Part 4: Gröbner Basics

Tim Duff

February 14, 2025

In general, we are interested in solving problems of the following form

$$f_1(\mathbf{x};\mathbf{p}) = f_2(\mathbf{x};\mathbf{p}) = \cdots = f_s(\mathbf{x};\mathbf{p}) = 0,$$

where $\mathbf{x} \in \mathbb{C}^n$ are *unknowns*, or *variables*, $\mathbf{p} \in \mathbb{C}^m$ are *given data* or *parameters*, and $f_1, \ldots, f_s$ are equations are polynomial functions[1] of $\mathbf{x}$ and $\mathbf{p}$. Here is a simple example with $n > 1$.

Example 1. For rectangle with length x_1 and width x_2, we can easily compute the area p_1 and the perimeter p_2. The *inverse problem* asks: given $\mathbf{p} = (p_1, p_2) \in \mathbb{R}^2$, can we recover $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$ satisfying

$$\begin{aligned} f_1(\mathbf{x};\mathbf{p}) &= 2(x_1 + x_2) - p_1 = 0, \\ f_2(\mathbf{x};\mathbf{p}) &= x_1 x_2 - p_2 = 0. \end{aligned} \tag{1}$$

To eliminate variables "by hand", we can try to work with various "polynomial consequences of eq. (1). For instance, if $g_1, g_2 \in \mathbb{C}[\mathbf{x}]$ are *arbitrary* polynomials in the unknowns, these equations also imply that

$$g_1(\mathbf{x}) \cdot f_1(\mathbf{x};\mathbf{p}) + g_2(\mathbf{x}) \cdot f_2(\mathbf{x};\mathbf{p}) = 0.$$

A fortuitous choice is given by $(g_1, g_2) = (x_2, -2)$, from which we obtain

$$2x_2^2 - p_1 x_2 + 2p_2 = 0.$$

The roots of this univariate polynomial can be computed in radicals:

$$x_2 = \frac{p_1 \pm \sqrt{p_1^2 - 16p_2}}{4} = 2 \text{ or } 3,$$

from which we also easily obtain, using the equation for perimeter,

$$x_1 = p_1/2 - x_1 = \frac{p_1 \mp \sqrt{p_1^2 - 16p_2}}{4} = 3 \text{ or } 2.$$

Our search for "polynomial consequences" in the previous example motivates the following definition.

Definition 0.1. Let $\mathbb{K}$ be a field, and $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$ be the polynomial ring over $\mathbb{K}$ in n indeterminates. For fixed $f_1, \ldots, f_s \in \mathbb{K}[\mathbf{x}]$, the *ideal generated* by these polynomials is the set

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} g_i f_i \mid g_1, \ldots, g_s \in \mathbb{K}[\mathbf{x}] \right\}.$$

Hilbert's basis theorem states that every polynomial ideal has the form given in Definition 0.1. In hopes of reducing multivariate polynomial system solving to univariate polynomial system solving, we pose the *elimination problem*: for a given ideal $\langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[\mathbf{x}]$, how can we compute generators for the ideal $\langle f_1, \ldots, f_s \rangle \cap \mathbb{K}[x_2, \ldots, x_n]$? We will show how a complete solution to this problem can be obtained by computing a Gröbner basis with respect to a *lexicographic order* (Definition 0.3.)

In addition to the elimination problem, we also consider the *ideal membership problem*: for given $f, f_1, \ldots, f_s \in \mathbb{K}[\mathbf{x}]$, can we decide whether or not $f \in \langle f_1, \ldots, f_s \rangle$? In the *univariate case* $n = 1$, it is easy to solve this problem using the *division algorithm.*

[1] Or perhaps even rational/algebraic functions

Example 2. Let $g = \underline{x^2} - 1$, and consider the ideal $I = \langle g \rangle$. We use the division algorithm to show that $f = \underline{x^4} + x^3 - x - 1 \in I$. Note that we have underlined the terms of highest degree. Anticipating the multivariate case, we write $\mathrm{LT}(g) = x^2$ and $\mathrm{LT}(f) = x^4$ to denote the *leading term* of f and g. The condition $f \in I$ is the same as saying $f \equiv 0 \mod I$, or, since I principal, that I is a polynomial multiple of g. The division algorithm proceeds as follows:

$$\begin{aligned}
\underline{x^4} + x^3 - x - 1 &= x^2 \cdot \mathrm{LT}(g) + x^3 - x - 1 \\
&= x^2 \cdot \left(g + \underbrace{(\mathrm{LT}(g) - g)}_{1} \right) + x^3 - x - 1 \\
&\equiv x^2 + x^3 - x - 1 \mod I \\
&= \underline{x^3} + x^2 - x - 1 \\
&= x \cdot (x^2 - 1) + x + x^2 - x - 1 \\
&\equiv \underline{x^2} - 1 \mod I \\
&\equiv 0 \mod I.
\end{aligned}$$

There are several obstacles to adapting polynomial division to the *multivariate case* $n > 1$. One obstacle is that most ideals are not principal. Another obstacle is that the concept of a leading term does not extend uniquely. Indeed, the usual ordering of monomials when $n = 1$,

$$1 < x < x^2 < x^3 < \cdots$$

has a number of properties that are easy to take for granted. These properties are crystalized in the following definition. Recall that a *monomial* in $\mathbb{K}[x_1, \ldots, x_n]$ is a polynomial with exactly one term whose coefficient equsls $1_{\mathbb{K}}$. A monomial $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \cdots \cdot x_n^{\alpha_n}$ may be written more compactly in *multi-index notation* as $\mathbf{x}^{\boldsymbol{\alpha}}$, where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ is a lattice point in the positive orthant of $\mathbb{R}^n$. For visualization purposes, it is standard to identity monomials and lattice points (especially when $n = 2$ or 3.)

Definition 0.2. A *monomial order* is any total, multiplicative order $<$ on the set of monomials in $\mathbb{K}[x_1, \ldots, x_n]$ such that 1 is the minimum element.

Exercise 1. There is a unique monomial order on the univariate polynomial ring $\mathbb{K}[x]$.

Though they may seem unmotivated at first, it is worthwhile to build up a repertoire of several different monomial orders. For now, we define two classes of monomials orders that are easy to understand, though not always the most useful.

Definition 0.3. The *lexicographical order* with $x_1 > x_2 > \cdots > x_{n-1} > x_n$, denoted in Macaulay2 by `Lex`, is defined as follows:

$$\mathbf{x}^{\boldsymbol{\alpha}} > \mathbf{x}^{\boldsymbol{\beta}} \quad \Leftrightarrow \quad \boldsymbol{\alpha} - \boldsymbol{\beta} = (0, 0, \ldots, 0, \underbrace{\alpha_i - \beta_i}_{>0}, \ldots).$$

Definition 0.4. The *graded lexicographical order* with $x_1 > x_2 > \cdots > x_{n-1} > x_n$, denoted in Macaulay2 by `GLex`, is defined as follows:

$$\begin{aligned}
\mathbf{x}^{\boldsymbol{\alpha}} > \mathbf{x}^{\boldsymbol{\beta}} \quad \Leftrightarrow \quad & \sum_{i=1}^{n} (\alpha_i - \beta_i) > 0, \quad \textbf{OR} \\
& \sum_{i=1}^{n} (\alpha_i - \beta_i) = 0, \quad \mathbf{x}^{\boldsymbol{\alpha}} >_{\texttt{Lex}} \mathbf{x}^{\boldsymbol{\beta}}.
\end{aligned}$$

In more plain language, `Lex` compares monomials as though they were words in a dictionary, whereas `GLex` compares monomials based on their total degree, breaking any ties with `Lex` as needed. Note that both orders depend on the chosen ordering of the variables: in other words, Definitions 0.3 and 0.4 describe a total of $2n!$ monomial orders on $\mathbb{K}[x_1, \ldots, x_n]$.

An important property of monomial orders is that they are all *well orders*; that is, given $<$ as in Definition 0.2, any nonempty set of monomials has a smallest element with respect to $<$. This can proved using the following special case of Hilbert's basis theorem.

Lemma 0.5 (Gordan's Lemma)**.** Every monomial ideal is finitely generated by monomials. That is, if $I \subset \mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \dots, x_n]$ is an ideal such that every element of I has the form

$$g_1\mathbf{x}^{\boldsymbol{\alpha}_1} + \cdots + g_s\mathbf{x}^{\boldsymbol{\alpha}_s} \quad \text{w/} \quad \mathbf{x}^{\boldsymbol{\alpha}_1}, \dots, \mathbf{x}^{\boldsymbol{\alpha}_s} \in I, \tag{2}$$

then $I = \langle \mathbf{x}^{\boldsymbol{\beta}_1}, \dots, \mathbf{x}^{\boldsymbol{\beta}_k} \rangle$ for some finite subset $\{\mathbf{x}^{\boldsymbol{\beta}_1}, \dots, \mathbf{x}^{\boldsymbol{\beta}_k}\} \subset I$.

Remark: Lemma 0.5 is sometimes called "Dickson's Lemma", despite the fact that Gordan proved it well before Dickson did.

Proof. Induction on n. If $n = 1$, then I is a principal ideal. Writing $I = \langle p \rangle$, then writing p in the form 2 shows that p is divisible by some $x^k \in I$, so the chain of inclusions

$$\langle x^k \rangle \subset I = \langle p \rangle \subset \langle x^k \rangle$$

shows that $I = \langle x^k \rangle$ is finitely generated by a single monomial.

For $n > 1$, assume the result for all smaller n. Define for each $j \in \mathbb{Z}_{\geq 0}$ the monomial ideal

$$I_j = \langle x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} \mid x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} x_n^j \in I \rangle.$$

By inductive hypothesis, each I_j is finitely generated by monomials. Moreover, since we have an ascending chain $I_0 \subset I_1 \subset I_2 \subset \cdots$, the union $\cup_{k \geq 0} I_k$ is also an ideal that is finitely generated by monomials. This implies that the ascending chain eventually stabilizes: that is, there exists some r such that $I_r = I_{r+k}$ for all $k \geq 0$. It follows that $\mathbf{x}^{\boldsymbol{\alpha}} \in I$ iff $x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} \in I_r$. If $B_0, \dots, B_r$ are monomial generating sets for $I_0, \dots, I_r$, then it follows that

$$I = \langle B_0 \sqcup x_n B_1 \sqcup x_n^2 B_2 \sqcup \cdots \sqcup x_n^r B_r \rangle,$$

since monomial in I (and consequently, also every polynomial in I) belongs to the ideal on the right. □

Corollary 0.6. Every monomial order is a well-order.

Proof. Let $S = \{\mathbf{x}^{\boldsymbol{\alpha}_i} \mid i \in I\}$ be a nonempty set of monomials. We need to show that S has a minimum element with respect to any fixed monomial order $<$. If not, we could construct an infinite descending chain of elements in S,

$$\mathbf{x}^{\alpha_1} > \mathbf{x}^{\alpha_2} > \mathbf{x}^{\alpha_3} > \dots$$

However, Gordan's lemma implies that this chain must eventually stabilize at in particular, for some i

$$\langle \mathbf{x}^{\alpha_1}, \dots\dots, \mathbf{x}^{\alpha_k} \rangle = \langle \mathbf{x}^{\alpha_1}, \dots\dots, \mathbf{x}^{\alpha_k}, \mathbf{x}^{\alpha_{k+1}} \rangle,$$

in which case for some $i \in \{1, \dots, k\}$, $\gamma \in \mathbb{Z}^n_{\geq 0}$, we have

$$\mathbf{x}^{\alpha_{k+1}} = \mathbf{x}^{\alpha_i + \gamma} \geq \mathbf{x}^{\alpha_i},$$

a contradiction. □

For any fixed monomial order $<$ on $\mathbb{K}[\mathbf{x}]$ and any nonzero polynomial $f \in \mathbb{K}[x]$, we may write

$$f = c_1\mathbf{x}^{\boldsymbol{\alpha}_1} + c_2\mathbf{x}^{\boldsymbol{\alpha}_2} + \cdots + c_k\mathbf{x}^{\boldsymbol{\alpha}_k}$$

with its coefficients in sorted order, i.e.

$$\mathbf{x}^{\boldsymbol{\alpha}_k} < \cdots < \mathbf{x}^{\boldsymbol{\alpha}_2} < \mathbf{x}^{\boldsymbol{\alpha}_1}.$$

The leading term/coefficient/monomial of f with respect to $<$ are then defined as follows:

$$\begin{aligned} \mathrm{LT}_<(f) &= c_1 x^{\boldsymbol{\alpha}_1}, \\ \mathrm{LC}_<(f) &= c_1, \\ \mathrm{LM}_<(f) &= x^{\boldsymbol{\alpha}_1}. \end{aligned}$$

When $f = 0$, those notions are left undefined. When $\mathrm{LC}_<(f) = 1$, we say f is *monic* with respect to $<$.

Emulating the pattern of Example 2, let us try to solve the ideal membership problem on an example, using some of the monomial orders introduced so far.

Example 3. Consider the Lex order on $\mathbb{Q}[x, y, z]$ with $x < y < z$, and let

$$\begin{aligned} f &= \underline{z^2} - y \\ f_1 &= \underline{y} - x, \\ f_2 &= \underline{z^2} - x. \end{aligned}$$

We would like to decide the ideal membership query

$$f \in I = \langle f_1, f_2 \rangle?$$

We begin by trying to divide $\mathrm{LT}_<(f)$ by $\mathrm{LT}_<(f_1)$ or $\mathrm{LT}_<(f_2)$—if that succeeds, then we can write

$$f = \mathbf{x}^{\boldsymbol{\alpha}} \cdot f_i + \tilde{f}$$

for some $\tilde{f}$ with strictly smaller leading monomial: $\mathrm{LM}_<(\tilde{f}) < \mathrm{LM}_<(f)$. Applying the same procedure with $\tilde{f}$ in place of f, we obtain the following sequence of operations:

$$\begin{aligned} f &= \underline{z^2} - y \\ &= \underbrace{(z^2 - x)}_{f_2} + x - y \\ &\equiv \underline{-y} + x \mod I \\ &= -f_1 \\ &\equiv 0 \mod I. \end{aligned}$$

This calculation produces a certificate of ideal membership in the form of the multipliers $(g_1, g_2) = (1, -1)$ appearing in Definition 0.1:

$$f = 1 \cdot f_1 + (-1) \cdot f_2 \in I.$$

Now suppose instead that we chose the Lex order with the order of variables reversed: $x > y > z$. Our ideal-membership query is the same (up to sign) as before), but we have different leading terms:

$$\underline{y} - z^2 \in I = \langle \underline{x} - y, \, \underline{x} - z^2 \rangle?$$

Applying the same algorithm as before, we see that $\mathrm{LT}_<(f)$ is not divisible by $\mathrm{LT}_<(f_1)$ or $\mathrm{LT}_<(f_2)$, so we do not succeed in our strategy of rewriting f as an element of I. Notice how, in the previous case, the leading monomials $\mathrm{LM}(f_1), \mathrm{LM}(f_2)$ function like "pivots" in the familiar algorithm of Gaussian elimination. When we change the monomial order in this example, the number of these "pivots" drops from 2 to 1! Fortunately, this is not a deficiency of the monomial order, but rather of the *generating set* used to represent I. Indeed, if we were to discover independently that $f \in I$, we could add it to our set of generators for I, thus obtaining a new leading term $\underline{y^2}$. The definition of a Gröbner basis captures in precise terms when a generating set of an ideal has "enough" leading terms to make the division algorithm work.

Definition 0.7. Fix a monomial order $<$ on $\mathbb{K}[\mathbf{x}]$, and let $I \subset \mathbb{K}[\mathbf{x}]$ be an ideal. The *initial ideal* of I with respect to $<$ is defined as follows:

$$\mathrm{in}_<(I) = \langle \mathrm{LM}_<(f) \mid f \in I \rangle. \tag{3}$$

A *Gröbner basis* $G = \{g_1, \ldots, g_s\} \subset I$ with respect to $<$ is a finite subset of I whose leading monomials generate the initial ideal: $\mathrm{in}_<(I) = \langle \mathrm{LM}_<(g_1), \ldots, \mathrm{LM}_<(g_s) \rangle$.

Example 4. Continuing with Example 3, consider the following Macaulay2 session:

```
i1 : R = QQ[z,y,x];
i2 : f = z^2 - y;
i3 : f1 = y-x;
i4 : f2 = z^2 - x;
i5 : I = ideal(f1, f2);
o5 : Ideal of R
i6 : G = gb I
o6 = GroebnerBasis[status: done; S-pairs encountered up to degree 1]
o6 : GroebnerBasis
i7 : gens G
o7 = | y-x z2-x |
```

It seems that $\{f_1, f_2\}$ is a Gröbner basis for I, but with respect to which monomial order? The following comparisons rule out the possibility of Lex or GLex.

```
i8 : y < z
o8 = true
i9 : x < y -- so z > y > x
o9 = true
i10 : x^2 < y -- not Lex!
o10 = false
i11 : y^2 < z*x -- not GLex!
o11 = false
```

As it turns out, any object of class PolynomialRing such as R in this example represents not just a polynomial ring, but a polynomial ring together with several pieces of satellite data, including a monomial order. The mystery monomial order, used by default in Macaulay2, is revealed to be GRevLex.

```
i12 : describe R
o12 = QQ[z, y, x, Degrees => {3:1}, Heft => {1},
MonomialOrder => {MonomialSize => 32}, DegreeRank => 1]
                 {GRevLex => {3:1}  }
                 {Position => Up    }
```

Definition 0.8. The *graded reverse lexicographical order* with $x_1 > x_2 > \cdots > x_{n-1} > x_n$, denoted in Macaulay2 by GRevLex, is defined as follows:

$$\mathbf{x}^{\boldsymbol{\alpha}} > \mathbf{x}^{\boldsymbol{\beta}} \quad \Leftrightarrow \quad \sum_{i=1}^{n}(\alpha_i - \beta_i) > 0, \quad \textbf{OR}$$

$$\sum_{i=1}^{n}(\alpha_i - \beta_i) = 0, \quad \boldsymbol{\alpha} - \boldsymbol{\beta} = (\ldots, \underbrace{\alpha_i - \beta_i}_{<0}, \ldots, 0)$$

Thus GRevLex first compares monomials by total degree, then breaks ties by picking the greater monomial to be the one with the *smaller* power of x_n, then breaking further ties using x_{n-1}, and so on.

To compute Gröbner bases using the Lex orders considered originally in Example 3, we must specify these orders manually:

```
i8 : S = newRing(R, MonomialOrder => Lex);
i9 : gens gb sub(I, S)
o9 = | y-x z2-x |

              1       2
o9 : Matrix S  <--- S
i10 : T = QQ[reverse gens R, MonomialOrder => Lex];
i11 : gens gb sub(I, T)
o11 = | y-z2 x-z2 |

               1       2
o11 : Matrix T  <--- T
```

Before explaining how to compute Gröbner bases in the next section, we will show that they lead to a simple, constructive proof of Hilbert's basis theorem, and that they enable us to solve both the ideal membership problem and the elimination problem. To begin, we observe that a Gröbner basis, *a priori* only a subset of some ideal, is in fact a generating set for that ideal.

Proposition 0.9. Let G be a Gröbner basis for I. Then G generates I.

Proof. Suppose not—then, since $\langle G\rangle \subsetneq I$, there exists a polynomial $f \in I \setminus \langle G\rangle$. Appealing to Corollary 0.6, we may choose such an f with $\mathrm{LM}_<(f)$ minimal. Then, since G is a Gröbner basis, we have $\mathrm{LT}_<(f) = cm\,\mathrm{LT}_<(g)$ for some $g \in G$, $c \in \mathbb{K}$ and monomial m. If we set $\tilde{f} = f - cmg$, then we have $\tilde{f} \in I$ and $\mathrm{LM}_<(\tilde{f}) < \mathrm{LM}_<(f)$, contradicting the minimality of f. □

Proposition 0.9 leads directly to a cornerstone result in commutative algebra.

Theorem 1 (Hilbert's Basis Theorem)**.** Every ideal in $\mathbb{K}[\mathbf{x}]$ is finitely generated.

Proof. Let $I \subset \mathbb{K}[\mathbf{x}]$ be any ideal. Gordan's lemma (Lemma 0.5) implies that I has a Gröbner basis $G = \{g_1, \ldots, g_s\}$. Thus $I = \langle g_1, \ldots, g_s \rangle$ by Proposition 0.9. □

Exercise 2. Show that every ascending chain of ideals in $\mathbb{K}[\mathbf{x}]$ stabilizes. That is, if we have ideals $I_1, I_2, \ldots$ in this ring with

$$I_1 \subset I_2 \subset \cdots,$$

then there exists some $n \in \mathbb{Z}_{\geq 0}$ such that for all $m \in \mathbb{Z}_{\geq 0}$ we have $I_n = I_{n+m}$.

An important property of the univariate division algorithm is that the remainder and quotient representation are *unique.* The next example illustrates some subtleties in the multivariate case.

Example 5. As in Example 3, let $I = \langle \underline{x} - y, \underline{x} - z^2 \rangle$, with the `Lex` $x > y > z$ order. Division of $f = x$ by the given generators depends on how they are ordered: we could get a "remainder" of y or z^2, depending on the order in which we test the divisibility of $\mathrm{LM}_<(f)$ by the leading monomials of the generators.

Thus, in general, the quotient and remainder when we try to divide a polynomial by a generating set of an ideal are not unique. However, no such ambiguity can arise when the generators form a Gröbner basis.

Proposition 0.10. Fix a monomial order $<$ and an ideal $I \subset \mathbb{K}[\mathbf{x}]$. Then any $f \in \mathbb{K}[\mathbf{x}]$ has a unique *normal form* $\mathrm{NF}_{I,<}(f) \in \mathbb{K}[\mathbf{x}]$ such that $f - \mathrm{NF}_{I,<}(f) \in I$ and no monomial of $\mathrm{NF}_{I,<}(f)$ is contained in $\mathrm{in}_<(I)$.

The monomials not contained in $\mathrm{in}_<(I)$ are called the *standard monomials* for I with respect to $<$.

Proof. For the existence statement, let G be a Gröbner basis for I. For any polynomial f, we can run the naive division algorithm, first rewriting any term of f that is divisible by $\mathrm{in}_<(g)$ for some $g \in G$. This terminates in finitely many steps by Gordan's lemma, and we are left with a remainder which is either 0 or whose leading monomial is standard. Continuing in this way for any non-leading terms in f, we obtain a remainder r which is either 0 or such that *all* monomials in r are standard.

For uniqueness, suppose r, r' are both such that $f - r, f - r' \in I$ and r, r' are in the span of standard monomials. This implies $r - r' \in I$ is also in the span of the standard monomials. We cannot have $r \neq r'$, since this would imply that $\mathrm{LM}_<(r - r') \in \mathrm{in}_<(I)$ is standard. □

Example 6. Let $I \subset S = \mathbb{Q}[r_{11} \ldots r_{33}]$ be the ideal defining all 3×3 orthogonal matrices: that is,

$$R = \begin{pmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{pmatrix} \quad , \quad I = \langle f_1, \ldots, f_9 \rangle = \langle \text{entries of } RR^T - I_{3\times 3} \rangle.$$

For any monomial order, the normal form of $f = (\det R)^2$ is 1. This can be computed using the operator `%`.

```
i1 : S = QQ[r_(1,1)..r_(3,3)];
i2 : R = genericMatrix(S,3,3);

                3       3
o2 : Matrix S  <--- S
i3 : I = ideal(R * transpose R - id_(S^3));
o3 : Ideal of S
i4 : f = (det R)^2;
i5 : f % I
o5 = 1
o5 : S
```

Similarly, you can use the operator `//` find coefficients $h_1, \ldots, h_9 \in S$ expressing $f = \displaystyle\sum_{i=1}^{9} h_i f_i + 1$.

```
MEMBERSHIP $(f, I)$

  1. Compute a Gröbner basis $G$ for $I$ wrt. some monomial order $<$,
  2. Let $r = \mathrm{NF}_{I,<}(f)$, computed using the division algorithm and $G$ from the first step.
  3. Output YES if $r = 0$ and NO otherwise.
```

Figure 1: An algorithm for deciding ideal membership $f \in I$.

Exercise 3. Show that the mapping from $\mathbb{K}[\mathbf{x}]$ into itself that associates a polynomial with its normal form is $\mathbb{K}$-linear. Can you describe its image and kernel?

The normal form furnishes a simple algorithm that solves the ideal membership problem. This algorithm is described in Figure 1. Its correctness follows from Proposition 0.10. To make it effective, all that we need is a procedure for computing the Gröbner basis G in step 1. This can be done using *Buchberger's algorithm*, given in Figure 2.

It is important to note that Gröbner bases are not unique: indeed, if G is a Gröbner basis for I, we can add in more polynomials in I and still have a Gröbner basis. However, if and when we need uniqueness, we may appeal to the notion of a *reduced* Gröbner basis.

Definition 0.11. We say a Gröbner basis G is *reduced* if every element of $g \in G$ is monic, all non-leading monomials of g are standard, and the set $\{\mathrm{LM}_<(g) \mid g \in G\}$ minimally generates $\mathrm{in}_<(I)$: that is, no proper subset of the leading monomials generates $\mathrm{in}_<(I)$.

Proposition 0.12. For any ideal $I \subset \mathbb{K}[\mathbf{x}]$ and monomial order $<$, there exists a unique reduced Gröbner basis for I with respect to $<$.

Proof. To get a reduced Gröbner basis from an arbitrary Gröbner basis G, replace every polynomial in G with its normal form and remove any normal forms that equal zero. For uniqueness, suppose G and G' are two reduced Gröbner bases for I. Then for any $g \in G$ there exists a $g' \in G'$ such that $\mathrm{LT}_<(g) = \mathrm{LT}_<(g')$, and reducedness implies that $g - g'$ is its own normal form. On the other hand, $g - g' \in I$, so we must have $g = g'$. □

The commands `gb` and `groebnerBasis` produce "almost-reduced" Gröbner bases in the sense that the generators might not be monic, but the other conditions of Definition 0.11 are satisfied.

Finally, we address the elimination problem. As it turns out, there is a wide class of *elimination orders* that can be useful for this task. In what follows, we consider polynomial rings in which the variables form two "groups." Generalizing to the case of more than two groups is straightforward.

Definition 0.13. Consider a polynomial ring $\mathbb{K}[\mathbf{x}, \mathbf{y}] = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. We say that $<$ is an *elimination order* with $\mathbf{x} > \mathbf{y}$ if every variable from $\mathbf{x}$ is greater than all monomials in $\mathbf{y}$ alone.

It may help to think as variables in the group $\mathbf{x}$ as being "expensive" and variables in $\mathbf{y}$ as being "cheap". The normal form maps defined by an elimination order try to rewrite "expensive" monomials in terms of "cheap" ones. For example, the `Lex` order on $\mathbb{K}[x_1, \ldots, x_n]$ with $x_1 > \cdots > x_n$ is an elimination order with respect to the grouping $\mathbf{x} = \{x_1\}$, $\mathbf{y} = \{x_2, \ldots, x_n\}$. For the singleton grouping $\mathbf{x}_1 = \{x_1\}, \ldots, \mathbf{x}_n = \{x_n\}$, this `Lex` is also an elimination order with $\mathbf{x}_1 > \cdots > \mathbf{x}_n$.

Theorem 2. Let $I \subset \mathbb{K}[\mathbf{x}, \mathbf{y}]$ be an ideal and $<$ an elimination order with $\mathbf{x} > \mathbf{y}$. Suppose G is a Gröbner basis for I with respect to $<$. Then $G_{\mathbf{y}} = G \cap \mathbb{K}[\mathbf{y}]$ is a Gröbner basis for the elimination ideal $I_{\mathbf{y}} = I \cap \mathbb{K}[\mathbf{y}]$. Moreover, if G is reduced, then $G_{\mathbf{y}}$ is also reduced.

Proof. If $f \in I_{\mathbf{y}}$, then $\mathrm{LM}_<(f)$ must be by divisible $\mathrm{LM}_<(g)$ for some $g \in G$. Since $\mathrm{LM}_<(f) \in \mathbb{C}[\mathbf{y}]$, we must have $\mathrm{LM}_<(g) \in \mathbb{C}[\mathbf{y}]$ as well. The fact that $<$ is an elimination order then implies that $g \in \mathbb{C}[\mathbf{y}]$. Thus, for the order on $\mathbb{C}[\mathbf{y}]$ induced by $<$, we see that $G_{\mathbf{y}}$ is a Gröbner basis. When G is reduced, reducedness of $G_{\mathbf{y}}$ follows straightforwardly from Definition 0.11. □

Example 7. If we want to know all polynomial relations on the set of 2×2 minors of the $2 \times n$ matrix

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ x_{21} & \cdots & x_{2n} \end{pmatrix},$$

```
BUCHBERGER $(I, <)$:
  1. Initialize:
      1. A set of unprocessed $S$-pairs, S-pairs $= \{(f_1, f_2), \ldots, (f_{s-1}, f_s\})$
      2. A partial Gröbner basis, $G = \{f_1, \ldots, f_s\}$
  2. while $\exists$ an unprocessed $S$-pair, $(f, p) \in$ S-pairs:
      i. $h \leftarrow S_{f,p}$
      ii. while $\exists g \in G$, terms $t, t_h$ w/ $t_h$ a term of $h$ and $t_h = t \cdot \mathrm{LT}_<(g)$:
          update $h \leftarrow h - t \cdot g$
      iii if $h \neq 0$
          update $G \leftarrow G \cup \{h\}$
          update unprocessed S-pairs, S-pairs $=$ (S-pairs $\setminus \{(f, p)\}) \cup \{(g, h) \mid g \in G\}$
  3. Output $G$
```

Figure 2: Buchberger's algorithm for computing a Gröbner basis of an ideal $I = \langle f_1, \ldots, f_s \rangle$ in a polynomial ring $\mathbb{K}[\mathbf{x}]$ with respect to a monomial order $<$.

we should first form an ideal with $\binom{n}{2}$ generators in a ring with $2n + \binom{n}{2}$ variables, namely

$$I = \langle y_S - \det(X_S) \mid S \subset [n],\ \#S = 2 \rangle \subset \mathbb{Q}[\mathbf{x}, \mathbf{y}],$$

and then compute the elimination ideal for an appropriate elimination order. The code below does exactly this for $n = 9$ using one of the so-called *block* or *product* orders. This is a monomial order that compares monomials using GRevLex in the variables $\mathbf{x}$ first and then breaks ties using GRevLex in the variables in $\mathbf{y}$. We see that the reduced Gröbner basis G for I has 330 elements. For the elimination ideal $I_{\mathbf{y}}$, we have a reduced Gröbner basis $G_{\mathbf{y}}$ of cardinality 126. What happens if you use Lex instead?

```
n = 9
R = QQ[x_(1,1)..x_(2,n), apply(subsets(n,2), S -> y_S), MonomialOrder => Eliminate(2*n)]
X = transpose genericMatrix(R,n,2)
I = ideal apply(subsets(n,2), S -> y_S - det X_S)
elapsedTime G = gens gb I;
```

Suppose we are given a polynomial ideal specified by a finite set of generators: $I = \langle f_1, \ldots, f_s \rangle$. We would like to compute a Gröbner basis for I with respect to a particular monomial order $<$. In particular, this will allow us to determine whether or not the original generators form a Gröbner basis. To make progress towards computing a Gröbner basis, we need to generate leading terms that aren't already in the ideal $< \mathrm{in}_<(f_1), \ldots, \mathrm{in}_<(f_s) \rangle$. One way to do this is to take a pair (f_i, f_j) and cancel leading terms by producing the following element of I:

$$S_{f_i, f_j} = \frac{\mathrm{lcm}(\mathrm{LM}_<(f_i), \mathrm{LM}_<(f_j))}{\mathrm{LT}_<(f_i)} \cdot f_i - \frac{\mathrm{lcm}(\mathrm{LM}_<(f_i), \mathrm{LM}_<(f_j))}{\mathrm{LT}_<(f_j)} \cdot f_j. \tag{4}$$

Equation (4) is called the *S-polynomial* associated to the *S-pair* (f_i, f_j). If you look back at examples 1 and 3, you will see that these calculations were really computing S-pairs in disguise. A more systematic procedure generalizing these examples can be found in Figure 2. This is called *Buchberger's algorithm.*

Buchberger's algorithm may be summarized as follows. For each of the possibile S-pairs, we apply a division procedure analogous to that described in Proposition 0.10. If h is the polynomial obtained from $S_{f_i f_j}$ in step 2.ii., we say $S_{f_i f_j}$ *reduces* to h. In fact, many authors would define the normal form $\mathrm{NF}_{G,<}(h)$ with respect to an *ordered* set G as the ouput of this procedure. With that definition, we would then have $\mathrm{NF}_{I,<} = \mathrm{NF}_{G,<}$ precisely when G is a Gröbner basis (regardless of how we order the elements of G.) If some S-pair reduces to a nonzero polynomial h, we add h to our partial Gröbner basis, and we now need to reduce further S-pairs involving h. Once all S-pairs are processed, our partial Gröbner basis is, in fact, a Gröbner basis. The following theorem establishes this fact, and much more.

Theorem 3. Fix $G = \{g_1, \dots, g_s\} \subset \mathbb{K}[\mathbf{x}]$ and $<$ a monomial order. The following are equivalent:

1. G is a Gröbner basis with respect to $<$
2. Buchberger's algorithm run on $(<, \langle G \rangle)$ outputs G.
3. Every S-polynomial formed from G has a *standard representation*: that is, whenever $1 \le i < j \le s$ we can write
$$S_{g_i,g_j} = \sum_{k=1}^{s} h_k g_k \tag{5}$$
where $\mathrm{LM}_<(h_k g_k) \le \mathrm{LM}_<(S_{g_i g_j})$ for all k with $h_k g_k \ne 0$.
4. Every S-polynomial formed from G has a *lcm representation*: that is, whenever $1 \le i < j \le s$ we can write
$$S_{g_i,g_j} = \sum_{k=1}^{s} h_k g_k \tag{6}$$
where $\mathrm{LM}_<(h_k g_k) < \mathrm{lcm}(\mathrm{LM}_<(g_i), \mathrm{LM}_<(g_j))$ for all k with $h_k g_k \ne 0$.

Here is a (unrealistically simple) example of Buchberger's algorithm in action:

Example 8. Let $f_1 = \underline{x^2}$, $f_2 = \underline{xy} + y^2$. We use the `Lex` order with $x > y$. We compute

$$\begin{aligned} S_{f_1 f_2} &= y f_1 - x f_2 \\ &= -\underline{xy^2} && \text{(divisible by } \mathrm{LM}_<(f_2)) \\ &= -f_2 + \underline{y^3}. \end{aligned}$$

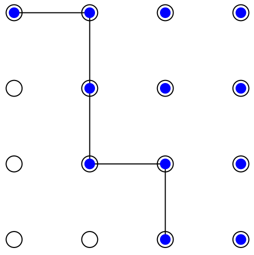
Since y^2 is not divisible by $\mathrm{LM}_<(f_1)$ or $\mathrm{LM}_<(f_2)$, we set $f_3 = y^2$, and set $G = \{f_1, f_2, f_3\}$. Now we have two more S-polynomials to check:

$$S_{f_1 f_3} = y^3 x^2 - x^2 y^3 = 0,$$

and

$$\begin{aligned} S_{f_2 f_3} &= y^2 f_2 - x f_3 \\ &= \underline{y^4} && \text{(divisible by } \mathrm{LM}_<(f_3)) \\ &= y f_2 + 0. \end{aligned}$$

Theorem 3 implies G is a Gröbner basis, and $\mathrm{in}_<(I) = \langle x^2, xy, y^3 \rangle$. The standard monomials $1, x, y, y^2$ can be visualized as the lattice points in $\mathbb{Z}^2_{\ge 0}$ below a "staircase" formed by the generators of the initial ideal.



Proposition 0.14 establishes that Buchberger's algorithm *terminates* in finite time. Combined with Theorem 3, it's straightforward to see that the output G forms a Gröbner basis, since the S-pairs formed from G are among the (potentially very large) set of S-pairs that are processed.

Proposition 0.14. For any input $(I, <)$, Buchberger's algorithm (Figure 2) terminates after finitely-many steps.

Proof. To see that Buchberger's algorithm terminates, let

$$I_1 = \langle \mathrm{LM}_<(f_1), \dots, \mathrm{LM}_<(f_s) \rangle.$$

Note that $I_1 \subset \mathrm{in}_<(I)$, and that the inclusion is strict iff $\{f_1, \ldots, f_s\}$ is not a Gröbner basis with respect to $<$. If h is the result of reducing some S-pair when running the algorithm, set $I_2 = I_1 + \langle \mathrm{LM}_<(h) \rangle$. Constructing $I_3, I_4, \ldots$ in a similar way, we obtain an ascending chain of monomial ideals which must stabilize by Exercise 2. Suppose the chain stabilizes after processing n S-pairs, and consider the reduction of any subsequent S-pair. This will be some polynomial h with $\mathrm{LM}_<(h) \in I_{n+1}$. We claim $h = 0$; if not, then we would have $\mathrm{LM}_<(h) \notin I_n$, however $I_n = I_{n+1}$. Thus, after n steps, all remaining S-polynomials reduce to zero. □

Proof of Theorem 3. (1) ⇒ (2): If h is the result of reducing any S-pair formed from G, we must show that h is zero. If that were not the case, then we would have, just as in the proof of termination, that $\mathrm{LM}_<(h)$ was not divisible by any $\mathrm{LM}_<(g_i)$, contradicting the fact that G is a Gröbner basis.

(2) ⇒ (3): Suppose we were to trace the "quotients" produced in each reduction step (step 2.ii) of Buchberger's algorithm. Since we assume each S-pair reduces to zero, this would give us a representation

$$S_{g_i,g_j} = \sum_{k=1}^{s} h_k g_k.$$

If $h_k \neq 0$, then h_k is a sum of polynomials whose leading terms have the form $t_{i,j} / \mathrm{LM}_<(g_k)$ for some term $t_{ij} < \mathrm{LM}_<(S_{g_i g_j})$, thus showing that this representation is standard.

(3) ⇒ (4): Every standard representation is also an lcm representation.

(4) ⇒ (1): Proof by contradiction. Let $f \in \langle G \rangle$, and suppose that $\mathrm{LM}_<(f)$ is not divisible by $\mathrm{LM}_<(g)$ for any $g \in G$. Consider the following representation of f as an element of $\langle G \rangle$:

$$f = \sum_{j=1}^{s} h_s g_s. \tag{7}$$

Without loss of generality, we may assume the $h_s g_s$ are sorted by leading monomial[2],

$$\mathrm{LM}_<(h_s g_s) \leq \mathrm{LM}_<(h_{s-1} g_{s-1}) \leq \cdots \leq \mathrm{LM}_<(h_{\mu+1} g_{\mu+1}) < \mathrm{LM}_<(h_\mu g_\mu) = \mathrm{LM}_<(h_{\mu-1} g_{\mu-1}) = \cdots = \mathrm{LM}_<(h_1 g_1).$$

We choose a representation 7 such that $\mathrm{LM}_<(h_1 g_1)$ is minimal, and further such that the number μ of leading monomials is also minimal.

If $\mu = 1$, then $\mathrm{LM}_<(h_1 g_1)$ occurs as a monomial of some $h_s g_s$ iff $s = 1$. Thus $\mathrm{LM}_<(f) = \mathrm{LM}_<(h_1 g_1)$, which implies $\mathrm{LM}_<(g_1)$ divides $\mathrm{LM}_<(f)$, a contradiction.

Since $\mu > 1$, we may consider the monomial

$$m = \frac{\mathrm{LM}_<(h_1 g_1)}{\mathrm{lcm}(\mathrm{LM}_<(g_1), \mathrm{LM}_<(g_2))} = \frac{\mathrm{LM}_<(h_2 g_2)}{\mathrm{lcm}(\mathrm{LM}_<(g_1), \mathrm{LM}_<(g_2))}. \tag{8}$$

In particular, for some $c \in \mathbb{K}$ we may write

$$\mathrm{LT}_<(h_1)\, \mathrm{LT}_<(g_1) = cm\, \mathrm{lcm}(\mathrm{LM}_<(g_1), \mathrm{LM}_<(g_s)). \tag{9}$$

Now consider an lcm representation of $S_{g_1 g_2}$,

$$S_{g_1 g_2} = \sum_{k=1}^{s} \hat{h}_k g_k, \quad \text{where } \hat{h}_k g_k \neq 0 \;\Rightarrow\; \mathrm{LM}_<(\hat{h}_k g_k) < \mathrm{lcm}(\mathrm{LM}_<(g_1), \mathrm{LM}_<(g_2)). \tag{10}$$

Multiplying this equation by cm and then subtracting $cm\, S_{g_1 g_2}$ from both sides, we obtain (using 8) a representation of 0 as an element of $\langle G \rangle$,

$$0 = \Big(cm\hat{h}_1 - \mathrm{LT}_<(h_1)\Big)\, g_1 + \Big(cm\hat{h}_2 + c'\, \mathrm{LT}_<(h_2)\Big)\, g_2 + \sum_{k=3}^{s} (cm\hat{h}_s)\, g_s, \tag{11}$$

[2] In this case, if $h_i g_s = 0$, we should take $\mathrm{LM}_<(h_i g_i) = 1$.

where $c' \in \mathbb{K}$ may depend on c and $\mathrm{LC}_<(g_2)$. Adding 11 to 7, we obtain a new representation of f as an element of $\langle G \rangle$. For this representation, observe that

$$\begin{aligned} \mathrm{LM}_< \left(\left(h_1 - \mathrm{LT}_<(h_1) + cm\hat{h}_1 \right) g_1 \right) &\leq \max \left((h_1 - \mathrm{LT}_<(h_1))\, \mathrm{LM}_<(g_1),\, m\, \mathrm{LM}_<(\hat{h}_1 g_1) \right) \\ &< \max \left(\mathrm{LM}_<(h_1 g_1),\, m \ \mathrm{lcm}(\mathrm{LM}_<(g_1), \mathrm{LM}_<(g_2)) \right) && \text{(using 10)} \\ &= \mathrm{LM}_<(h_1 g_1) && \text{(using 9.)} \end{aligned}$$

Similarly, one may show

$$\begin{aligned} \mathrm{LM}_< \left(\left(h_2 - c'\, \mathrm{LT}_<(h_2) + cm\hat{h}_2 \right) g_2 \right) &\leq \mathrm{LM}_<(g_2 h_2), \quad \text{strict iff } c = c', \\ \mathrm{LM}_< \left(\left(h_s + cm\hat{h}_s \right) g_s \right) &\leq \mathrm{LM}_<(h_s g_s) \quad \forall s \geq 3. \end{aligned}$$

Thus, for this new representation, we have either fewer leading monomials, or if $\mu = 2$ and $c' = c$, a smaller leading monomial. In either case, this contradicts the minimality of 7. □

A weakness of Buchberger's algorithm is that it spends a huge amount of time reducing *superfluous* S-pairs which can ultimately be reduced to 0. Thus, it is a huge advantage to be able to predict in advance when this will occur. This leads naturally to *Buchberger's criteria*. The first of these criteria is the simplest to use, and its proof follows easily from the lcm representation appearing in Theorem 3.

Proposition 0.15. [Buchberger's first criterion] Suppose $f, g \in G$ are such that $\mathrm{LM}_<(f)$ and $\mathrm{LM}_<(g)$ are relatively prime. Then S_{fg} has a lcm representation with respect to G and $<$.

Proof. We define the "tails" of f and g wrt $<$ to be

$$\mathrm{tail}_<(f) = f - \mathrm{LT}_<(f), \quad \mathrm{tail}_<(g) = g - \mathrm{LT}_<(g).$$

WLOG assume $\mathrm{LC}_<(f) = \mathrm{LC}_<(g) = 1$. We then calculate

$$\begin{aligned} S_{fg} &= \mathrm{LM}_<(g) f - \mathrm{LM}_<(f) g \\ &= (g - \mathrm{tail}_<(g)) f - (f - \mathrm{tail}_<(f)) g \\ &= \mathrm{tail}_<(f) g - \mathrm{tail}_<(g) f. \end{aligned}$$

The last of these formulae is a lcm representation, since

$$\begin{aligned} \mathrm{LM}_< \left(\mathrm{tail}_<(f) g \right) \ &< \ \mathrm{LM}_<(fg) = \mathrm{lcm}(\mathrm{LM}_<(f), \mathrm{LM}_<(g)), \\ \mathrm{LM}_< \left(\mathrm{tail}_<(g) f \right) \ &< \ \mathrm{LM}_<(fg) = \mathrm{lcm}(\mathrm{LM}_<(f), \mathrm{LM}_<(g)). \end{aligned}$$

□

There are many examples which show that Gröbner bases are not preserved under specialization of variables. For instance, if we take $G = \{\underline{ax} + y + b, \underline{by} + z\}$, then Proposition 0.15 implies this is a Gröbner basis for the Lex order with $a > y > b > z > x$. However, if we set $a = 1$, and work with the induced Lex order on the remaining variables, our polynomials become $G = \{x + \underline{y} + b, \underline{by} + z\}$, and we get the S-polynomial

$$b(x + \underline{y} + b) - (\underline{by} + z) = \underline{b^2} + bx - z \quad \text{w/} \quad b^2 \notin \langle y, by \rangle.$$

Nevertheless, we *can* prove a specialization property for elimination orders with $\mathbf{x} > \mathbf{y}$, provided that we specialize the cheap variables $\mathbf{y}$ to *sufficiently generic* values.

Proposition 0.16. Let $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}[\mathbf{x}, \mathbf{y}] = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ be a Gröbner basis with respect to an elimination order with $\mathbf{x} > \mathbf{y}$. Let us partition the set G as

$$G = \{g_1, \ldots, g_{s'}\} \cup \{g_{s'+1}, \ldots, g_s\}$$

where $g_1, \ldots, s_{s'} \in \mathbb{K}[\mathbf{y}]$ and $g_{s'+1}, \ldots, g_s \notin \mathbb{K}[\mathbf{y}]$. We may write for $i = s' + 1, \ldots, s$,

$$g_i(\mathbf{x}, \mathbf{y}) = c_i(\mathbf{y}) \mathbf{x}^{\boldsymbol{\alpha}_i} + \text{l.o.t.},$$

where $\mathrm{LT}_<(g_i) = \mathrm{LT}_<(c_i) \cdot \mathbf{x}^{\boldsymbol{\alpha}_i}$ where $x^{\boldsymbol{\alpha}_i} > 1$. Then, if $\bar{y} \in \mathbb{K}^m$ is a point such that $c_i(\bar{y}) \neq 0$ for all $s' + 1 \leq i \leq s'$, and $g_i(\bar{y}) = 0$ for $1 \leq i \leq s'$, the set of specialized polynomials $\{g_1(\mathbf{x}, \bar{y}), \ldots, g_s(\mathbf{x}, \bar{y})\}$ is a Gröbner basis.

To prove Proposition 0.16, we develop further the notion of a standard representation appearing in Theorem 3.

Proposition 0.17. Let $G = \{g_1, \dots, g_s\} \subset \mathbb{K}[\mathbf{x}]$ and fix a monomial order $<$.

1. If we have
$$\mathrm{LM}_<(g_1 + g_2 + \cdots g_s) < \mathrm{LM}_<(g_1) = \mathrm{LM}_<(g_2) = \cdots = \mathrm{LM}_<(g_s), \tag{12}$$
then $g_1 + \cdots + g_s$ is a $\mathbb{K}$-linear combination of S-polynomials formed from G.

2. If G is a Gröbner basis, then every $f \in \langle G \rangle$ has a standard representation,
$$f = \sum_{i=1}^{s} h_i g_i \quad \text{w/} \quad h_i g_i \neq 0 \Rightarrow \mathrm{LM}_<(h_i g_i) \leq \mathrm{LM}_<(f).$$

Proof. For part 1, our assumption 12 implies that
$$\mathrm{LC}_<(g_1) + \mathrm{LC}_<(g_2) + \cdots + \mathrm{LC}_<(g_s) = 0. \tag{13}$$

It follows that a suitable $\mathbb{K}$-linear combination is given by
$$\begin{aligned}\sum_{i=1}^{s-1} \mathrm{LC}_<(g_i) S_{g_i g_s} &= \sum_{i=1}^{s-1} \mathrm{LC}_<(g_i) \left(\frac{g_i}{\mathrm{LC}_<(g_i)} - \frac{g_s}{\mathrm{LC}_<(g_s)} \right) \\ &= \sum_{i=1}^{s-1} g_i - \left(\sum_{i=1}^{s-1} \frac{\mathrm{LC}_<(g_i)}{\mathrm{LC}_<(g_s)} \right) g_s \\ &= \sum_{i=1}^{s} g_i & \text{(by 13.)}\end{aligned}$$

For part 2, take any $f = \sum_{i=1}^{s} h_i g_i \in I$. Let $\mathbf{x}^{\boldsymbol{\alpha}}$ be the maximum element of $\{\mathrm{LM}_<(h_i g_i) \mid 1 \leq i \leq s\}$, and write
$$f = \sum_{\substack{i \text{ w/} \\ \mathrm{LM}_<(h_i g_i) = \mathbf{x}^{\boldsymbol{\alpha}}}} \mathrm{LT}_<(h_i) g_i \; + \sum_{\substack{i \text{ w/} \\ \mathrm{LM}_<(h_i g_i) = \mathbf{x}^{\boldsymbol{\alpha}}}} \mathrm{tail}_<(h_i) g_i \; + \; \text{l.o.t.}$$

By Part 1, the first summand as a linear combination of S-polynomials formed from G, and thus Theorem 3 implies it has a standard representation. Since the second and third summands contribute smaller leading terms than the first, we conclude that f has a standard representation. □

Proof of Proposition 0.16. Consider the "partial S-polynomials" defined by
$$S_{ij}(\mathbf{x}, \mathbf{y}) = \frac{\mathrm{lcm}(\mathbf{x}_i^{\boldsymbol{\alpha}}, \mathbf{x}_j^{\boldsymbol{\alpha}})}{c_i(\bar{y})\, \mathbf{x}_i^{\boldsymbol{\alpha}}} g_i(\mathbf{x}, \mathbf{y}) - \frac{lcm(\mathbf{x}_i^{\boldsymbol{\alpha}}, \mathbf{x}_j^{\boldsymbol{\alpha}})}{c_j(\bar{y})\, \mathbf{x}_j^{\boldsymbol{\alpha}}} g_j(\mathbf{x}, \mathbf{y}).$$

If we specialize, we get an honest S-polynomial with respect to the induced order on $\mathbb{K}[\mathbf{x}]$,
$$S_{ij}(\mathbf{x}, \bar{y}) = S_{g_i(\mathbf{x}, \bar{y}) g_j(\mathbf{x}, \bar{y})}.$$

By Proposition 0.17, $S_{ij}(\mathbf{x}, \mathbf{y})$ has a standard representation in $\mathbb{K}[\mathbf{x}, \mathbf{y}]$,
$$S_{ij}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{s} h_i(\mathbf{x}, \mathbf{y}) g_i(\mathbf{x}, \mathbf{y}). \tag{14}$$

For each summand whose specialization doesn't vanish, $h_i(\mathbf{x}\bar{y}) g_i(\mathbf{x}, \bar{y}) \neq 0$, we have
$$\begin{aligned}\mathrm{LM}_< \left(h_i(\mathbf{x}, \bar{y}) g_i(\mathbf{x}, \bar{y})\right) &\leq \mathrm{LM}_< \left(h_i(\mathbf{x}, \mathbf{y}) g_i(\mathbf{x}, \mathbf{y})\right) \\ &\leq \mathrm{LM}_<(S_{ij}) \\ &< \mathrm{lcm}(\mathbf{x}^{\boldsymbol{\alpha}_i}, \mathbf{x}^{\boldsymbol{\alpha}_j})\end{aligned}$$

where the first and third inequalities use the fact that $<$ is an elimination order. Thus, specializing the standard representation 14 in $\mathbb{K}[\mathbf{x}, \mathbf{y}]$, we obtain a lcm representation for the corresponding S-polynomial in $\mathbb{K}[\mathbf{x}]$,

$$S_{g_i(\mathbf{x},\bar{y})g_j(\mathbf{x},\bar{y})} = \sum_{i=1}^{s} h_i(\mathbf{x}, \bar{y}) g_i(\mathbf{x}, \bar{y}).$$

Thus, Theorem 3 implies that $\{g_1(\mathbf{x}, \bar{y}), \ldots, g_s(\mathbf{x}, \bar{y})\}$ forms a Gröbner basis. □

References: Cox, Little, O'Shea, *Ideals Varieties and Algorithms* (4th edition), Chapters 1–3.