET** algorithms of section 1.2 will indeed generate a large enough cover of the given initial conditions to determine sets of polynomials. However, since these algorithms merely push coefficients of polynomials onto the green and red lists of a condition when necessary, it can happen that the output cover will contain conditions γ for which the set Σ_γ is empty. To make the idea clear, we present two typical examples of this phenomenon.

Example 2.1.1 Let $\gamma = (\{uv^2 + 2v^2, u^4 - 2u^2 + 1\}, \{\})$, and

$$f = (-u^2 + v + 1)xy + 5y \in k[u, v][x, y].$$

Theorem 2.1.1 (Radical Membership) *Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal in $k[x_1, \ldots, x_n]$, and f be a polynomial. Form the ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle$ in $k[x_1, \ldots, x_n, y]$. Then $f \in \sqrt{I}$ if and only if $1 \in \tilde{I}$.*

Proof: Let $f \in \sqrt{I}$. Then there exists an integer $m \geq 1$ such that $f^m \in I \subset \tilde{I}$. Since now both $1 - yf$ and f^m are in $\tilde{I}$ we have $1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1-yf)(\sum_{i=0}^{m-1} (yf)^i) \in \tilde{I}$. The other direction is proved by the Rabinowitsch trick [1]. Write $1 \in \tilde{I}$ as

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n)(1 - yf).$$

Then setting $y = 1/f$ in the above gives

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i.$$

This is a rational function, so choose a positive integer m big enough to clear the denominators by multiplying both sides by f^m. We get

$$f^m = \sum h_i f_i$$

with $h_i \in k[x_1, \ldots, x_n]$. This shows $f \in \sqrt{I}$ and ends the nice proof.

For any ideal I, it is not hard to see that we always have the inclusion $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$. The reverse inclusion is not true in general if the field k is not algebraically closed. For a counterexample, take k to be the reals, and take $I = \langle u^2 + 1 \rangle \subset k[u]$. Then $\mathbf{V}(I) = \emptyset$, and (vacuously) $\mathbf{I}(\mathbf{V}(I)) = k[u]$, but $1 \notin \sqrt{I}$).

Theorem 2.1.2 (Hilbert Nullstellensatz) *Let k be algebraically closed, $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, and $I = \langle f_1, \ldots, f_s \rangle$. Then $f \in \mathbf{I}(\mathbf{V}(I))$ implies $f \in \sqrt{I}$.*

In words, if a polynomial f vanishes on the variety determined by a finite set of polynomials, then f is in the radical of the ideal generated by this set.

Let $f_1, \ldots, f_s \in P$. A common problem is to decide if $V = \mathbf{V}(f_1, \ldots, f_s) \subset k^n$ is nonempty (see section 4.1 of [2].

powers of polynomials in the red list, i.e. expressions of the form: $f = \prod(r_i)^{m_i}$, where $r_i \in r$ and m_i are nonnegative integers.

Definition 2.1.1 *Let k be a field. We will make use of the following notions from algebraic geometry.*

(i) *Let $f_1, \ldots, f_k \in P$. The* **affine variety** *defined by $f_1, \ldots, f_k$ is the set*

$$\begin{aligned} V &= \mathbf{V}(f_1, \ldots, f_k) \\ &= \{(a_1, \ldots, a_m) \in k^m \mid f_i(a_1, \ldots, a_m) = 0, 1 \leq i \leq s\}. \end{aligned}$$

(ii) *For I an ideal of P, the* **variety of the ideal** *is*

$$V = \mathbf{V}(I) = \{(a_1, \ldots, a_m) \in k^m \mid f(a_1, \ldots, a_m) = 0, \forall f \in I\}.$$

(iii) *Let V be an affine variety. The* **ideal of the variety** *is*

$$I = \mathbf{I}(V) = \{f \in P \mid f(x) = 0, \forall x \in V\}.$$

(iv) *An ideal I is* **radical** *if $f^m \in I$ for any integer $m \geq 1$ implies that $f \in I$.*

Definition 2.1.2 *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The* **radical** *of I, written $\sqrt{I}$, is the set*

$$\sqrt{I} = \{f \mid f^m \in I \text{ for some integer } m \geq 1\}.$$

By the Hilbert Basis Theorem, $\mathbf{V}$(I) is indeed an affine variety since I has a finite basis. Other relevant facts are that $\sqrt{I}$ is a radical ideal that contains I (in general, the containment is proper) and that $\mathbf{I}(V)$ is a radical ideal. It is a nontrivial problem to compute bases for the radical of an ideal. Nonetheless, there is a nice algorithm ([2], [1]) to determine whether a polynomial f is in the radical of a given ideal I. Furthermore, this algorithm works over any field k.

in advance. In the third section of this chapter we show how to generalize these optimizations for constructions of Comprehensive Groebner Bases.

Finally, along the way we will amplify how the saturated form of a condition relates back to the spectrum S_γ of a condition described in Weispfenning's paper [7]. We conclude the chapter with further discussions of implementations and further simplification procedures that will prove useful for computations in this framework.

2.1 Eliminating Contradictory Cases by Ideal Saturation

In this section we make more specific our notion of the "saturated form" of a condition. We give two typical guide examples for this construction. Next, we show relevant computations with saturated ideals which form the theoretical underpinning of our new determine algorithm. Along the way we will make good use of elementary concepts in algebraic geometry.

2.1.1 Ideal of a Condition and some Algebraic Geometry

Let $\gamma = (g, r) = (\{g_1, \ldots, g_s\}, \{r_1, \ldots, r_t\})$ be a condition and denote by I_g the ideal in P generated by the polynomials in the green list of γ, $I_g = \langle g \rangle = \{\sum_{i=1}^{s} h_i g_i \,|\, h_i \in P\}$ (we assume that an empty green list corresponds to the ideal $\langle 0 \rangle = \{0\}$). By the arithmetic color rules from section 1.3, *green* + *green* is *green*, and any polynomial in parameters times a *green* is also *green*. Hence, we may view I_g as "closed" under the operation of adding and multiplying *green* colored polynomials. All elements of I_g are thus *green*. By definition, $\mathrm{gr}(\gamma) \subset P - k$, and hence, I_g will always be a *proper* ideal of P. Since *red* + *red* may or may not be *red*, but a *red* times a *red* is still *red*, we may view multiplications of *red* polynomials as "closed," but not addition of *red*'s. That is, we may think of the red list of a condition as a multiplicative set. All products of elements in r are thus *red*. For any $\sigma \in \Sigma_\gamma$, we have $\sigma(f) = 0$ for all $f \in I_g$, and $\sigma(f) \neq 0$ for any product of

Suppose $\gamma = (\{uw, vw\}, \{w\})$. Then Σ_γ will be

$$\Sigma_\gamma = \{\sigma : (u, v, w) \mapsto (a, b, c) \in k^3 \,|\, ac = bc = 0, c \neq 0\}.$$

Now observe that for the condition $\delta = (\{u, v\}, \{w\})$, we have $\Sigma_\gamma = \Sigma_\delta$. This observation can be related to the *quotient* (or *colon*) ideal [2], since

$$\begin{aligned} \langle uw, vw\rangle : \langle w\rangle &= \{f \in k[u, v, w] \,|\, w \cdot f \in \langle uw, vw\rangle\} \\ &= \{f \in k[u, v, w] \,|\, w \cdot f = Auw + Bvw\} \\ &= \{f \in k[u, v, w] \,|\, f = Au + Bv\} \\ &= \langle u, v\rangle. \end{aligned}$$

So in δ above, the green list of δ consists of generators for the quotient ideal $\langle uw, vw\rangle : \langle w\rangle$. Closely associated with the quotient is the *saturation* of an ideal. We will show in this chapter that by keeping the conditions γ in a certain "saturated form," we avoid contradictory conditions. We will also show that only way Σ_γ can become empty (over an algebraically closed field) is for the condition to be "contradictory." Therefore, Σ_γ will never be empty (over an algebraically closed field) when γ is in our saturated form. This will also allow us to never carry any "virtual" Buchberger algorithms as discussed in the appendix of Becker and Weispfenning [1].

This form for conditions allows for more refined coloring criteria beyond testing for set membership. We will describe these algorithms in detail. Following this, we will show our new determine algorithm **SAT DET** (see table 2.2), for obtaining saturated successors to determine head terms of polynomials.

In Cox, Little, O'Shea [2], there are described two further optimizations of the Buchberger algorithm that make use of the theory of bases of homogeneous syzygies for a given list of polynomials. Because the arithmetic steps to compute S-polynomials and Normal Forms are the most computationally intensive tasks, syzygy theory allows for systematic criteria to ignore certain S-polynomial pairs

2 IMPROVEMENTS TO THE CONSTRUCTION

In this chapter we give improvements that represent a new design philosophy over the entire scope of the algorithms. These have resulted in greater efficiency of the algorithms and the output.

In the previous chapter, coloring assignments were made solely on the basis of naive membership in either the red or green lists of a condition. Such procedures often lead to "contradictory conditions," that is, conditions γ for which (loosely speaking) the set of specializations Σ_γ are empty. By its own, this may seem a minor drawback, but considered over the course of the entire **GROEBNERSYSTEM** algorithm, we lose overall efficiency because it continue to form branches upon branches of successors that will be eventually useless as final output. We will detail our new methodology which will avoid such unnecessary branches.

To do this, we show in the first section that we may view the elements of the green list as an ideal. But, in order to do that, we have to restrict the scope of the discussion to polynomials whose coefficients are polynomials, and not rational functions. With this restriction we will also be barred from true division of coefficients in S-polynomial and Normal Form computations, i.e. we will be forced to use the pseudo-division in the arithmetic. Yet, the third section of this chapter, we will show improvements to the pseudo-division computations.

Viewing the green list of a condition as an ideal of polynomials in parameters has several advantages which we shall explore in detail. First, as an ideal, we may compute a regular Groebner Basis for it. So, as we compute Comprehensive Groebner Bases, our conditions will have usual Groebner Bases for the green lists of the conditions! Clearly, the set of specializations Σ_γ of a condition is unchanged if we replace $\mathrm{gr}(\gamma)$ by its Groebner Basis. But we are not done yet.

Thus p may be eliminated from the basis G. For this paper we define

Definition 1.5.7 *A Groebner Basis G of I is* **minimal** *if*

$\mathrm{HM(g)} \notin \langle \mathrm{HM}(G - \{g\}) \rangle$ *for all* $g \in G$.

This definition differs from that in [2] in that we do not also require $\mathrm{HC}(g) = 1$ for all $g \in G$. A minimal Groebner Basis is not unique (see pg. 90-91 of [2] for an example). We also make the following definition.

Definition 1.5.8 *A Groebner Basis G of I is* **reduced** *if*

(i) *G is minimal, and*
(ii) *for all $g \in G$, no monomial of g is in* $\langle \mathrm{HM}(G - \{g\}) \rangle$.

For any ideal $I \neq \{0\}$, a reduced Groebner Basis is unique [2]. It is possible to generate reduced Comprehensive Groebner Bases. The main idea is to continue to find successor conditions so that each element g in G, with a well-defined head term, has none of its monomial's normal forms *nongreen* upon reduction by the (defined) conditional head monomials in $\mathrm{HM}_\gamma(G - \{g\})$. We implemented this algorithm without substantial changes. It gives a Groebner system where each pair (γ, G) has G reduced up to a constant multiples of the head monomials of each generators (see appendix B).

Example 1.5.3 For the example 1.5.1, a reduced Groebner system is

$$GS = \{((\{\}, \{1-t\}), \{x, (1-t)y\}), ((\{1-t\}, \{\}), \{x+ty\})\}.$$

In MACSYMA, the built in Groebner algorithm will give $\{x, y\}$ as a reduced Groebner basis for the generating set $F = \{x + y, x + ty\}$ with $x > y$ unless the switch grobner_primitive is set to true. That is, MACSYMA will assume that the t is nonzero. So we see already that a Comprehensive Groebner Basis takes into account all cases of specializations of the parameters.

Definition 1.5.6 *A* **Comprehensive Groebner Basis** *of an ideal I of $S = k(u_1, \ldots, u_m)[x_1, \ldots, x_n]$, with respect to a given monomial order $\leq$,* **over a case distinction** *B, is a finite subset G of I such that $\sigma(G)$ is a Groebner Basis of $\sigma(I)$ in $k[x_1, \ldots, x_n]$ for all specializations $\sigma \in \bigcup_{\beta \in B} S_\beta$. Note that if $B = \emptyset$, then G is a Comprehensive Groebner Basis of I.*

Let I be an ideal of S and let $F = \{f_1, \ldots, f_n\}$ be some finite basis for I. Let $GS = \{(\gamma, G)\}$ be a Groebner System for F over a case distinction B. Then, we can construct a Comprehensive Groebner Basis for I over B by appending all sets G of the Groebner pairs in G.

Example 1.5.2 In the previous example, $G = \{x + y, x + ty, (1 - t)y\}$ is a Comprehensive Groebner Basis of $I = \langle x + y, x + ty \rangle$.

Thus we see how to construct Comprehensive Groebner Bases for ideals over given case distinctions by use of Groebner systems. That is, any Groebner system of an ideal (over a case distinction) determines a CGB (over the case distinction).

The converse is also true [7]. Let G be a CGB of I over a B. Then it may not be the case that B determines G. So set $\Gamma = \bigcup_{\beta \in B} \{\mathbf{DET}(\beta, G)\}$, and $GS = \{(\gamma, G) \,|\, \gamma \in \Gamma\}$. This GS is a Groebner system for I over B. Clearly parts (i) and (ii) of the Groebner pair definition hold for every (γ, G) in this GS. Further, if a normal form of an S-polynomial becomes zero upon specialization by $\sigma \in S_\beta$, where $\beta \in B$, then, since $\gamma \in \Gamma$ are successors to β, this normal form will still become zero upon specialization by $\sigma \in S_\gamma$. Thus (iii) of the Groebner pair definition holds also.

Groebner Bases constructed from the Buchberger algorithm may, in general, contain unnecessary generators. It is a fact that if $G = \{g_1, \ldots, g_n, p\}$ is a Groebner Basis for I and $p \in G$ has $\mathrm{HM}(p) \in \langle \mathrm{HM}(G - \{p\}) \rangle$, then the set $G - \{p\}$ is also a Groebner Basis for I. To see this just note that

$$\langle \mathrm{HM}(I) \rangle \subseteq \langle \mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_n), \mathrm{HM}(p) \rangle \subseteq \langle \mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_n) \rangle.$$

generality that $i_1 < \cdots < i_k$. Now take $j_0 > i_k$. Then the monomial t_{j_0} is in I and so must be divisible by some monomial $t_i = x^{\alpha_i}$, $i < j_0$. But this contradicts our assumptions on s. End of proof.

In implementing the **GROEBNERSYSTEM** algorithm, we found it convenient for internal memory space to just carry the subscript list of pairs to be checked rather than a four tuple of the form (γ, F, f, g) where γ determines the set F, and $f \neq g \in F$. There is also a typographical error on pg 13 of [7] in the algorithm. The last set in the union of P should be indexed over all conditions in Δ/Δ' and not just Δ.

Example 1.5.1 We review the example in the introduction of this chapter. Let $F = \{x + y, x + ty\} \subset k(t)[x, y]$ with $x > y$, and let $B = \{(\{\}, \{\})\}$ be the case distinction containing just the empty condition. A Groebner system for F over B is

$$GS = \{((\{\}, \{1 - t\}), \{x + y, x + ty, (1 - t)y\}), ((\{1 - t\}, \{\}), \{x + y, x + ty\})\}.$$

The reader may readily check that each pair in this simple, yet illustrative, example is a Groebner Pair. Note that the $1-t$ in the green list of the condition $(\{1 - t\}, \{\})$ is precisely what is needed for the S-polynomial of $x + y, x + ty$ to be "zero". So, each condition γ of a Groebner pair (γ, G) encodes information to determine head terms of polys in G *and* all auxillary information necessary so that normal forms of S-polynomials will be "zero." From Weispfenning's paper [7] we have the following definitions.

Definition 1.5.5 *A* **Comprehensive Groebner Basis** *(CGB) of an ideal I of $S = k(u_1, \ldots, u_m)[x_1, \ldots, x_n]$, with respect to a given monomial order $\leq$, is a finite subset G of I such that $\sigma(G)$ is a Groebner Basis of $\sigma(I)$ in $k[x_1, \ldots, x_n]$ for all specializations σ of parameters into values in k.*

also have

$$\sigma(\mathrm{Spoly}_\delta(g_i, g_j)) = \mathrm{Spoly}(\sigma(g_i), \sigma(g_j)) \stackrel{\sigma(G)}{\Longrightarrow} \sigma(k) = 0$$

for all $\sigma \in S_\delta$, by lemmas 1.3.1, and 1.4.2. When P becomes empty, all pairs of polynomials in G will satisfy the Buchberger criterion, and hence, the pair (δ, G) will satisfy part (iii) of the Groebner Pair definition. Therefore, all pairs in CLOSED are Groebner Pairs.

The algorithm terminates when OPEN is empty. A triple (γ, G, P) will get pushed out to CLOSED when its list P becomes empty. P increases only when $\Delta \neq \{\gamma\}$, so $\Delta' \neq \emptyset$. We can thus prove termination [7] as follows. Each replacement of triples may be thought of as adding on finitely many more branches to a tree. If all branches terminate, then so does the whole tree by Koing's Tree Lemma [1]. So suppose we have a branch of triples, $b = \{(\gamma_i, G_i, P_i)\}$, so that, (i) $\gamma_i \subseteq \gamma_{i+1}$, and (ii) $G_{i+1} = G_i \cup \{k_i\}$, where k_i is the normal form modulo G_i relative to γ_i of some S-poly pair of polynomials in G_i. It is critical to observe that, because γ_{i+1} is a successor to γ_i, the head monomial of k_i, $\mathrm{HM}_{\gamma_{i+1}}(k_i) = \mathrm{HM}_{\gamma_i}(k_i)$, is not divisible by any head monomial $\mathrm{HM}_{\gamma_i}(g) = \mathrm{HM}_{\gamma_{i+1}}(g)$ with $g \in G_i$. Let $t_i = \mathrm{HM}_{\gamma_i}(k_i)$. If the tree b were infinite, we could then find a sequence of monomials $\{t_i\}_{i=1}^{\infty}$ with the property that t_i does not divide t_j whenever $i < j$. But this is impossible by the next lemma. **End**

Lemma 1.5.1 *There are no infinite sequences $s = \{t_i = x^{\alpha_i}\}_{i=1}^{\infty}$ of monomials of M with the property that t_i does not divide t_j whenever $i < j$.*

Proof: Suppose there was such a sequence s. Note that for $i < j$, $t_i \neq t_j$ by definition of s. Let $A = \{\alpha_i \mid t_i = x^{\alpha_i} \text{ is an element of } s\}$, and form the monomial ideal $I = \langle x^{\alpha_i} \mid \alpha_i \in A \rangle$. Every monomial in the sequence s belongs to this ideal. By Dickson's lemma, I is finitely generated, so there exist multindicies $\alpha_{i_1} \ldots \alpha_{i_k} \in A$ such that $I = \langle t_{i_1} = x^{\alpha_{i_1}}, \ldots, t_{i_k} = x^{\alpha_{i_k}} \rangle$. We may assume without loss of

If successful, the flag "found" is set to true. Any triple (γ, G, P) where either P is empty, or for all pairs $\{i,j\} \in P$

$$\text{cond\_part}(\text{col}^0_\gamma(g_i)) = \text{cond\_part}(\text{col}^0_\gamma(g_j)) = 0,$$

will have the corresponding pair (γ, G) added to the CLOSED list. Any triple with this second property, trivially, has (γ, G) satisfying (iii) of the definition to be a Groebner Pair. It will be shown that all pairs in CLOSED are Groebner Pairs.

Suppose now that found=true for the triple (γ, G, P) with pair $= \{i,j\}$. We then compute the normal form, k, of this pair's S-polynomial, $\text{Spoly}_\gamma(g_i, g_j)$, modulo G relative to γ. Because of the colored arithmetic operations, it is not necessarily true that k will have a well-defined head term. Hence, the next step is to call **DET1** and generate a cover of sucessors, Δ, to the current condition γ that will determine k. At least one of these successors $\delta \in \Delta$ will make all terms of $\text{col}^0_\delta(k)$ zero. Indeed, if all terms of k are already assigned *green* from the normal form algorithm, then $\Delta = \{\gamma\}$. The set $\Delta' \subset \Delta$ consists of all conditions where k will have a well-defined, *red*, head term. Consequently, if $\beta \in \Delta'$, for any $\sigma \in S_\beta$, we will have $\sigma(k) \neq 0$. On the other hand $\sigma(k) = 0$ for all $\sigma \in S_\beta$ with $\beta \in \Delta/\Delta'$.

Therefore, the routine replaces the triple (γ, G, P), popped from OPEN, with a finite set of new triples, one for each new condition in Δ. Note that since Δ contains successors of γ, for any $\delta \in \Delta$, we have $\text{HT}_\delta(g) = \text{HT}_\gamma(g)$ for all $g \in G$. If $\delta \in \Delta'$, then we color k by this δ, add it to G, and update the list P of pairs to be checked with the new addition to G. If $\delta \in \Delta/\Delta'$, then k is "zero" by this condition. By the "pop" operation, the new triple (δ, G, P) has $P = P - \{\{i,j\}\}$. Thus, we see that all new triples (δ, G', P') replacing (γ, G, P) have the property that their pairs (δ, G) satisfy parts (i) and (ii) of the definition to be a Groebner Pair.

Furthermore, every triple (δ, G, P), with $\delta \in \Delta/\Delta'$, has the additional property that, since $\text{Spoly}_\delta(g_i, g_j) \overset{G}{\Longrightarrow} k[\delta]$, where $\{i,j\}$ is the pair popped from P, then we

Table 1.6, Algorithm **GROEBNERSYSTEM**

Input: Case Distinction B, list of distinct polynomials
$F = \{f_1, \ldots, f_n\}$, monomial order $\leq$
Output: A Groebner System $GS = \{(\gamma, G)\}$ for F over B

$\Gamma := \bigcup_{\beta \in B} \{\mathbf{DET}(\beta, F)\}$
$P := \{\{i, j\} \,|\, i, j \in \{1, \ldots, n\}, i < j\}$
OPEN:=$\{(\gamma, \mathrm{col}^0_\gamma(F), P) \,|\, \gamma \in \Gamma\}$
CLOSED:= $\emptyset$
WHILE OPEN $\neq \emptyset$ **DO**
  found:=false
  WHILE OPEN $\neq \emptyset$ **and** found = false**DO**
    (γ, G, P):= pop(OPEN)
    WHILE $P \neq \emptyset$ **and** found =false **DO**
      pair:= pop(P) (=$\{i_0, j_0\}$)
      $i := i_0, j := j_0$
      IF $\mathrm{HM}_\gamma(g_i)$ **and** $\mathrm{HM}_\gamma(g_j)$ are defined **THEN**
        found:= true
    IF found = false **THEN**
      CLOSED:=CLOSED $\cup\{(\gamma, G)\}$
  IF found = true **THEN**
    h:=**SPOLY**$_\gamma(g_i, g_j)$
    k:=**NORMALFORM**(γ, h, G)
    Δ:= **DET1**(γ, k)
    Δ':= $\{\delta \in \Delta \,|\, T_{red,\delta}(k) = \{a \cdot t \in T(k) \,|\, \mathrm{col}^0_\delta(a) = red\} \neq \emptyset\}$
    OPEN:= OPEN
      $\bigcup_{\delta \in \Delta'} \{(\delta, G \cup \{\mathrm{col}^0_\delta(k)\}, P \cup \{\{i, n+1\} \,|\, 1 \leq i \leq n\})\}$
      $\bigcup_{\delta \in \Delta / \Delta'} \{(\delta, G, P)\}$
Return(CLOSED)

---

specializations represented by these conditions. The algorithm computes normal forms of conditional S-polys on pairs of polynomials. It then examines these normal forms to see if they consist entirely of *green*, that is, "zero" terms. If they are not zero, the algorithm generates successors to the current condition to determine the normal form.

Analysis of GROEBNERSYSTEM: Initialization step: We first set Γ to be the union of all covers of conditions in the initial case distinction necessary to determine the input list F. So for any condition $\gamma \in \Gamma$, and any $f \in F$, we have either $\mathrm{HT}_\gamma(\mathrm{f})$ is defined or $T_{green,\gamma}(f) = T(f)$ (equivalently, $\mathrm{cond\_part}(\mathrm{col}^0_\gamma(\mathrm{f})) = 0$). We set P to the list of all distinct pairs $\{i, j\}$ (with $i < j$) of subscripts of polynomials in F. Each of these pairs corresponds to a pair of distinct polynomials in F. We then initialize the list OPEN to be all triples of the form $(\gamma, \mathrm{col}^0_\gamma(F), P)$, where γ determines F, $\gamma \in \Gamma$. In the course of the algorithm, given a triple (γ, G, P), it is a loop invariant that γ always determines G. The list P is to be thought of as the list of all pairs of distinct polynomials of G whose normal form of this pair's S-polynomial is yet to be examined. Lastly, we initialize the set CLOSED to be empty. The algorithm returns the desired Groebner System in this set CLOSED.

If A is a nonempty list, the operation, $a := \mathrm{pop}(A)$, means that a is set to the first element in the list A, and, simultaneously, A is reassigned as the difference $A - \{a\}$. After initialization, the routine searches the list OPEN for the first triple (γ, G, P) such that

(i) $P \neq \emptyset$, and

(ii) there exists a pair of subscripts $\{i, j\} \in P$ such that $\mathrm{HM}_\gamma(g_i)$ and $\mathrm{HM}_\gamma(g_j)$ are defined, $g_i, g_j \in G$.

head monomials takes place in the sum. It turns out that these cancellations may be accounted for by S-polynomials of pairs of polynomials of G. Since the normal forms of these S-polynomials are zero, each S-polynomial may be written as a linear combination of the generators in G where the leading terms do not all cancel. Hence, it is possible to write an expression for f so that the multidegree inequality is again an equality.

We start our construction of Comprehensive Groebner Bases from the construction of a Groebner system for an ideal with respect to an initially set case distinction [7].

Definition 1.5.4 *Let B be a given case distinction, and $I \subset S$ be an ideal. Then a* **Groebner System**, *GS, for I over B is a finite set of ordered pairs of the form (γ, G), called* **Groebner Pairs**, *such that*

(i) *G is a finite subset of I determined by the condition γ,*
(ii) *The set $\Gamma = \{\gamma \mid (\gamma, G) \in GS\}$ is a cover of* each *$\delta \in B$, and*
(iii) *For every specialization $\sigma \in S_\gamma$, $\sigma(G)$ is a Groebner Basis for $\langle \sigma(G) \rangle$ in $k[x_1, \ldots, x_n]$.*

The purpose for specifying the initial case distinction is to reduce the complexity of the computations and allow some specializations in advance. This becomes useful for reducing the number possible degenerate cases in algebraic geometric theorem proving (see section 3.1). That is, we can preset some polynomial and rational functions in the symbolic parameters to be interpreted as equalities and inequalities throughout the course of the computation.

In table 1.6 is our algorithm **GROEBNERSYSTEM** which computes a GS for I over B. Essentially, the algorithm carries out the Buchberger procedure, but with the added feature that it keeps careful record, via conditions and the coloring rules, of those coefficients of polynomial terms that will become zero or nonzero by

$i \neq j$,

$$\mathrm{Spoly}(g_i, g_j) \stackrel{G}{\Longrightarrow} 0.$$

This result led to the celebrated Buchberger Algorithm to construct a Groebner Basis for an ideals $I = \langle f_1, \ldots, f_t \rangle$: first set G to be the generating set $\{f_1, \ldots, f_t\}$, and then compute the normal form of the S-polynomial of a pair of polynomials $p \neq q$ in G. If this normal form is different from zero, then append it to the list G to make a new list G'. Then, continue this procedure of appending nonzero normal forms of S-polynomials of distinct pairs of polynomials to the current generating list until, for all distinct pairs of polynomials, the normal form of each S-polynomial of each pair is zero modulo the current generating list. If this algorithm never terminated, we would have, first, a strictly increasing chain of subsets

$$G \subset G_1 \subset \cdots \subset G_i \subset G_{i+1} \subset \cdots,$$

where $G_{i+1} = G_i \cup \{k\}$ and k is the nonzero normal form of some S-polynomial of a pair of polynomials in G_i. Note that, by definition, $\mathrm{HM}(k)$ is not in $\langle \mathrm{HM}(G_i) \rangle$. Secondly, the above chain would then give rise to the strictly increasing chain

$$\langle \mathrm{HM}(G) \rangle \subset \langle \mathrm{HM}(G_1) \rangle \subset \cdots \subset \langle \mathrm{HM}(G_i) \rangle \subset \langle \mathrm{HM}(G_{i+1}) \rangle \subset \cdots$$

of monomial ideals. But such chains are impossible by the Hilbert Basis Theorem (pg. 77 of [2]). Alternatively, all one needs to show termination is the lemma 1.5.1 (pp.213-214 of [1]) below.

We refer to [2], [1] for the technical proof that this procedure gives a Groebner Basis as defined above. In outline, if $f \in I$, and $G = \{g_1, \ldots, g_t\}$ is a generating set for I from the Buchberger algorithm, then f may be written in the form $f = \sum h_i \, g_i$ for some $h_i \in R$ where $\mathrm{multideg}(f) \leq \max(\mathrm{multideg}(h_i \, g_i))$. If equality holds, then, for some i, we have that $\mathrm{HM}(f)$ is divisible by $\mathrm{HM}(g_i)$, and thus $\mathrm{HM}(f)$ is in $\langle \mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_t) \rangle$. If the inequality is strict, then some cancellations of

Definition 1.5.3 *Fix a monomial order $\leq$ on M. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal I is a* **Groebner Basis** *of I if*

$$\langle \mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_t) \rangle \supseteq \langle \mathrm{HM}(I) \rangle.$$

Thus we see that, if G is a Groebner Basis for I, then we have a finite generating set for the monomial ideal $\langle \mathrm{HM}(I) \rangle$.

Groebner bases can be used to solve the **ideal membership problem**: given an ideal I and a polynomial $f \in R$, the problem is to determine if $f \in I$. So let G be a generating set for I. Then clearly, if the normal form of f modulo G is zero, then f may be written as a linear combination of the generators of I, and hence is in I. Since the normal form of f modulo G depends on the given monomial order, and the sequence of divisors used to do the reductions, it is not true in general that if $f \in I$ then the normal form of f modulo any finite basis for I must necessarily be zero. But, suppose that G is a Groebner Basis of I. Then let r be a normal form of f modulo G, so $f = g + r$ where $g = a_1 g_1 + \cdots + a_t g_t$ is in I. If $f \in I$, then $r = f - g \in I$ also. By definition of normal form, no monomial of r is divisible by any $\{\mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_t)\}$. If r is nonzero, we then have a contradiction since, $\mathrm{HM}(r) \in \langle \mathrm{HM}(I) \rangle = \langle \mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_t) \rangle$ by definition of G. Therefore, r must be zero, and we have the nice result that if G is a Groebner Basis for I, then $f \in I$ if and only if the normal form of f modulo G is zero. In fact, we may alternatively define a Groebner Basis for I to be any generating set G for I with the property that, if $f \in I$, then the normal form of f modulo G must be zero [2]. This argument also shows that any Groebner Basis of I is a basis for I.

For any given monomial order, it can be shown that any nontrivial ideal I has a Groebner Basis. All algorithms to construct Groebner Bases have their foundations in the following result of Buchberger (see pgs. 84-90 of [2], and chapter 5 of [1]).

Theorem 1.5.2 (Buchberger's Criterion) *Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Groebner Basis for I if and only if for all pairs*

$f_1, \ldots, f_t \in I$. Any finite subset $\{f_1, \ldots, f_t\}$ of I such that $I = \langle f_1, \ldots, f_t \rangle$ is called a generating set or **basis** for I. In this section we present our main algorithm **GROEBNERSYSTEM** (Table 1.6) [7] which computes a "Groebner system." This is then used to construct a Comprehensive Groebner Basis. To make the construction clear, we first recall the definition and construction of Groebner Bases from facts about monomial ideals and normal forms (remainders) of S-polynomials.

Definition 1.5.1 *An ideal I of $k[x_1, \ldots, x_n]$ is a* **monomial ideal** *if there exists a subset $A \subset \mathbf{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, \ldots, x_n]$. In this case, we write $I = \langle x^\alpha : \alpha \in A \rangle$.*

It is a fact that any monomial x^β lies in a monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ if and only if x^β is divisible by some monomial x^α, $\alpha \in A$. It is also true that a polynomial f is in a monomial ideal I if and only if every monomial of f is in I. We also have the following important theorem [2].

Theorem 1.5.1 (Dickson's Lemma) *Every monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ may be written in the form $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$ where the generators x^{α_i} have their multindicies $\alpha_i \in A$. Thus we can always extract a finite generating set for I from the set $\{x^\alpha : \alpha \in A\}$.*

Definition 1.5.2 *Let $I \neq \{0\}$ be an ideal of $R = k[x_1, \ldots, x_n]$. Then we denote by* $\mathrm{HM}(I)$ *the set of head monomials of all polynomials in I. We denote by* $\langle \mathrm{HM}(I) \rangle$ *the monomial ideal generated by the set* $\mathrm{HM}(I)$.

Note that whenever a set of polynomials $\{g_1, \ldots, g_t\}$ is a generating set for an ideal I, then, since $f \in I$ implies $\mathrm{HM}(f_i) \in \mathrm{HM}(I)$, we always have the inclusion

$$\langle \mathrm{HM}(g_1), \ldots, \mathrm{HM}(g_t) \rangle \subseteq \langle \mathrm{HM}(I) \rangle.$$

term of g, nor to select the *first* nongreen term of g divisible by the head term of this divisor. In fact, in the proof of Proposition 5.22 in [1], the unconditional **NORMALFORM** algorithm only requires that, while there exists *some* divisor p of P and *some* nongreen term of $a \cdot t$ of g such that g can be reduced, then perform the reduction. Thus, our algorithm **REDUCIBLE** is but one of several possible ways to chose a divisor $p \in P$ useful for reduction. It seems to be an interesting, and to our knowlege, open question as to the perhaps optimal way for chosing divisors to minimize the number of reduction steps. Perhaps, given a divisor set $P = \{p_1, \cdots, p_m\}$, substantial savings could be gained by first re-ordering P so that $\mathrm{HM}_\gamma(p_i)$ is greater than $\mathrm{HM}_\gamma(p_{i+1})$ and then move sequentially through this re-ordered list as we do in our **REDUCIBLE**. The advantage may be that larger terms would then be canceled first.

We end this section by quoting the rest of lemma 3.2 in [7].

Lemma 1.4.2 *Let γ be a condition such that $\Sigma_\gamma \neq \emptyset$, let $\sigma \in \Sigma_\gamma$, and $P \subset S$. Then*

(i) $f \xrightarrow{P} g[\gamma]$ *implies* $\sigma(f) \xrightarrow{\sigma(P)} \sigma(g)$ *or* $\sigma(f) = \sigma(g)$,
(ii) $f \overset{P}{\Rightarrow} g[\gamma]$ *implies* $\sigma(f) \overset{\sigma(P)}{\Longrightarrow} \sigma(g)$, *and*
(iii) *if f is irreducible modulo P relative to γ, then $\sigma(f)$ is irreducible modulo $\sigma(P)$ in $k'[x_1, \cdots, x_n]$.*

We omit the mechanical proof since it follows as in the proof of lemma 1.3.1. The conclusion $\sigma(f) = \sigma(g)$ of (i) may occur if the chosen σ specializes the *white* coefficient a in the reducible term $a \cdot t$ of f to zero.

1.5 Main Groebner System Algorithm

By the Hilbert Basis Theorem we know that every ideal I of $R = k[x_1, \ldots, x_n]$ is finitely generated, that is $I = \langle f_1, \ldots, f_t \rangle = \left\{ \sum_{i=1}^{t} h_i f_i \,|\, h_i \in R \right\}$ for some

Table 1.5, Algorithm **NORMALFORM**

Input: Condition γ, set of divisors F determined by γ, polynomial f.
Output: A normal form of f with respect to F relative to γ.
$g := f$
$P := F - \{f \in F \,|\, \text{cond\_part}_\gamma(f) = 0\}$
pair:=**REDUCIBLE**(g, P, γ)
WHILE pair $\neq \emptyset$ **DO**
    $s := t/\text{HM}_\gamma(p_i)$
    $g := \text{HC}_\gamma(p_i) \cdot g - a \cdot s \cdot p_i$ (or) $g := g - \left(\dfrac{a}{\text{HC}_\gamma(p_i)}\right) \cdot s \cdot p_i$
    pair:= **REDUCIBLE**(g, P, γ)
Return(g)

If pair is not the empty set then we have found a divisor p_i in P that can be used to reduce g. The subtraction step subtracts, at least, the term $a \cdot t$ from g. We then call **REDUCIBLE** again on this new g. Just like in the usual division algorithm, we again scan through our set of divisors, starting with the first divisor p_1 in P, until we find one that will reduce the new g.

If the algorithm never terminated, then we would have an infinite chain of reductions of the form

$$g \xrightarrow{P} g_1[\gamma] \xrightarrow{P} g_2[\gamma] \cdots.$$

By the lemma 1.4.1, this chain would then give rise to the strictly decreasing, nonterminating chain

$$\text{cond\_part}_\gamma(g) > \text{cond\_part}_\gamma(g_1) > \text{cond\_part}_\gamma(g_2) > \cdots.$$

But this contradicts the well-ordering property of the quasi order $\leq$ on S. **End**

From the proof of lemma 1.4.1 we see that our **REDUCIBLE** algorithm could be made more flexible. It is not necessary, in general, in our choice of pair=$[p_{i_0}, a \cdot t]$, to always select the *first* divisor in P whose head monomial divides a nongreen

Again, it is not necessarily the case that all terms in the first sum are greater than all terms in the second sum. Now look at the r_i's. Note that none of them can be zero, else they would be colored *green*. They are either of the form $r_i = d_i - \tilde{a}_i$ for like terms $t_i^f = t_j$ in $\sum_2$, or just of the form $r_i = d_i$. The main point is that the number of summands in $\sum r_i \cdot t_i^g$ is less or equal to the number of summands in $\sum d_i \cdot t_i^f$; so $m \leq n$.

Let $g' = \text{cond\_part}(g) = \sum_{i=1}^{m} r_i \cdot t_i^g + \sum' h_i' \cdot s_i^g$, where h_i''s are nongreen terms of the third sum of g.

Now, $T(f') = \{d_i \cdot t_i^f, a \cdot t, e_i' \cdot s_i^f\}$, and $T(g') = \{r_i \cdot t_i^g, h_i' \cdot s_i^g\}$. Let $B = M(f') = \{t_i^f, t, s_i^f\}$, and $A = M(g') = \{t_i^g, s_i^g\}$. Since A and B are finite subsets of monomials, we finish the proof by showing that $A <' B$. This will imply that $g' < f'$ by definition of the order $\leq$ on S.

If $n = m$, then the sets A and B agree until, after the $(n+1)$-st step in the comparison, we have

$$\max(A') = \text{some } s_i^g < t = \max(B').$$

If $n > m$, then there exists an index i_0, $1 \leq i_0 \leq m$ such that A and B agree until, at the i_0-th step we have

$$\max(A') = (i_0+1)\text{-st term in list } A < t_{i_0}^f = \max(B').$$

This ends the proof.

Analysis of NORMALFORM: The first approximation to the normal form of f is f itself, so we initially set the output variable g to be f. We next discard all the divisors in F that are essentially zero under specialization. This means we do not divide by any "zero" polynomials. We then call **REDUCIBLE** to get the first divisor in P that can be used to reduce g relative to the condition γ. If there are no such divisors, then pair will be the empty set and the algorithm terminates. By our earlier remarks, g will be the desired normal form.

two sums have $t_i^f > t$ while the terms in the third sum have $s_i^f < t$. It is not necessarily the case that all terms in the first sum are greater than all terms in the second sum.

Let $f' = \text{cond\_part}(f) = \sum_{i=1}^{n} d_i \cdot t_i^f + a \cdot t + \sum' e_i' \cdot s_i^f$, where e_i''s are nongreen terms in third sum of f. The main idea of this proof is to ignore green terms greater than the term $a \cdot t$ of f in the subtraction.

So, in a subtraction step to construct g (say the one that allows for division of the head coefficient [the proof in the other case follows similarly]), first note that we have $\tilde{p}$ defined as

$$\tilde{p} \equiv \frac{a}{\text{HC}_\gamma(p)} \cdot s \cdot p = \sum \tilde{a}_j \cdot \tilde{t}_j + a \cdot t + \sum \tilde{b}_j \cdot \tilde{s}_j \tag{1.1}$$

where, $\tilde{a}_j = \dfrac{a \cdot a_j}{\text{HC}_\gamma(p)}$, $\tilde{t}_j = s \cdot t_j$, $\tilde{b}_j = \dfrac{a \cdot b_j}{\text{HC}_\gamma(p)}$, and $\tilde{s}_j = s \cdot s_j$. Now, by the rules for coloring products, the $\tilde{a}_j$'s remain colored *green*. The color of the $\tilde{b}_j$'s depends on the color of a and b_j. To prepare for the subtraction step, the first sum in the above may be split into two parts:

$$\sum_1 \tilde{a}_j \cdot \tilde{t}_j + \sum_2 \tilde{a}_j \cdot \tilde{t}_j, \tag{1.2}$$

where the first sum consists of terms whose monomials are unlike the monomials of any term in the second sum of f, and the second sum consists of terms whose monomials are like some monomial of some term in the second sum of f.

After subtraction, write g as

$$\begin{aligned} g &= f - \tilde{p} \\ &= \left(\sum c_i \cdot t_i^f - \sum_1 \tilde{a}_j \cdot \tilde{t}_j\right) + \left(\sum_{i=1}^{n} d_i \cdot t_i - \sum_2 \tilde{a}_j \cdot \tilde{t}_j\right) + 0 + \sum h_i \cdot s_i^g \\ &= \sum q_i \cdot t_i^g + \sum_{i=1}^{m} r_i \cdot t_i^g + 0 + \sum h_i \cdot s_i^g \end{aligned}$$

where q_i's are *green*, r_i's are nongreen, and h_i's can be any color. All terms in the first and second summations have $t_i^g > t$, and those in the third sum have $s_i^g < t$.

$$\max(A) = \max(B) \text{ and } A' \leq' B'.$$

Thus, we see that if the maxima of the sets A and B agree, we drop this maxima from A and B and test again $\leq'$ on the sets A' and B'. The reader can convince himself that if A is a proper subset of B then $A <' B$, where this means $A \leq' B$ but $B \not\leq' A$. By Theorem 4.69 of [1], $(\mathcal{P}_{\text{fin}}(M), \leq')$ is, like M, a total, well-ordered set.

Now, let $f = \sum a_i \cdot t_i \in S$. We have $T(f) = \{a \cdot t \,|\, a \cdot t \text{ is a summand in } f\}$ as the set of all terms of f. Let $M(f) = \{t \in M \,|\, a \cdot t \in T(f)\}$ be the set of monomials of terms of f. We then define the relation $\preceq$ on S by

$$f \preceq g \text{ if and only if } M(f) \leq' M(g).$$

By Theorem 5.12 of [1], $\preceq$ is a quasi (reflexive, transitive, anti-symmetric), well-order on S. Note that $\preceq$ is not a total order. For example, if $f = ax^2y + by$ and $g = cx^2y + dy$, where a, b, c, d are distinct, then $M(f) = M(g) = \{x^2y, y\}$, and we have both $f \preceq g$ and $g \preceq f$ with $f \neq g$. In the sequel we will write $\leq$ for $\preceq$ on S.

Lemma 1.4.1 *If* $f \xrightarrow{p} g[\gamma]$ *then* $\text{cond\_part}_\gamma(g) < \text{cond\_part}_\gamma(f)$ *(see lemma 3.2 of [7]).*

Proof. By definition of $f \xrightarrow{p} g[\gamma]$, we may write p as

$$p = \sum a_j \cdot t_j + \text{HC}_\gamma(p) \cdot \text{HM}_\gamma(p) + \sum b_j \cdot s_j$$

where all a_j are *green*, $t_j > \text{HM}_\gamma(p)$, HC_γ(p) is *red*, b_j's may be any color, $s_j < \text{HM}_\gamma(p)$, and we may write f as

$$f = \sum c_i \cdot t_i^f + \sum_{i=1}^{n} d_i \cdot t_i^f + a \cdot t + \sum e_i \cdot s_i^f$$

where, (i) $t = s \cdot \text{HM}_\gamma(p)$ for some monomial s, and (ii) the c_i are *green*, d_i are nongreen, a is either *red* or *white*, e_i are any color. Further, the terms in the first

monomial of any nongreen term of f. **End**

Table 1.5 gives our algorithm to compute a normal form. The algorithm differs significantly from the usual division algorithm in that we do not keep track of quotients nor do we detach terms from intermediate dividends to a seperate remainder polynomial. For our purposes, we are primarily interested in just the normal forms (remainders) in our analog to the Buchberger algorithm to generate Comprehensive Groebner Bases.

To smoothly prove the termination part of the **NORMALFORM** algorithm, we state the definitions to construct a quasi, well-founded order on S, i.e. this order will be reflexive and transitive and have the very important property that any strictly descending chain of elements must terminate (see [7], and sections 4.2-4.3, 5.1 of [1]).

Due to the one-to-one correspondence between monomials x^α and their multindicies $\alpha \in \mathbf{Z}^n_{\geq 0}$, any ordering $\leq$ on $\mathbf{Z}^n_{\geq 0}$ gives an ordering $\leq$ on the set of monomials $M = \{x^\alpha\}$, i.e $\alpha \leq \gamma$ if and only if $x^\alpha \leq x^\gamma$. Recall, that $\leq$ is a **monomial ordering** ([2]) if, (i) $\leq$ is a total (linear) order (so precisely one of $\alpha < \gamma$, $\alpha = \gamma$, or $\alpha > \gamma$ is true), (ii) $\leq$ is preserved under addition (so for $\delta \in Z^n_{\geq 0}$, and $\alpha < \gamma$, we have $\alpha + \delta \leq \gamma + \delta$), and (iii) $\leq$ is a well-ordering (so every strictly decreasing sequence

$$\alpha_1 > \alpha_2 > \ldots$$

terminates).

Let $\mathcal{P}_{\text{fin}}(M)$ be the set of all finite subsets of M including $\emptyset$. If $A \in \mathcal{P}_{\text{fin}}(M)$ is not empty, then A has a maximal and minimal element with respect to the ordering $\leq$ on M. Denote these elements by $\max(A)$ and $\min(A)$ respectively. Let $A' = A - \{\max(A)\}$. Then we define a relation $\leq'$ on $\mathcal{P}_{\text{fin}}(M)$ as follows. Let $A, B \in \mathcal{P}_{\text{fin}}(M)$. Then if $A = \emptyset$, $A \leq' B$, otherwise $A \leq' B$ iff $B \neq \emptyset$ and

$$\max(A) < \max(B) \text{ or}$$

Table 1.4, Algorithm **REDUCIBLE**

Input: Polynomial f, divisor set P, and a condition γ such that $\mathrm{HM}_\gamma(p)$ is defined for all $p \in P$ for $P \neq \emptyset$
Output: Either the pair $[p_{i_0}, a \cdot t]$, as described above, or $\emptyset$

found:=false
pair:=$\emptyset$
IF $P \neq \emptyset$ **and** cond_part(f) $\neq 0$ **THEN**
  FOR $i := 1$ **WHILE** ($i \leq |P|$ **and** found = false) **DO**
    FOR $j := 1$ **THRU** $|T(\text{cond\_part(f)})|$ **DO**
      term$_j$:= j-th term, $a \cdot t$, in the ordered list T(cond_part(f))
      IF $\mathrm{HM}_\gamma(p_i) | t$ **THEN**
        pair:= $[p_i, a \cdot t]$
        found:=true
Return(pair)

Analysis of REDUCIBLE: Let $|A|$ be denote the cardinality of a finite set A. If P is empty or all terms of f are *green*, then f is conditionally irreducible modulo the divisor set P relative to γ, and the routine returns $\emptyset$. So assume $P \neq \emptyset$, $\mathrm{HM}_\gamma(p)$ is defined for all $p \in P$, and cond_part(f) $\neq 0$. Taking each divisor p_i in turn, starting from the first one, p_1, and moving sequentially through the list P, the routine searches the ordered set of nongreen terms of f for the first term $a \cdot t$ such that $\mathrm{HM}_\gamma(p_i)$ divides t. If successful, the routine sets the output variable "pair" equal to $[p_{i_0}, a \cdot t]$, where p_{i_0} is the first divisor whose head monomial divides the monomial of a nongreen term of f, and $a \cdot t$ is the first such nongreen term such that $\mathrm{HM}_\gamma(p_{i_0})$ divides t. Pair will then have the desired properties. The routine then sets found=true and exists both **FOR** loops. If we exhaust all the divisors in P, the counter i will increment to $i + 1 > |P|$. When this happens, the routine returns the default value, pair = $\emptyset$. Thus, no $\mathrm{HM}_\gamma(p)$, for any $p \in P$, divides the

i) *either* $g = f$ *or* g *is obtained from* f *by a finite number of iterated reductions using the elements of* P, *i.e. there exists a finite sequence of the form*

$$f \xrightarrow{P} f_1[\gamma] \xrightarrow{P} f_2[\gamma] \xrightarrow{P} \cdots \xrightarrow{P} f_{n-1}[\gamma] \xrightarrow{P} g[\gamma]$$

where each $f_i \in S$, *and*

ii) g *is not reducible modulo* P *relative to* γ.

The definition means that a polynomial g is a normal form of a polynomial f if, after iterated subtractions of nongreen terms divisible by defined head monomials of elements in P, g is a Q-linear combination of monomials such that no nongreen one is divisible by any defined $\mathrm{HM}_\gamma(p)$, p in P. Thus, we see that the set P acts as a set of divisors, and the normal form is the conditional analogue to the usual remainder in the multivariable division algorithm (see also [7], and pgs. 155, 175, 196-199 of [1]).

In our algorithm **NORMALFORM** in Table 1.5, we used the subroutine, **REDUCIBLE**, in Table 1.4. The subroutine decides, given a polynomial $f \in S$, a set of divisors $P \subset S$, and a condition γ, if f is reducible modulo P relative to γ. The routine allows the input divisor list P to be empty or nonempty. If $P = \emptyset$, the routine returns $\emptyset$ indicating that f is (vacuously) irreducible. If $P = \{p_1, \ldots, p_m\} \neq \emptyset$, the routine assumes that $\mathrm{HT}_\gamma(p)$ is defined for each p in P. In this case, the algorithm searches for an ordered pair $[p_{i_0}, a \cdot t]$ where

i) p_{i_0} is the first polynomial in the subscripted list P whose head monomial divides the monomial of some nongreen term of f, and

ii) $a \cdot t$ is the first nongreen term of g such that $\mathrm{HM}_\gamma(p_{i_0})$ divides t.

This pair gives the first polynomial p_{i_0} in P such that f reduces modulo p_{i_0} relative to γ. If $P \neq \emptyset$ and no such pair with the above properties may be found for a given f and condition γ, then the routine returns $\emptyset$.

(ii) f **reduces to** g **modulo** P **relative to** γ, (written $f \xrightarrow{P} g[\gamma]$), *if* $f \xrightarrow{p} g[\gamma]$ *for some* $p \in P$,

(iii) f *is* **reducible modulo** p **relative to** γ, *if there exists* $g \in S$ *such that* $f \xrightarrow{p} g[\gamma]$, and

(iv) f *is* **reducible modulo** P **relative to** γ, *if there exits* $g \in S$ *such that* $f \xrightarrow{P} g[\gamma]$.

The subtraction steps in parts (i) of the above are constructed to remove, at least, the term $a \cdot t$ from f, e.g. note,

$$\frac{a}{\mathrm{HC}_\gamma(p)} \cdot s \cdot \mathrm{HT}_\gamma(p) = \frac{a}{\mathrm{HC}_\gamma(p)} \cdot s \cdot \mathrm{HC}_\gamma(p) \cdot \mathrm{HM}_\gamma(p) = a \cdot t.$$

As in the choice for the S-polynomial, we will refer to the subtraction steps where we do not divide by the head coefficient of p as performing pseudo-division.
We next give definitions ([7],[1]) for normal forms of a polynomial.

Definition 1.4.3 *A* **normal form of a polynomial** $f \in R$ **with respect to a set of polynomials** $P \subset R$, *is a polynomial* $g \in R$, *(denoted* $f \overset{P}{\Rightarrow} g$*), such that*

i) *either* $g = f$ *or* g *is obtained from* f *by a finite number of iterated reductions using the elements of* P, *i.e. there exists a finite sequence of the form*

$$f \xrightarrow{P} f_1 \xrightarrow{P} f_2 \xrightarrow{P} \cdots \xrightarrow{P} f_{n-1} \xrightarrow{P} g$$

where each $f_i \in S$, *and*

ii) g *is not reducible modulo* P.

Definition 1.4.4 *A* **normal form of a polynomial** $f \in S$ **with respect to a set of polynomials** $P \subset S$ ***relative to a condition*** γ, *is a polynomial* $g \in S$, *(denoted* $f \overset{P}{\Rightarrow} g[\gamma]$*), such that*

tions for polynomials in $R = k[x_1, \ldots, x_n]$. For reference, see [7], pgs. 195-200 of [1], and section 3, chapter 2 of [2].

Definition 1.4.1 *Let f, p, g be polynomials in $R = k[x_1, \ldots, x_n]$, and let P be a subset of R. Then we say*

(i) f **reduces to** g **modulo** p, (written $f \xrightarrow{p} g$), if

a) *there exists some term $a \cdot t$ of f such that* $\mathrm{HM}(p)$ *divides t, i.e. we have $t = s \cdot \mathrm{HM}(p)$ for some monomial s, and,*

b) $g = \mathrm{HC}(p) \cdot f - a \cdot s \cdot p$ (alternatively) $g = f - \dfrac{a}{\mathrm{HC}(p)} \cdot s \cdot p$,

(ii) f **reduces to** g **modulo** P, (written $f \xrightarrow{P} g$), *if $f \xrightarrow{p} g$ for some $p \in P$,*

(iii) f *is* **reducible modulo** p, *if there exists $g \in R$ such that $f \xrightarrow{p} g$,* and

(iv) f *is* **reducible modulo** P, *if there exits $g \in R$ such that $f \xrightarrow{P} g$.*

Conditional versions [7] of these are:

Definition 1.4.2 *Let f, p, g be polynomials in S, let γ be a condition, and let P be a subset of S. Then we say*

(i) f **reduces to** g **modulo** p **relative to the condition** γ, (written $f \xrightarrow{p} g[\gamma]$), if

a) $\mathrm{HT}_\gamma(p)$ *is defined, and*

b) *there exists some term $a \cdot t$ of f such that $t \in T_{red}(f) \cup T_{white}(f)$ and $\mathrm{HM}_\gamma(p)$ divides t, i.e. we have $t = s \cdot \mathrm{HM}_\gamma(p)$ for some monomial s, and,*

c) $g = \mathrm{HC}_\gamma(p) \cdot f - a \cdot s \cdot p$ (alternatively) $g = f - \dfrac{a}{\mathrm{HC}_\gamma(p)} \cdot s \cdot p$,

then declare f to be: i) *green* if at least one of the numerator factors is *green* and all the denominator factors are *red*, or ii) *red* if all factors of numerator and denominator are *red*, or iii) *white*. Unfortunately, although most computer algebra systems have some sort of factoring facilities available if k is the field of rational numbers, these algorithms would prove ultimately to be impractical for our use (see [3]). These more refined tests would slow down our computations considerably. See our section 2.1, however, for discussion of ways around this difficulty.

Therefore, we deliberately chose, in our implementation for the basic construction that, a function would be declared *green* (*red*) if and only if that function is either $0 \in k$ (in $k - \{0\}$) or a nonzero constant times a function in the respective *green* (*red*) list of a condition. The trade-off for doing such simple coloring tests is that the condition lists tend to get quite large. This is what happens in the MAS implementation.

Implementing algorithmic procedures to color polynomials and perform all the arithmetic is far from trivial! We present the main ideas of our MACSYMA implementation in the appendix. Part of the difficulty lies in that one must always carry along the color of the coefficient of a term in f.

1.4 Conditional Division Algorithm

In this section we present our normal form algorithm which plays the role of the usual multivariable long division algorithm. Recall that in the usual long division algorithm, we perform a series of iterated subtractions from an intermediate dividend p when the head monomial of some polynomial in a fixed set of divisors divides the head monomial in p. As in the case of the S-polynomial, there are several ways to perform the subtractions. We will indicate two of the customary alternatives in the definitions that follow. They differ as to whether one allows multiplications by reciprocals of the head coefficients. First, we give the defini-

be the polynomial obtained from f by deleting all the green colored terms. Hence $T(\text{cond\_part}(f)) = T_{red}(f) \cup T_{white}(f)$.

Remarks: Essentially, computing cond_part(f) means to compress out of f all terms that will become zero under specialization. Note that cond_part$(f) = f$ if and only if $T_{green}(f) = \emptyset$, and cond_part$(f) = 0$ if and only if $T(f) = T_{green}(f)$. If δ is a sucessor to γ, then $T_{green,\gamma}(f) \subseteq T_{green,\delta}(f)$. Hence, $T(\text{cond\_part}(\text{col}^0_\delta(f)))$ $\subseteq T(\text{cond\_part}(\text{col}^0_\gamma(f)))$. We will use the conditional part of a polynomial in our algorithms in the next sections.

1.3.1 Theoretical and Practical Remarks about Colorings

First, it is important to observe that in our scheme for direct assignments of colors and the colored arithmetic rules, we are only allowed to color the sum, product, or reciprocal of functions in Q given that we know *a priori* their colors according to a fixed condition γ. This becomes important because any element in Q may be written as a sum of two other elements in Q but *not* uniquely. For example, suppose $\gamma = (\{2u + v\}, \{-5v\})$, and $f = 2u - 4v \in Q = k(u, v)$. Let $g = 2u + v$ and let $h = -5v$. Then, since $\text{col}^0_\gamma(g)$ is *red* and $\text{col}^0_\gamma(h)$ is *green*, the color of

$$f = g + h = (2u + v) + (-5v) = 2u - 4v$$

is *red*. But if we write $f = a + b$ where $a = 2u$, and $b = -4v$, then our scheme would color f *white*. Therefore, in our implementation, we took as our working methodology that, if we were to color a sum of two elements *green* or *red*, then we must first know the color of each summand *a priori*. We took this same view toward products of any two elements, i.e. we insisited that we must know the color of each of the two terms *a priori* before we could assign a color to their product.

Since R is a unique factorization domain, we could, in theory, take a rational function f in Q, factor both its numerator and denominator into irreducibles, and

Proof. Since $\mathrm{HC}_\gamma(f)$ is *red*, then, upon specialization by $\sigma \in \Sigma_\gamma$, $\sigma(\mathrm{HC}_\gamma(f))$ will be nonzero. Thus, it is not hard to see that

$$\sigma(\mathrm{HT}_\gamma(f)) = \sigma(\mathrm{HC}_\gamma(f)) \cdot \sigma(\mathrm{HM}_\gamma(f)) = \mathrm{HC}(\sigma(f)) \cdot \mathrm{HM}(\sigma(f)) = \mathrm{HT}(\sigma(f)).$$

Similarly for g. Therefore, since σ is a ring homomorphism, we have (using the second version of conditional S-polynomial)

$$\begin{aligned} \sigma(\mathrm{Spoly}_\gamma(f,g)) &= \sigma\left(\frac{1}{\mathrm{HC}_\gamma(f)} \cdot s \cdot f\right) - \sigma\left(\frac{1}{\mathrm{HC}_\gamma(g)} \cdot t \cdot g\right) \\ &= \frac{1}{\mathrm{HC}(\sigma(f))} \cdot s \cdot \sigma(f) - \frac{1}{\mathrm{HC}(\sigma(g))} \cdot s \cdot \sigma(g) \\ &= \mathrm{Spoly}(\sigma(f), \sigma(g)). \end{aligned}$$

The proof is similar for the first version of the conditional S-polynomial. This ends the proof.

Let f and g be two polynomials that have been directly colored by some condition γ. In general, as the result of some computation using f and g, (such as computing the S-poly above), the resulting polynomial's coefficients will inherit their colors. This means that it is possible for some coefficients to be *green* or *red* even though they may not appear in the green or red lists of γ, nor may they satisfy other criteria in the definition of what it means to be colored directly by γ. From this observation, we have found it helpful to distinguish between a "direct" colorings (in the sense of the definition) and "indirect" colorings. Given any colored polynomial, however obtained, we define the sets $T_{green}(f)$, $T_{red}(f)$, and $T_{white}(f)$ to be the ordered subsets of $T(f)$ of terms that have been assigned, by some rules, the colors *green*, *red*, and *white* respectively. The absence of the subscript γ in these notations (as distinct from that which appears in the notation $T_{green,\gamma}(f)$) is to indicate that these are sets of terms whose colors have been inherited by some computations involving colored polynomials.

Definition 1.3.2 *Let f be a polynomial whose coefficients have been assigned colors by some scheme. Then we define the* **conditional part** *of f,* $\mathrm{cond\_part}(f)$*, to*

definition makes sense for all successor conditions to γ since the color of nonwhite functions are preserved by the successors.

With this definition it is clear how to define a *colored arithmetic* on polynomials in S with respect to a given condition γ. That is, we add and multiply the polynomials in the usual way with the additional feature that any term *inherits* the color of its combined coefficients according to the color rules established by γ. Therefore, our calculation for the $\mathrm{Spoly}_\gamma(f,g)$ is well-defined. It cancels the conditonal head terms from f and g and colors all terms in the difference. The colorings of these terms will usually vary widely depending on the condition γ.

Example 1.3.1 Let $k = \mathbf{R}$, $f = (u^2-2)x^3y + (w+1)xy + 4v$, $g = x^2 + u$ in $k(u,w,v)[x,y]$ with $x > y$. Let $\gamma = (\{u^2-2\},\{w+1\})$. Then $\mathrm{HT}_\gamma(f) = (w+1)xy$, and $\mathrm{HT}_\gamma(g) = x^2$. Thus, $t_0 = x^2y$, $s = x$, $t = y$, and (inverting the head coefficients) gives

$$\mathrm{Spoly}_\gamma(f,g) = \frac{u^2-2}{w+1}x^4y + \frac{4v}{w+1}x - uy$$

where the first term is *green*, and the last two are *white*. Observe that in this case the conditional head term of $\mathrm{Spoly}_\gamma(f,g))$ is undefined.

Lemma 1.3.1 *Let γ be a condition, and let $\sigma \in \Sigma_\gamma$. Then for any f,g with $\mathrm{HT}_\gamma(f)$, $\mathrm{HT}_\gamma(g)$ defined, we have*

$$\sigma(\mathrm{Spoly}_\gamma(f,g)) = \mathrm{Spoly}(\sigma(f),\sigma(g)).$$

This lemma (lemma 3.2 in [7]) says that, for any $f,g \in S$ with defined head terms, the specialization of their conditional S-polynomial is the usual S-polynomial of their specializations $\sigma(f),\sigma(g) \in R$.

In the sequel, we will refer to the first alternative in the **SPOLY** algorithm as using "pseudo-division" since we do not invert the head coefficients. The **SPOLY** algorithm simply cancels the conditional head terms from f and g. However, it is important to keep in mind that we are performing all arithmetical operations here on colored polynomials. Thus, in order for the above calculation to make sense, we need to define some rules for combining coefficients in Q colored by some given condition. This will be our next task. This definition is what we will refer to as the "arithmetic" aspect of colorings.

Definition 1.3.1 *Let γ be a condition, let a, b be functions in Q colored by γ or any successor to γ. Then we define the following* **colored arithmetic governed by** γ *as follows:*

$\mathrm{col}(-a) = \mathrm{col}(a)$,
$\mathrm{col}(a+b) =$ *red, if a is colored red, and b is colored green, or vice versa,*
$\mathrm{col}(a+b) =$ *green, if both a and b are colored green,*
$\mathrm{col}(a \cdot b) =$ *red, if both a and b are colored red,*
$\mathrm{col}(a \cdot b) =$ *green, if a or b is colored green, and*
$\mathrm{col}(1/a) =$ *red, if a is colored red.*
In all other cases, $\mathrm{col}(a) =$ *white.*

The working philosophy behind this definition is that functions colored *green* (*red*) will be specialized to zero (nonzero) for any specialization $\sigma \in \Sigma_\gamma$. Thus adding a *green* to a *red* is like adding zero to a nonzero element in k. Similarly, multiplying a *green* times a function of any color is like multiplying zero times any nonzero element in k. Notice that multiplying a function by a *red* will preserve the color of that function; *red* times *green*, *red*, or *white* will be *green*, *red*, or *white* respectively. Further, a *green* minus a *green*, *red*, or *white* will again be *green*, *red*, or *white* respectively. We also allow for taking the reciprocal of a *red*. The

1.3 Conditional S-Polys and Arithmetic of Colored Polynomials

For any two polynomials $f, g \in R = k[x_1, \ldots, x_n]$, let

$$t_0 = \mathrm{LCM}(\mathrm{HM}(f), \mathrm{HM}(g)),$$

$s = t_0/\mathrm{HM}(f)$, and $t = t_0/\mathrm{HM}(g)$. In the literature (e.g. [2], [7]) it is customary to define the S-polynomial of f and g, $\mathrm{Spoly}(f, g)$, as either

$$\mathrm{Spoly}(f, g) = \mathrm{HC}(g) \cdot s \cdot f - \mathrm{HC}(f) \cdot t \cdot g$$

or

$$\mathrm{Spoly}(f, g) = \frac{1}{\mathrm{HC}(f)} \cdot s \cdot f - \frac{1}{\mathrm{HC}(g)} \cdot t \cdot g.$$

In either case the construction is designed to cancel the head terms from f and g. In Table 1.3 we give S-polynomial algorithms for use in constructing Comprehensive Groebner Bases. The algorithms also give our definitions of a **Conditional S-polynomial**, denoted $\mathrm{Spoly}_\gamma(f, g)$, for two polynomials f and g with well-defined conditional head terms. These are the direct analogues to the definitions above. In [7], the first version is preferred without inversion of the head coefficients.

Table 1.3, Algorithm **SPOLY**

Input: Condition γ, polynomials f, g with $\mathrm{HT}_\gamma(f), \mathrm{HT}_\gamma(g)$ defined
Output: Conditional S-polynomial, $\mathrm{Spoly}_\gamma(f, g)$ of f and g defined as:

$t_0 := \mathrm{LCM}(\mathrm{HM}_\gamma(f), \mathrm{HM}_\gamma(g))$
$s := t_0/\mathrm{HM}_\gamma(f), t := t_0/\mathrm{HM}_\gamma(g)$
$\mathrm{Spoly}_\gamma(f, g) := \mathrm{HC}_\gamma(g) \cdot s \cdot f - \mathrm{HC}_\gamma(f) \cdot t \cdot g$ (alternatively)
$\mathrm{Spoly}_\gamma(f, g) := \left(\frac{1}{\mathrm{HC}_\gamma(f)}\right) \cdot s \cdot f - \left(\frac{1}{\mathrm{HC}_\gamma(g)}\right) \cdot t \cdot g$
$\mathrm{Return}(\mathrm{Spoly}_\gamma(f, g))$

Table 1.2, Algorithm **DET**

Input: Condition γ, list of polynomials F
Output: Cover Γ of γ that determines F

IF $F = \emptyset$ **THEN**
$\Gamma := \{\gamma\}$
ELSE
$\Gamma := \bigcup_{\delta \in \mathbf{DET1}(\gamma, f_1)} \mathbf{DET}(\delta, F - \{f_1\})$
Return(Γ)

Analysis of DET: The algorithm clearly terminates because we have it call itself on a finite set with fewer and fewer elements. Eventually, the input to **DET** will be empty. This algorithm is another example of "first-rest" recursion. The algorithm first generates all successor conditions δ from γ necessary to determine the first polynomial, f_1, in F. Then, in the union, for each of these successors, we call the algorithm again to get a set of successors to each successor that will determine the rest of the polynomials in F after f_1. By the remark above, each of these new successors will still determine the first polynomial in F. On the second call to the algorithm, the first polynomial in $F - \{f_1\}$ will be f_2 of F, and so on. This proves the partial correctness of the algorithm. **End**

Basically, the algorithm generates a tree structure of sucessor conditions. That is to say, we first branch off a finite number of successors to the "root" condition γ. These determine f_1. We then treat each of these successors as the "root" for a new tree to branch off from. The union operation then picks the "leaves", i.e. the final successors needed to determine polynomial f_n, off the whole tree. Finally, note that $\mathbf{DET}(\gamma, \{f\}) = \mathbf{DET1}(\gamma, f)$.

of all possible conditions that will determine f.

On the first pass through the above algorithm, $g = f$, and

$$\text{term1}(g) = (u+v)x^2y^2.$$

Since the conditional of the **IF** statement is false, we have

$$\Gamma = \{(\{\}, \{u+v\})\} \cup \mathbf{DET1}((\{u+v\}, \{\}), wy+z).$$

On the second pass through the algorithm, $g = wy + z$, and $\text{term1}(g) = wy$. Thus we have,

$$\Gamma = \{(\{\}, \{u+v\})\} \cup \{(\{u+v\}, \{w\})\} \cup \mathbf{DET1}((\{u+v, w\}, \{\}), z)),$$

etc. The output cover of γ is then the following set of four conditions

$$\Gamma = \{(\{\}, \{u+v\}), (\{u+v\}, \{w\}), (\{u+v, w\}, \{z\}), (\{u+v, w, z\}, \{\})\}.$$

Note that the last condition makes the conditional part of f zero, and that this cover is just large enough to take into account all possible cases of colorings of the coefficients of f to be able to deduce the conditional head term of f.

Example 1.2.2 Let $f = (\frac{u^2+1}{2v})x^3y^3 + (6u(v+1))xy + 32 \in k(u,v)[x,y]$ with $x > y$, and again set $\gamma = (\{\}, \{\})$. The output cover to determine f from γ is $\Gamma = \{\gamma_1, \gamma_2, \gamma_3\}$ where,

$$\begin{aligned}
\gamma_1 &= \left(\{\}, \{\tfrac{u^2+1}{2v}, 2v\}\right), \\
\gamma_2 &= \left(\{\tfrac{u^2+1}{2v}\}, \{2v, 6u(v+1)\}\right), \\
\gamma_3 &= \left(\{\tfrac{u^2+1}{2v}, 6u(v+1)\}, \{2v\}\right).
\end{aligned}$$

The next algorithm, **DET** uses **DET1** to generate a cover of a condition to determine the head terms of a finite set of polynomials $F = \{f_1, \ldots, f_n\}$ of S.

If the conditon on the first "**IF**" statement is false, then this means term1(g) is not the conditional head term of f. Indeed, this first nongreen term must then be colored *white*. Hence, if we color it *red*, then it will become the head term of f. On the other hand, if we color it *green*, then we will have to examine the *next* terms after it as candidates for the head term of f. We thus perform a "first-rest" recursion procedure to take into account both of these eventualities.

We thus first create a successor condition to γ by pushing coef1(g) into the red list of γ (with denominator as necessary). According to this new successor condition, coef1(g) is to be assumed "nonzero." This successor condition then determines f because now term1(g) *will* be the head of f. We now have a condition in the cover Γ that determines f. Next, we call the algorithm again on a second successor condition to γ where we have pushed coef1(g) into the green list of γ (with denominator in redlist, again, as necessary). This declares coef1(g) to be "zero" according to this second successor condition. The head term for f, according to this condition, will now have to be sought from those terms in the polynomial $g - \text{term1}(g)$. To summarize, we may read the first **IF** statement of the algorithm as follows.

If γ does not already determine f, then branch γ into two distinct successor conditions by pushing the coefficient of the first nongreen term of f, coef1(g), into the red list and then the green list of γ (with denominator, if needed). The first successor condition then determines f since term1(g) is now red, the second successor condition will then be used to generate a cover that determines the rest of f.

The algorithm terminates because we have it call itself on a polynomial with fewer and fewer terms. Eventually, g must equal zero. **End**

Example 1.2.1 Suppose that $f = (u+v)x^2y^2 + wy + z \in k(u,v,w,z)[x,y]$ with $x > y$, and $\gamma = (\{\}, \{\})$, the empty condition. We will use γ to generate a cover

Table 1.1, Algorithm **DET1**

Input: Condition γ, polynomial f
Output: Cover Γ of γ that determines f

$g := f$
IF g = 0 **THEN** Return($\Gamma := \{\gamma\}$)
WHILE $g \neq 0$ **and** $\mathrm{col}^0_\gamma(\mathrm{coef1}(g)) = \mathit{green}$ **DO**
    $g := g - \mathrm{term1}(g)$
IF $g = 0$ **or** $\mathrm{col}^0_\gamma(\mathrm{coef1}(g)) = \mathit{red}$ by γ **THEN**
    $\Gamma := \{\gamma\}$
ELSE
    IF $\mathrm{denom}(\mathrm{coef1}(g)) = 1$ **THEN**
        $\Gamma := \{(\mathrm{gr}(\gamma), \mathrm{rd}(\gamma) \cup \{\mathrm{coef1}(g)\})\} \cup$
            DET1$((\mathrm{gr}(\gamma) \cup \{\mathrm{coef1}(g)\}, \mathrm{rd}(\gamma)), g - \mathrm{term1}(g))$
    ELSE
        $\Gamma := \{(\mathrm{gr}(\gamma), \mathrm{rd}(\gamma) \cup \{\mathrm{coef1}(g), \mathrm{denom}(\mathrm{coef1}(g))\})\} \cup$
            DET1$((\mathrm{gr}(\gamma) \cup \{\mathrm{coef1}(g)\}, \mathrm{rd}(\gamma) \cup \{\mathrm{denom}(\mathrm{coef1}(g))\}),$
                $g - \mathrm{term1}(g))$
Return(Γ)

Definition 1.2.4 *Let γ be a condition, $f \in S$, and F a finite subset of S. Then we say*

(i) *a* **cover of a condition γ that determines a polynomial** *f is a case distinction Γ of successor conditions to γ that determines f, and*

(ii) *a* **over of a condition γ that determines a set of polynomials** *F is a case distinction Γ of successors to γ that determines F.*

Our two algorithms **DET1** and **DET** (Tables 1.1 and 1.2) give covers of a condition to determine a single polynomial and a set of polynomials respectively. The first algorithm, **DET1**, gives *all* possible successor conditions to a given condition necessary to determine a polynomial. We present the algorithm, give an analysis of how it works, and then present an example. Given any polynomial $f = \sum a_i \cdot t_i$, let term1(f) denote the first (greatest) term in the summation. Recall that we have assumed the terms in the sum are ordered from greatest to least. For term1(f) = $a \cdot t$, let coef1(f) = a, and monom1(f) = t. If $f = p/q \in Q$, where $q \in Q - k$, then let denom(f) = q. If $f \in P$, then set denom(f) = 1.

Analysis of DET1: Upon entering the algorithm, we first set g to be f. If $g = 0$, then we are done. The output cover to determine f is simply $\Gamma = \{\gamma\}$. Otherwise, starting from first (greatest) term of g, we sequentially discard terms from g colored *green* by γ until the first (greatest) term of g is *red* or *white*, or g becomes zero. Note that this first term is not necessarily the conditional head term of f. It is though the first *nongreen* colored term.

We now show the partial correctness of the algorithm. If $g = 0$ then γ determines f by the second part of the definition of what it means to determine a polynomial. If $g \neq 0$ and coef1(g) is colored *red*, then this means term1(g) is indeed the conditional head term of f. Thus, γ has sucessfully determined f. So, in either of these two cases, the algorithm returns just γ in the cover Γ which is sufficient to determine f.

Thus the conditional head term of f is simply the first *red*, i.e. "nonzero" term one comes to in scanning the terms of f past the *green*, i.e. "zero" terms of f. Note that $\mathrm{HT}_\gamma(f)$ is undefined for a polynomial with a *white* term before its first *red* term, or a polynomial with all terms colored *green*. Hence, it is possible here for $\mathrm{HT}_\gamma(f)$ to be undefined for some polynomials f and γ. The reader is warned that here we have broken with the definitions in [7]. In that paper the head monomial is taken to be our head term, and the head term is taken to be our head monomial.

Definition 1.2.2 *Let γ be a condition, Γ a case distinction, $f \in S$, and F a finite subset of S. Then we say*

(i) γ **determines** f *if* $\mathrm{HT}_\gamma(f)$ *is defined* or *all terms of f are colored green by γ*,
(ii) γ **determines** F *if γ determines each $f \in F$*,
(iii) Γ **determines** f *if γ determines f for all $\gamma \in \Gamma$, and*
(iiv) Γ **determines** F *if Γ determines each $f \in F$.*

Definition 1.2.3 *A* **successor to a condition** γ *is another condition, δ, such that the green and red lists of γ are subsets, respectively, of the green and red lists of δ. Notation: $\delta \supseteq \gamma$.*

Remark 1 It is important to note that if δ is a successor to γ, and γ determines a polynomial f, then so does its successor condition δ. In fact, if $\mathrm{HT}_\gamma(f)$ is defined and $\delta \supseteq \gamma$, then $\mathrm{HT}_\delta(f) = \mathrm{HT}_\gamma(f)$. Thus, successor conditions maintain all previous information about head terms encoded in their predecessors. This observation plays an important role in our algorithm **GROEBNERSYSTEM**. Note also that, if f is a polynomial colored by γ, then to directly "recolor" f with respect to a sucessor to γ it is only necessary to color the terms left *white* according to γ.

Let $\gamma = (\{u\}, \{v, w\})$. Then $3ux^2y$ will be directly colored *green*, vy^2 and wy will be directly colored *red*, and $(v + w)y$ will be colored *white* by γ. For this example, $\Sigma_\gamma = \{\sigma : (u, v, w) \mapsto (a, b, c) \,|\, a = 0, b, c \neq 0\}$. Thus, for the specializations, say, $\sigma_1 : (u, v, w) \mapsto (0, 4, 1)$ and $\sigma_2 : (u, v, w) \mapsto (0, 1, -2)$ in Σ_γ, we have $\sigma_1(f) = 4xy^2 + y + 9y$ and $\sigma_2(f) = xy^2 - 2y$ in $k[x, y]$.

Let $f \in S$ and let γ be some given condition. Suppose f has been colored by γ. Denote by $T_{green,\gamma}(f)$, $T_{red,\gamma}(f)$, and $T_{white,\gamma}(f)$ the disjoint subsets of $T(f)$ consisting of those terms of f directly colored *green*, *red*, or *white* respectively by γ. We will assume that these sets are ordered like $T(f)$ by the given monomial ordering $\leq$ on M.

1.2 Conditional Head Terms and the Determine Algorithm

In the algorithmic machinery used to compute Groebner Bases, e.g. the division algorithm and S-polynomials, it is of paramount importance to be able to determine the leading, or head, term of any given polynomial with respect to some well-defined monomial ordering. In our algorithms we will be dealing with colored polynomials. Let $\leq$ be a monomial ordering on M.

Definition 1.2.1 *Let f be a polynomial in S, and let γ be a condition. Then we say*

> (i) *a term $a \cdot t \in T(f)$ is the* **conditional head term of f relative to γ**, *denoted* $\mathrm{HT}_\gamma(f)$, *if a is directly colored red by γ and all greater terms $b \cdot t' \in T(f)$, where $t' \geq t$, have b directly colored green by γ, and*
> (ii) *if $\mathrm{HT}_\gamma(f) = a \cdot t$, then a is the* **conditional head coefficient of f relative to γ**, *denoted* $\mathrm{HC}_\gamma(f)$, *and t is the* **conditional head monomial of f relative to γ**.

defined as follows:

$\mathrm{col}^0_\gamma(a) =$ *green, if* a *is the zero in* k,

$\mathrm{col}^0_\gamma(a) =$ *red, if* a *is invertible in* k,

$\mathrm{col}^0_\gamma(a) =$ *green, if* $a \in \mathrm{gr}(\gamma)$,

$\mathrm{col}^0_\gamma(a) =$ *green, if* $a = ca'$ *for some nonzero* $c \in k$ *and some* $a' \in \mathrm{gr}(\gamma)$,

$\mathrm{col}^0_\gamma(a) =$ *red, if* $a \in \mathrm{rd}(\gamma)$,

$\mathrm{col}^0_\gamma(a) =$ *red, if* $1/a \in \mathrm{rd}(\gamma)$,

$\mathrm{col}^0_\gamma(a) =$ *red,* $a = ca'$ *for some nonzero* $c \in k$ *and some* $a' \in \mathrm{rd}(\gamma)$, *and*

$\mathrm{col}^0_\gamma(a) =$ *red,* $a = c/a'$ *for some nonzero* $c \in k$ *and some* $a' \in \mathrm{rd}(\gamma)$.

In all other cases, $\mathrm{col}^0_\gamma(a) =$ *white.*

Essentially, the coloring scheme is used to decide if, with respect to some γ, a rational function will become zero, *green*, or nonzero, *red*, upon specialization by a σ in Σ_γ. Functions that are colored *green* are effectively ignored as if they did not exist since these are the ones that will be specialized away to zero by all σ in Σ_γ. If it is not currently possible to tell by this definition whether some particular rational function will become zero or nonzero when specialized by a σ in Σ_γ, then the scheme colors this function *white*.

Given a polynomial $f = \sum a_i \cdot t_i$ in S and a condition γ, we **color** f by assigning colors to each coefficient a_i of each term of f via the coloring scheme set up by γ. We will often refer to this assignment procedure as a **direct coloring by** γ. The color of each individual term of f and that term's monomial will be the color of its coefficient. Prior to coloring we will assume that each term of f is *white*. In the sequel, we will denote the result of directly coloring a polynomial f with respect to a given condition γ by the notation, $\mathrm{col}^0_\gamma(f)$. If F is a finite set of polynomials of S, and γ is a given condition, let $\mathrm{col}^0_\gamma(F) = \{\mathrm{col}^0_\gamma(f) \mid f \in F\}$.

Example 1.1.2 Let $k = \mathbf{R}$, and

$$f = 3ux^2y + vxy^2 + wy + (2v + w)y \in k(u, v, w)[x, y].$$

Note that these subsets are well-defined since the green and red lists of a condition are disjoint. It is also possible for these sets to be empty for some conditions (see section 2.1 of Chapter 2). In words, these are sets of all possible specializations that will make the functions in the green list of a given condition zero, and all functions in the red list nonzero. Hence, we may think of each individual condition as representing such a subset of specializations. Furthermore, we may think of the green list of a condition as representing a set of rational *equalities* of the symbolic parameters, and the red list as representing a set of rational *inequalities*. So, a given condition represents a collection of specializations that will make some specified rational functions zero or nonzero.

Example 1.1.1 Let k be the field of complex numbers, $Q = k(u, v)$, and γ be the condition $\gamma = \left(\{\frac{u}{5v}\}, \{5v, v^2 + 1\}\right)$. Then

$$\Sigma_\gamma = \{\sigma : (u, v) \mapsto (a, b) \,|\, a = 0, b \neq 0, b \neq i\}.$$

Thus, Σ_γ consists of all possible specializations of the symbolic parameters u, v that make the fraction in the green list of γ zero, and make the functions in the red list nonzero. Note that if k is the real field, then Σ_γ is just the set of all specializations that make u zero and v nonzero.

We next introduce a coloring scheme for elements in Q with respect to a given condition γ. This scheme will assign to each element of Q one of the three colors *green, red*, or *white*. At first glance this scheme appears artificial, but it proves its usefulness in the precision of the algorithms to follow. We will use the notation col^0_γ to express the distinction between this definition from that found in [7]. This definition is what we shall refer to as the "assignment" aspect of colorings.

Definition 1.1.4 *Let γ be a given condition. Then a* **coloring of Q with respect to γ** *is a mapping,*

$$\mathrm{col}^0_\gamma : Q \to \{green, red, white\},$$

Thus, σ is just the evaluation map. With the above, we now define a ring homomorphism that sends a polynomial $f = \sum a_i \cdot t_i$ in S to a polynomial in $R = k[x_1, \ldots, x_n]$ by the rule $\sigma(f) = \sum \sigma(a_i) \cdot t_i$. If $G = \{f_1, \ldots, f_k\}$ is a subset of S, then denote by $\sigma(G)$ the set $\{\sigma(f_1), \ldots, \sigma(f_k)\}$.

Let Σ denote the set of all possible specializations of parameters (a large set indeed if k is an infinite field; if k is finite then Σ has r^m elements where r is the number of elements of k). To aid in classifying specializations in Σ we make the following definition.

Definition 1.1.1 *A* **condition** γ *is an ordered pair, denoted by* $\gamma = (g, r)$*, where*

i) g *and* r *are finite, possibly empty, disjoint subsets of* $Q - k$*, and*
ii) *if* $f = p/q \in g$ *or* r*, then* q *is also in* r*.*

In anticipation of the coloring scheme to be introduced and for clarity of presentation of our algorithms, we make the following definition.

Definition 1.1.2 *The set* g *of a condition* γ *is called the* **green list** *of the condition and is denoted by* $\mathrm{gr}(\gamma)$*. The set* r *of a condition is called the* **red list** *of the condition and is denoted by* $\mathrm{rd}(\gamma)$*.*

Definition 1.1.3 *A* **case distinction** *is a finite set of conditions.*

As stated above, the set Σ of all possible specializations of parameters can be quite large. But note that when we specialize any rational function in Q we get an element of k that must be either zero or nonzero. This simple observation allows us to relate conditions to sets of specializations. That is to say, we can define for each given condition γ a subset Σ_γ of specializations:

$$\Sigma_\gamma = \{\sigma \in \Sigma \,|\, \sigma(g) = 0, \forall g \in \mathrm{gr}(\gamma), \text{ and } \sigma(r) \neq 0, \forall r \in \mathrm{rd}(\gamma)\}.$$

Let $T(f)$ denote the set of terms of a polynomial f in R or S. In the sequel, we shall often find it convenient to denote elements of M by single lowercase roman letters (e.g. $s, t, \ldots$). Thus, a term of f in R, (S) will be denoted as, say, $a \cdot t$, where it is assumed that a is in k, (Q) and $t \in M$. Particular usage will be clear from the context.

Let $\leq$ be a monomial ordering on M. We will tacitly assume that if $f = \sum a_i \cdot t_i \in R$, (S) then for all indices i in the sum, $t_i \geq t_{i+1}$. That is, the terms in the summation will be written in order, from greatest to least, according to the given monomial ordering on M. Hence, we will also always assume that the set $T(f)$ is ordered in this way as well. As in [2], we define the **head term**, $\mathrm{HT}(f)$, of $f \in R, (S)$ as the term $a \cdot t \in T(f)$ with greatest monomial t. The **head coefficient**, $\mathrm{HC}(f)$, and **head monomial**, $\mathrm{HM}(f)$, of f in R are then the a and t, respectively, of $\mathrm{HT}(f)$. If $\mathrm{HT}(f) = a \cdot t = a \cdot x^\alpha$, then we define the **multidegree** of f, $\mathrm{multideg}(f) = \alpha$, and the **total degree** of f as $|\mathrm{multideg}(f)|$.

By a **specialization of parameters** we mean a choice of a field element $a_i \in k$ for each symbolic parameter u_i. We can denote such a selection by a mapping σ from U to the affine space k^m, i.e. $\sigma : \ (u_1, \ldots, u_m) \mapsto (a_1, \ldots, a_m)$. Thus we assign values to each symbolic parameter in U, $\sigma(u_i) = a_i \in k$. Each σ can be naturally extended to the ring homomorphisms, which we will also denote by σ, $\sigma : P \mapsto k$, and $\sigma : Q \mapsto k$ defined as follows: if $u^\alpha = u_1^{\alpha_1} \cdots u_m^{\alpha}$ is a monomial of parameters, then $\sigma(u^\alpha) = (\sigma(u_1))^{\alpha_1} \cdots (\sigma(u_m))^{\alpha_m} \in k$; if $a \in k$, then $\sigma(a) = a$; and

i) for $f = \sum a_\alpha \cdot u^\alpha \in P$, we have

$$\sigma(f) = \sum a_\alpha \cdot \sigma(u^\alpha) \in k, \text{ and}$$

ii) for $f = p/q \in Q$ and $\sigma(q) \in k - \{0\}$, we have

$$\sigma(f) = \frac{\sigma(p)}{\sigma(q)} \in k.$$

tation used the data structure of ordered lists for polynomials (see appendix A for details). Interfacing to the prototype was provided by either interactively running MACSYMA or through batch processing available on the Suns.

1.1 Specializations, Conditions, and Colorings

To make the construction of the Comprehensive Groebner Basis precise, we make the following definitions. Again, let k be a field. We make no initial assumptions about k. We will though need to assume later that k is algebraically closed in order to use Hilbert's Nullstellensatz. Let $U = \{u_1, \ldots, u_m\}$ be a list of symbolic parameters, and let $X = \{x_1, \ldots, x_n\}$ be a list of indeterminates. Let

$$P = k[U] = k[u_1, \ldots, u_m], Q = k(U) = k(u_1, \ldots, u_m)$$

be the ring of polynomials and field of rational functions, respectively, in the parameters of U. Also, set $R = k[X] = k[x_1, \ldots, x_n]$. We will construct Comprehensive Groebner Bases for ideals I in the ring

$$S = Q[X] = k(U)[X] = k(u_1, \ldots, u_m)[x_1, \ldots, x_n].$$

We will refer to the indeterminates in X as "main variables."

Let M be the set of all monomials of the main variables; $M = \{x^\alpha\}$ using the standard multiindex notation, $\alpha = (\alpha_1, \ldots, \alpha_n) \in Z^n_{\geq 0}$, so $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Let $|\alpha| = \sum \alpha_i$. Write the zero polynomial in both R and S as $0 \in k$. Thus we may write any nonzero polynomial f in R, (S) in the form $f = \sum_\alpha a_\alpha x^\alpha$ where each a_α is in k, (Q) and the sum is taken over a finite set of distinct mulitindicies α. We shall refer to each summand $a_\alpha x^\alpha$, for $a_\alpha \neq 0$, as a **term** of f, and a_α as the **coefficient** of the monomial x^α. For convenience, we will assume that if f is a nonzero polynomial, then, when f is written in the form $f = \sum_\alpha a_\alpha x^\alpha$, all summands are terms ($a_\alpha \neq 0$), and the α's are all distinct.

System is a finite set of pairs of the form (γ, G) where γ is a "condition" that represents a particular subset of possible specializations of parameters and G is a Groebner Basis for J under these specializations. For the simple example above, the Groebner System consists of the two pairs $(\gamma_1, G_1), (\gamma_2, G_2)$ where

$$\begin{aligned}(\gamma_1, G_1) &= ((\{\}, \{1-t\}), \{x+y, x+ty, (1-t)y\}),\\ (\gamma_2, G_2) &= ((\{1-t\}, \{\}), \{x+y, x+ty\}).\end{aligned}$$

The condition γ_1 is to be interpreted as representing all specializations of the parameter t so that $t \neq 1$. The condition γ_2 then represents the specialization that makes $1-t=0$. The Comprehensive Groebner Basis G of our example is then simply the union of the sets G_1 and G_2. Note also that these two pairs are distinguished by considerations of the S-polynomial $h = (1-t)y$ of $x+y, x+ty$. If $t=1$, then $h=0$. If $t \neq 1$, then $h \neq 0$.

The plan of this first chapter is as follows: we fix notation, and carefully describe key routines for the main algorithm. These algorithms perform all arithmetic needed for constructions in this framework. We spend a substantial amount of time amplifying the notion of "color" assignments to coefficients. We found it very useful to split this discussion into the assignment aspects (see definition 1.1.4) and arithmetic aspects (see definition 1.3.1). Along the way we also highlight relevant facts from proofs of the algorithms to demonstrate partial correctness and termination. Throughout this dissertation, all algorithms will have a section of this type of analysis.

A word about implementations. In the book by Becker and Weispfenning [1], they mention an implementation of algorithms based on [7] to generate Comprehensive Groebner Bases using MAS, the Modular -Algebra- System. We experimented with this package and found that we could test our new ideas with new code. To this end we first wrote an extensive prototype in MACSYMA and ran compiled versions of this code on a Sun Sparc 10 Workstation under Unix. Our implemen-

until the ideal stabilizes. The primary difference is that the algorithm keeps very precise track of when a coefficient function will become zero or nonzero in some specialization. That is to say, we encode in a "condition" those coefficients which correspond to specializations that would make them zero and those that would make them nonzero.

In the usual Buchberger construction of Groebner Bases, given a well-defined monomial ordering of the main variables (say, lex, or grlex, etc) it is a simple matter to determine the head term of any polynomial. In this construction, we have to be much more careful since, *when we specialize parameters, the head term may change, or may not even exist!* This leads to notions we will introduce regarding "conditional head terms", "conditional S-polynomials," and "conditional normal forms." The Buchberger criterion for us will then be that all remainders of conditional S-polys will be "zero" under certain, very precise conditions. The algorithm allows for keeping careful track of all these conditions.

For a simple example, consider the ideal

$$J = \langle x + y, x + ty \rangle \subset k(t)[x, y]$$

with k equal to the reals and $x > y$ using lex order. A Comprehensive Groebner Basis for J is

$$G = \{x + y, x + ty, (1 - t)y\}.$$

For t specialized to 1, we see that $\tilde{G} = \{x + y\}$ (where we have tacitly ignored duplicates and 0) is a Groebner Basis for the specialized ideal $\tilde{J} = \langle x + y, x + y \rangle = \langle x + y \rangle$. For t specialized to some $t_0 \neq 1$, it is not hard to show by the Buchberger criterion that $\tilde{G} = \{x + y, x + t_0 y, (1 - t_0)y\}$ is a Groebner Basis of $\tilde{J} = \langle x + y, x + t_0 y \rangle = \langle x, y \rangle$. The above set G is not in the simplest possible form. It may be reduced by the **REDUCTION** algorithm in appendix B.

In practice, Comprehensive Groebner Bases are obtained via "Groebner Systems." Briefly, for a given ideal $J \subset S$ and a monomial ordering, a Groebner

1 FOUNDATIONS FOR THE BASIC CONSTRUCTION

In this chapter we study the basic construction of Comprehensive Groebner Bases given in the paper by V. Weispfenning in [7] from the point of view of finding key areas upon which to build a new design methodology for the overall construction.

To fix ideas more precisely, let k be a field, and consider the ring

$$S = k(u_1, \ldots, u_m)[x_1, \ldots, x_n]$$

of multivariable polynomials in the "main variables" $x_1, \ldots, x_n$ whose coefficients are rational functions of the "symbolic parameters" $u_1, \ldots, u_m$ with coefficients in k. Let

$$J = \langle f_1(u_1, \ldots, u_m, x_1, \ldots, x_n), \ldots, f_s(u_1, \ldots, u_m, x_1, \ldots, x_n) \rangle$$

be an ideal in S. By a *specialization of parameters* we mean a choice of substituting a particular element a_i of k for each symbolic parameter u_i. Once such a choice has been made we have then that

$$\tilde{J} = \langle f_1(a_1, \ldots, a_m, x_1, \ldots, x_n), \ldots, f_s(a_1, \ldots, a_m, x_1, \ldots, x_n) \rangle$$

is an ideal in $k[x_1, \ldots, x_n]$. The primary feature of a Comprehensive Groebner Basis $G \subset J$ is the following.

Advantage 1 *If G is a Groebner Basis of an ideal J of S, then for ANY specialization of the parameters, the specialized set $\tilde{G}$ is still a Groebner Basis for the specialized ideal $\tilde{J}$ in $k[x_1, \ldots, x_n]$.*

The primary idea of the main algorithm **GROEBNERSYSTEM** of this chapter (see table 1.6) is to follow the usual Buchberger construction for Groebner Bases, i.e. adding nonzero remainders of S-polynomials of pairs of polynomials

the way we make use of the theory of saturations of ideals. In Chapter 3, we show the precision of our new design in examples from several areas of commutative algebra. We demonstrate the simplicity that may be attained in examples from Automatic Geometric Theorem Proving, and in the study of parametric varieties. Also, we embed our new design in an algorithm that has potential use in the study of dimension bounds of parametric vareties.

ALGORITHMS AND APPLICATIONS OF COMPREHENSIVE GROEBNER BASES

Will-Matthis Dunn, III, Ph. D.

The University of Arizona, 1 9 9 5

Director: Marek R. Rychlik

In this dissertation we study several improvements to algorithms used to generate Comprehensive Groebner Bases of Volker Weispfenning [7]. Comprehensive Groebner Bases are bases for ideals in the ring of polynomials in several variables whose coefficients are polynomials in several symbolic parameters over a given field. These bases have the fundamental property that, for any possible assignment (specialization) of the field elements for the parameters, the Comprehensive Groebner Basis generators become generators for a usual Groebner Basis for the ideal of polynomials with coefficients in the field. Chapter 1 gives the necessary background for understanding the basic construction of Comprehensive Groebner Bases. We show how it is also possible to construct these bases for ideals in the ring of polynomials whose coefficients are rational functions of the symbolic parameters. We amplify the description of assigning "colors" to coefficients as given in [7]. These assignments are used to establish criteria to determine the effect specialization will bear upon a given coefficient of a given polynomial. We also amplify the constructions for S-polynomial and Normal Form computations in this realm. In Chapter 2, we present several modifications to the algorithms in Chapter 1. These modifications allow for more efficient machine computations and yield simpler output. We show a new design methodology for assignments of "colors" that allows for more readable and useful output. This design philosophy also allows for sharper precision when working with Comprehensive Groebner Bases. Along

ABSTRACT

In this dissertation we study several improvements to algorithms used to generate Comprehensive Groebner Bases of Volker Weispfenning [7]. Comprehensive Groebner Bases are bases for ideals in the ring of polynomials in several variables whose coefficients are polynomials in several symbolic parameters over a given field. These bases have the fundamental property that, for any possible assignment (specialization) of the field elements for the parameters, the Comprehensive Groebner Basis generators become generators for a usual Groebner Basis for the ideal of polynomials with coefficients in the field. Chapter 1 gives the necessary background for understanding the basic construction of Comprehensive Groebner Bases. We show how it is also possible to construct these bases for ideals in the ring of polynomials whose coefficients are rational functions of the symbolic parameters. We amplify the description of assigning "colors" to coefficients as given in [7]. These assignments are used to establish criteria to determine the effect specialization will bear upon a given coefficient of a given polynomial. We also amplify the constructions for S-polynomial and Normal Form computations in this realm. In Chapter 2, we present several modifications to the algorithms in Chapter 1. These modifications allow for more efficient machine computations and yield simpler output. We show a new design methodology for assignments of "colors" that allows for more readable and useful output. This design philosophy also allows for sharper precision when working with Comprehensive Groebner Bases. Along the way we make use of the theory of saturations of ideals. In Chapter 3, we show the precision of our new design in examples from several areas of commutative algebra. We demonstrate the simplicity that may be attained in examples from Automatic Geometric Theorem Proving, and in the study of parametric varieties. Also, we embed our new design in an algorithm that has potential use in the study of dimension bounds of parametric vareties.

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

DEDICATION

This dissertation is dedicated to the the author's grandfather

Rev. Lowell Oscar Ryan

and grandmother

Margaret Erla Rudd Dunn,

and the fond memory of their respective spouses

Herberta June Bissell Ryan

and

Rev. Will-Matthis Dunn, Sr., Ph. D.

ACKNOWLEDGMENTS

I take this page to express my sincerest thanks and gratitude to my advisor, Professor M. R. Rychlik, for everything he has taught me these past six years and during the time of our collaborative researches and preparation of this dissertation. I have learned an incredible amount from Dr. Rychlik in mathematics and computer operations. I am honored to have been one of his graduate students.

My thanks also to Professors H. Groemer, P. Fan, H. Rund, N. Ercolani, J. Cushing, for teaching in my graduate coursework; and to Professors D. Madden, W. McCallum, D. Hughes-Hallet, D. Lovelock, and D. Lomen for teaching me to teach.

Additional thanks to Robert Condon, and his industrious group of computer aides: James Abolt, Steve Uurtamo, Ricardo Martinez, Peter Miller and Mark Hays. And finally, all my love to my wife, Melinda, for all her love, care and encouragement throughout this long journey.

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the library.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED:_____

Get the official approval page from **The Graduate College** before your final defense

ALGORITHMS AND APPLICATIONS OF COMPREHENSIVE GROEBNER BASES

by

Will-Matthis Dunn, III

A Dissertation Submitted to the Faculty of the

DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements
For the Degree of

DOCTOR OF PHILOSOPHY

In the Graduate College

THE UNIVERSITY OF ARIZONA

1 9 9 5