2.5 Buchberger's Algorithm

Knowing + and × is good enough,
understanding their interaction is ideal.
(Bruno Buchberger)

In the last section we saw some theoretical applications of Gröbner bases, especially of reduced Gröbner bases. But Gröbner bases would be hardly more than a small side subject in commutative algebra if we did not have the possibility of computing them. The key to almost all applications of Gröbner bases in Computational Commutative Algebra, and therefore to the remainder of these volumes, is the algorithm developed by Bruno Buchberger in his doctoral thesis [Bu65].

As we mentioned in the introduction of Section 2.3, the algorithmic way to replace a given set of generators of a module with a Gröbner basis is based on the characterization of Gröbner bases via lifting of syzygies. The idea is that we need to check whether the set of generators satisfies Condition D_3). If a syzygy of the leading terms is found which does not lift to a syzygy of the generators, we can find an element of the module which has a *new* leading term. By adding it to the set of generators, we can achieve the desired lifting. Then the termination of the algorithm is guaranteed by Dickson's Lemma (more precisely, by Corollary 1.3.10), and its correctness follows from the fact that lifting of syzygies characterizes Gröbner bases (see Theorem 2.4.1).

Since Buchberger's Algorithm is the basic tool underlying most calculations in Computational Commutative Algebra, it is very important to study possibilities for optimizing it. First indications on how to avoid some unnecessary steps in the execution of the algorithm are given in Remark 2.5.6 and Proposition 2.5.8. Some additional possibilities are contained in Tutorial 25. For the case of systems of generators consisting of homogeneous polynomials or vectors of polynomials, an efficient version of Buchberger's Algorithm will be explained in Volume 2.

At the end of this section we discuss the Extended Buchberger Algorithm. Besides a Gröbner basis, it also yields the change of basis matrix from the given system of generators to the Gröbner basis (see Proposition 2.5.11).

As usual, let K be a field, let $n \geq 1$, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring, let $r \geq 1$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Our goal is to compute a σ-Gröbner basis of a P-submodule $M \subseteq P^r$ which is explicitly given by a system of generators $G = \{g_1, \ldots, g_s\} \subseteq P^r \setminus \{0\}$. Let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$. We start by writing $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$ with $c_i \in K \setminus \{0\}$, $t_i \in \mathbb{T}^n$, and $\gamma_i \in \{1, \ldots, r\}$ for $i = 1, \ldots, s$, and by recalling the fundamental diagram

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \mathrm{Syz}(\mathcal{G}) & \longrightarrow & P^s & \xrightarrow{\lambda} & P^r & \longrightarrow & P^r/M & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \mathrm{LF}} & & \downarrow{\scriptstyle \mathrm{LM}} & & & & \\
0 & \longrightarrow & \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) & \longrightarrow & P^s & \xrightarrow{\Lambda} & P^r & \longrightarrow & P^r/N & \longrightarrow & 0
\end{array}$$

studied in Section 2.3. Then we introduce or recall the following abbreviations.

Definition 2.5.1. Let $\mathbb{B}$ be the set $\mathbb{B} = \{(i,j) \mid 1 \leq i < j \leq s, \gamma_i = \gamma_j\}$. Moreover, let $t_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{t_i} = \frac{t_j}{\mathrm{gcd}(t_i,t_j)} \in \mathbb{T}^n$ and $\sigma_{ij} = \frac{1}{c_i} t_{ij} \varepsilon_i - \frac{1}{c_j} t_{ji} \varepsilon_j \in P^s$ for all $i,j \in \{1,\ldots,s\}$. For every pair $(i,j) \in \mathbb{B}$, we call

$$S_{ij} = \lambda(\sigma_{ij}) = \tfrac{1}{c_i}\, t_{ij}\, g_i - \tfrac{1}{c_j}\, t_{ji}\, g_j \in M$$

the **S-vector** of g_i and g_j. If $r = 1$, we call $S_{ij} \in P$ also the **S-polynomial** of g_i and g_j.

We can rephrase Theorem 2.3.7 by saying that if $(i,j) \in \mathbb{B}$, then σ_{ij} is a homogeneous element of P^s with $\deg_{\sigma,G}(\sigma_{ij}) = \mathrm{lcm}(t_i,t_j) e_{\gamma_i}$ and that the set $\Sigma = \{\sigma_{ij} \mid (i,j) \in \mathbb{B}\}$ is a homogeneous system of generators of the P-module $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Furthermore, we know by Theorem 2.4.1 that G is a σ-Gröbner basis of M if and only if all those elements σ_{ij} have liftings in $\mathrm{Syz}(\mathcal{G})$. For some of them, this is always the case.

Proposition 2.5.2. *Let $(i,j) \in \mathbb{B}$ be such that $S_{ij} \xrightarrow{G} 0$. Then σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$.*

Proof. If $S_{ij} = 0$, there is nothing to show, since σ_{ij} is a lifting of itself. Thus we may assume $S_{ij} \neq 0$. In view of Lemma 2.2.6, we can use $S_{ij} \xrightarrow{G} 0$ to obtain a representation $S_{ij} = \sum_{k=1}^s f_k g_k$ with $f_1,\ldots,f_s \in P$ such that $\mathrm{LT}_\sigma(S_{ij}) = \max_\sigma\{\mathrm{LT}_\sigma(f_k g_k) \mid 1 \leq k \leq s,\ f_k g_k \neq 0\}$. Since σ_{ij} is homogeneous, we have $\Lambda(\mathrm{LF}(\sigma_{ij})) = \Lambda(\sigma_{ij}) = 0$, and Proposition 2.3.6.b yields $\deg_{\sigma,G}(\sigma_{ij}) >_\sigma \mathrm{LT}_\sigma(S_{ij})$. Now we consider the element $\tau_{ij} = \sigma_{ij} - \sum_{k=1}^s f_k \varepsilon_k \in P^s$. From $\deg_{\sigma,G}(\sum_{k=1}^s f_k \varepsilon_k) = \mathrm{LT}_\sigma(S_{ij}) <_\sigma \deg_{\sigma,G}(\sigma_{ij})$ we deduce that $\mathrm{LF}_{\sigma,G}(\tau_{ij}) = \sigma_{ij}$. From $\lambda(\tau_{ij}) = \lambda(\sigma_{ij}) - S_{ij} = 0$ and $\mathrm{LF}(\tau_{ij}) = \sigma_{ij}$ we conclude that τ_{ij} is a lifting of σ_{ij} in $\mathrm{Syz}(\mathcal{G})$. □

Corollary 2.5.3. (Buchberger's Criterion)
Let $M \subseteq P^r$ be a P-submodule generated by $G = \{g_1,\ldots,g_s\} \subseteq P^r \setminus \{0\}$, and let $\mathcal{G} = (g_1,\ldots,g_s)$. Then the following conditions are equivalent.

a) The set G is a σ-Gröbner basis of M.
b) For all pairs $(i,j) \in \mathbb{B}$, we have $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$.

Proof. If G is a σ-Gröbner basis of M, then $S_{ij} \in M$ yields $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$ by Corollary 2.4.9.a and Proposition 2.4.10.a. Conversely, if condition b) holds, then $S_{ij} \xrightarrow{G} 0$. Using Proposition 2.5.2 we see that, for every pair $(i,j) \in \mathbb{B}$, the element σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$. Thus Condition D_3) of Theorem 2.4.1 holds. □

Let us see how this criterion applies in practice. The following example also shows that *the leading term ideal of the square of an ideal is, in general,* NOT *the square of the leading term ideal.*

Example 2.5.4. Let $P = \mathbb{Q}[x,y,z]$, let $\sigma = \texttt{DegRevLex}$, and let I be the ideal of P generated by $g_1 = x^2 - y^2$, $g_2 = xy^2 - z^3$, and $g_3 = y^4 - xz^3 = -y^2 g_1 + x g_2$. Successively, we compute

$$\begin{aligned} S_{12} &= -y^2 g_1 + x g_2 = y^4 - xz^3 \xrightarrow{g_3} 0 \\ S_{13} &= y^4 g_1 - x^2 g_3 = -y^6 + x^3 z^3 \xrightarrow{g_3} x^3 z^3 - xy^2 z^3 \xrightarrow{g_2} 0 \\ S_{23} &= y^2 g_2 - x g_3 = -y^2 z^3 + x^2 z^3 \xrightarrow{g_1} 0 \end{aligned}$$

Thus Buchberger's Criterion applies and says that $\{g_1, g_2, g_3\}$ is a σ-Gröbner basis of I. In particular, the leading term ideal of I is $\mathrm{LT}_\sigma(I) = (x^2, xy^2, y^4)$.

By the way, in this example the obvious inclusion $\mathrm{LT}_\sigma(I)^2 \subseteq \mathrm{LT}_\sigma(I^2)$ is a strict one, disproving a claim in [CLS92], p. 443. More precisely, the element $f = g_2^2 - g_1 g_3 = y^6 + x^3 z^3 - 3xy^2 z^3 + z^6 \in I^2$ has a leading term $\mathrm{LT}_\sigma(f) = y^6$ which is not in $\mathrm{LT}_\sigma(I)^2$.

The idea of Buchberger's Algorithm is to enlarge G in such a way that eventually all elements σ_{ij} with $(i,j) \in \mathbb{B}$ have a lifting in $\mathrm{Syz}(\mathcal{G})$. By Theorem 2.4.1, this ensures that the enlarged set is a σ-Gröbner basis of M.

Theorem 2.5.5. (Buchberger's Algorithm)
Let $\mathcal{G} = (g_1, \ldots, g_s) \in (P^r)^s$ be a tuple of non-zero elements which generate a submodule $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$. For $i = 1, \ldots, s$, let $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$ with $c_i \in K \setminus \{0\}$, $t_i \in \mathbb{T}^n$, and $\gamma_i \in \{1, \ldots, r\}$. Consider the following sequence of instructions.

1) *Let $s' = s$ and $B = \mathbb{B} = \{(i,j) \mid 1 \leq i < j \leq s', \gamma_i = \gamma_j\}$.*
2) *If $B = \emptyset$, return the result $\mathcal{G}$. Otherwise, choose a pair $(i,j) \in B$ and delete it from B.*
3) *Compute $S_{ij} = \frac{t_j}{c_i \gcd(t_i,t_j)} g_i - \frac{t_i}{c_j \gcd(t_i,t_j)} g_j$ and $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If the result is $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$, continue with step 2).*
4) *Increase s' by one. Append $g_{s'} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ to $\mathcal{G}$ and the set of pairs $\{(i,s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ to B. Then continue with step 2).*

This is an algorithm, i.e. it stops after finitely many steps. It returns a tuple $\mathcal{G}$ of vectors which form a σ-Gröbner basis of M.

Proof. Every time step 2) is executed, one pair is cancelled from B. The set B is enlarged only in step 4). When this happens, an element is appended to $\mathcal{G}$ which has a leading term with respect to σ which is not in the monomodule generated by the leading terms of the previous elements of $\mathcal{G}$. Corollary 1.3.10 shows that P^r cannot contain an infinite chain

$$\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s) \rangle \subset \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s+1}) \rangle \subset \cdots$$

Therefore step 4) can be executed only a finite number of times, i.e. the procedure stops after finitely many steps.

It remains to show that when the algorithm stops, the vectors in the resulting tuple $\mathcal{G}$ form a σ-Gröbner basis of M. During the execution of the procedure all pairs $(i,j) \in \mathbb{B}$ are considered, since whenever s' is increased in step 4), all necessary new pairs (i,s') are added to B. By Corollary 2.5.3, it suffices to show that, for every $(i,j) \in \mathbb{B}$, we have $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$. If at a certain step $S_{ij} = 0$ or $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$, there is nothing to prove. If at a certain step $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) \neq 0$, then $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ is added to the tuple $\mathcal{G}$. Hence $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ reduces to 0 via the rewrite rule defined by the vectors in the new tuple. □

A closer look at this proof shows that a number of variants and optimizations of Buchberger's Algorithm are possible. Some of the most effective ones will be discussed in Tutorial 25 and in Volume 2. Here we limit ourselves to pointing out some obvious opportunities for improvement.

Remark 2.5.6. (First Optimizations of Buchberger's Algorithm)

a) In Buchberger's Algorithm, one can substitute the computation of the normal remainder $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ by any procedure producing an element $m \in P^r$ which satisfies $S_{ij} \xrightarrow{G} m$, and $\mathrm{LT}_\sigma(m) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s'}) \rangle$ if $m \neq 0$.

b) If $\mathbb{B}' \subseteq \mathbb{B}$ is a subset with the property that also the set $\{\sigma_{ij} \mid (i,j) \in \mathbb{B}'\}$ generates $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$, it suffices to start with $B = \mathbb{B}'$ in step 1) of Buchberger's Algorithm. This follows from Proposition 2.3.11.

c) In step 2) of the theorem we did not specify which pair $(i,j) \in B$ we should choose. One possibility is to take the pair (i,j) for which $\mathrm{lcm}(t_i,t_j)$ is minimal with respect to σ. This is called the **normal selection strategy**. It works well in practice if the term ordering σ is degree-compatible. Another possibility which avoids sorting the terms $\mathrm{lcm}(t_i,t_j)$ with respect to σ is to take any pair (i,j) for which the degree of $\mathrm{lcm}(t_i,t_j)$ is minimal.

To help the reader understand Theorem 2.5.5 better, we now apply Buchberger's Algorithm in a concrete case.

Example 2.5.7. Let $n = 2$, let $r = 1$, let $M \subseteq P = K[x,y]$ be the ideal generated by $g_1 = x^2$ and $g_2 = xy + y^2$, and let $\mathcal{G} = (g_1, g_2)$. We want to compute a Gröbner basis of M with respect to $\sigma = \texttt{Lex}$ and follow the steps of Buchberger's Algorithm.

1) Let $s' = 2$ and $B = \{(1,2)\}$.
2) Choose $(1,2) \in B$ and set $B = \emptyset$.
3) We compute $S_{12} = yg_1 - xg_2 = -xy^2 \xrightarrow{g_2} y^3 = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{12}) \neq 0$.
4) Let $s' = 3$, let $\mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = y^3$, and let $B = \{(1,3),(2,3)\}$. Then return to step 2).
2) Choose $(1,3) \in B$ and set $B = \{(2,3)\}$.
3) We compute $S_{13} = y^3 g_1 - x^2 g_3 = 0$ and return to step 2).

2) Choose $(2,3) \in B$ and set $B = \emptyset$.
3) We compute $S_{23} = y^2 g_2 - x g_3 = y^4$. Then we calculate $S_{23} \xrightarrow{g_3} 0 = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{23})$ and return to step 2).
2) Since $B = \emptyset$, we return the result $\mathcal{G} = (g_1, g_2, g_3)$.

If $r = 1$, i.e. if M is an ideal in P, there is another optimization of Buchberger's Algorithm which turns out to be useful in practise.

Proposition 2.5.8. *Let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero polynomials, let $I = (g_1, \ldots, g_s) \subseteq P$, and let $t_i = \mathrm{LT}_\sigma(g_i)$ for $i = 1, \ldots, s$. Suppose that $\gcd(t_i, t_j) = 1$ for some pair $(i,j) \in \mathbb{B}$. Then σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$.*

Proof. This follows from the observations that $\sigma_{ij} = \frac{1}{c_i} t_j \varepsilon_i - \frac{1}{c_j} t_i \varepsilon_j$ and that $\tau_{ij} = \frac{1}{c_i c_j} g_j \varepsilon_i - \frac{1}{c_i c_j} g_i \varepsilon_j$ is a lifting of σ_{ij} in $\mathrm{Syz}(\mathcal{G})$. □

Remark 2.5.9. For $f, g \in P$, the pair $(-g, f)$ is called the **trivial syzygy** of (f, g). Therefore Proposition 2.5.8 can be rephrased by saying that if $\gcd(t_i, t_j) = 1$, then the trivial syzygy of $(\mathrm{LM}_\sigma(g_i), \mathrm{LM}_\sigma(g_j))$ can be lifted to the trivial syzygy of (g_i, g_j).

The above result can be used to detect some special Gröbner bases.

Corollary 2.5.10. *Let $G = \{g_1, \ldots, g_s\} \subseteq P \setminus \{0\}$, and let $I = (g_1, \ldots, g_s)$. Assume that the leading terms of the elements $g_1, \ldots, g_s$ are pairwise coprime. Then G is a σ-Gröbner basis of I.*

Proof. Let $\mathcal{G} = (g_1, \ldots, g_s)$. By Proposition 2.5.8, every element σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$. Thus G satisfies Condition D_3) of Theorem 2.4.1. □

Finally, we can extend Buchberger's Algorithm in such a way that it not only computes a Gröbner basis of a submodule $M \subseteq P^r$, but also a matrix of polynomials which describes how the Gröbner basis can be expressed in terms of the original system of generators of M.

Proposition 2.5.11. (The Extended Buchberger Algorithm)
Let $\mathcal{G} = (g_1, \ldots, g_s) \in (P^r)^s$ be a tuple of non-zero vectors in P^r which generate a submodule $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$. We write $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$ with $c_i \in K \setminus \{0\}$, $t_i \in \mathbb{T}^n$, and $\gamma_i \in \{1, \ldots, r\}$ for $i = 1, \ldots, s$. Consider the following sequence of instructions.

1) Let $s' = s$, let $\mathcal{A}$ be the $s \times s$ identity matrix, and let $B = \mathbb{B}$.
2) If $B = \emptyset$, return the result $(\mathcal{G}, \mathcal{A})$. Otherwise, choose a pair $(i,j) \in B$ and delete it from B.
3) Use the Division Algorithm 1.6.4 to compute a representation $S_{ij} = q_1 g_1 + \cdots + q_{s'} g_{s'} + p$, where $q_1, \ldots, q_{s'} \in P$ and $p \in P^r$, such that the conditions of Theorem 1.6.4 hold.
If $p = 0$, continue with step 2).

4) If $p \neq 0$ in step 3), then increase s' by one, append $g_{s'} = p$ to $\mathcal{G}$, add $\{(i,s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ to B, and append the column vector $\frac{t_j}{c_i \operatorname{gcd}(t_i,t_j)} a_i - \frac{t_i}{c_j \operatorname{gcd}(t_i,t_j)} a_j - q_1 a_1 - \cdots - q_{s'-1} a_{s'-1}$ to $\mathcal{A}$, where $a_1, \ldots, a_{s'-1}$ denote the previous columns of $\mathcal{A}$. Then continue with step 2).

This is an algorithm, i.e. it stops after finitely many steps. It returns a tuple $\mathcal{G} = (g_1, \ldots, g_{s'})$ of vectors which form a σ-Gröbner basis of M, where $s' \geq s$, together with an $s \times s'$-matrix $\mathcal{A} = (a_{ij})$ of polynomials such that $g_j = a_{1j} g_1 + \cdots + a_{sj} g_s$ for $j = 1, \ldots, s'$.

Proof. In view of Theorem 2.5.5, it suffices to prove the last claim. Each time a new column is appended to $\mathcal{A}$ in step 4), we have $g_j = a_{1j} g_1 + \cdots + a_{sj} g_s$ for $j < s'$, where s' is the current number of columns of $\mathcal{A}$. Now the calculation

$$\begin{aligned} g_{s'} = p &= S_{ij} - q_1 g_1 - \cdots - q_{s'-1} g_{s'-1} \\ &= \tfrac{t_{ij}}{c_i}(a_{1i} g_1 + \cdots + a_{si} g_s) - \tfrac{t_{ji}}{c_j}(a_{1j} g_1 + \cdots + a_{sj} g_s) \\ &\quad - \textstyle\sum_{k=1}^{s'-1} q_k (a_{1k} g_1 + \cdots + a_{sk} g_s) \\ &= (g_1, \ldots, g_s) \cdot \left(\tfrac{t_j}{c_i \operatorname{gcd}(t_i,t_j)} a_i - \tfrac{t_i}{c_j \operatorname{gcd}(t_i,t_j)} a_j - q_1 a_1 - \cdots - q_{s'-1} a_{s'-1}\right) \\ &= (g_1, \ldots, g_s) \cdot (a_{1s'}, \ldots, a_{ss'})^{\mathrm{tr}} = a_{1s'} g_1 + \cdots + a_{ss'} g_s \end{aligned}$$

finishes the proof. □

To show how this extended algorithm works in practice, let us apply it in the situation of Example 2.5.7.

Example 2.5.12. Let $n = 2$, let $r = 1$, let $M \subseteq P = K[x,y]$ be the ideal generated by $g_1 = x^2$ and $g_2 = xy + y^2$, and let $\mathcal{G} = (g_1, g_2)$. As in Example 2.5.7, we follow the steps of the Buchberger Algorithm, except that we now use the extended version above.

1) Let $s' = 2$, let $\mathcal{A} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and let $B = \{(1,2)\}$.
2) Choose $(1,2) \in B$ and set $B = \emptyset$.
3) We compute $S_{12} = -xy^2 = 0 \cdot g_1 + (-y) \cdot g_2 + y^3$ and let $q_1 = 0$, $q_2 = -y$, and $p = y^3$.
4) Let $s' = 3$, let $\mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = y^3$, and let $B = \{(1,3),(2,3)\}$. We append the column vector $ya_1 - xa_2 - 0 \cdot a_1 + ya_2$ to the matrix $\mathcal{A}$ and get $\mathcal{A} = \left(\begin{smallmatrix} 1 & 0 & y \\ 0 & 1 & -x+y \end{smallmatrix}\right)$. Then we return to step 2).
2) Choose $(1,3) \in B$ and set $B = \{(2,3)\}$.
3) We compute $S_{13} = y^3 g_1 - x^2 g_3 = 0$ and return to step 2).
2) Choose $(2,3) \in B$ and set $B = \emptyset$.
3) We compute $S_{23} = y^4 = 0 \cdot g_1 + 0 \cdot g_2 + y g_3$. Then we return to step 2).
2) Since $B = \emptyset$, we return the result $(\mathcal{G}, \mathcal{A})$, where $\mathcal{G} = (g_1, g_2, g_3)$ and $\mathcal{A} = \left(\begin{smallmatrix} 1 & 0 & y \\ 0 & 1 & -x+y \end{smallmatrix}\right)$.

Exercise 1. Let $P = K[x, y, z]$, let $\mathcal{G} = (x^2 - y, xy - z) \in P^2$, and let $\sigma = \texttt{DegRevLex}$. Perform all steps of Buchberger's Algorithm applied to $\mathcal{G}$. Then find a term ordering σ such that $\mathcal{G}$ is a σ-Gröbner basis of the ideal $(x^2 - y, xy - z)$.

Exercise 2. Apply Buchberger's Algorithm as in Example 2.5.7 to compute a $\texttt{DegLexPos}$-Gröbner basis of the submodule $M = \langle g_1, g_2, g_3, g_4 \rangle$ of $\mathbb{Q}[x, y]^3$ in the following cases.

a) $g_1 = (x^2, xy, y^2)$, $g_2 = (y, 0, x)$, $g_3 = (0, x, y)$, $g_4 = (y, 1, 0)$
b) $g_1 = (y - x, y, y)$, $g_2 = (xy, x, x)$, $g_3 = (x, y, y)$, $g_4 = (x, y, 0)$
c) $g_1 = (0, y, x)$, $g_2 = (0, x, xy - x)$, $g_3 = (y, x, 0)$, $g_4 = (y^2, y, 0)$

Exercise 3. In the cases of Exercise 2, determine representatives for a K-basis of $\mathbb{Q}[x, y]^3/M$.

Exercise 4. Find out which module $M \subseteq \mathbb{Q}[x, y]^3$ in Exercise 2 contains the vector

$$m = (x^2y - y^2 + xy^2,\ xy^2 - y^2 + x^2 + 2xy - x - y,\ x^2y + xy^2 - 3xy + x)$$

Exercise 5. A polynomial $f \in P = K[x_1, \ldots, x_n]$ is called a **binomial** if it is of the form $f = at + a't'$ with $a, a' \in K \setminus \{0\}$ and $t, t' \in \mathbb{T}^n$. Let σ be a term ordering on $\mathbb{T}^n$ and I a **binomial ideal**, i.e. an ideal generated by binomials.

a) Prove that the reduced σ-Gröbner basis of I consists of binomials.
b) Given a term $t \in \mathbb{T}^n$, show that $\mathrm{NF}_{\sigma,I}(t)$ is a scalar multiple of a term.

Exercise 6. Consider the polynomial ring $P = \mathbb{Q}[x, y]$, the P-submodule $M = \langle g_1, g_2, g_3, g_4 \rangle \subseteq P^3$ such that $g_1 = (xy, x, y)$, $g_2 = (y^2 + y, x + y^2, x)$, $g_3 = (-x, y, x)$, $g_4 = (y^2, y, x)$, and the module term ordering $\sigma = \texttt{LexPos}$.

a) Using the algorithm given in Proposition 2.5.11, compute a σ-Gröbner basis $\{g_1, \ldots, g_{s'}\}$ of M, where $s' \geq 4$, and a matrix $\mathcal{A}$ such that $(g_1, \ldots, g_{s'}) = (g_1, \ldots, g_4) \cdot \mathcal{A}$.
b) Now use the method described in the proof of Proposition 2.4.13 to compute the reduced σ-Gröbner basis $\{g'_1, \ldots, g'_6\}$ of M. Then find a matrix $\mathcal{A}'$ such that $(g'_1, \ldots, g'_6) = (g_1, \ldots, g_4) \cdot \mathcal{A}'$.
c) For the following elements of P^3, check whether they lie in M, and if they do, find their representations in terms of both $\{g'_1, \ldots, g'_6\}$ and $\{g_1, \ldots, g_4\}$.
   1) $m_1 = (-2y, y - 1, xy + y)$
   2) $m_2 = (xy^5 - xy + y, xy^4 + x + 2y^2 - y, y^5 + xy)$
d) For the following pairs of elements of P^r, check whether $m_1 + M$ agrees with $m_2 + M$ in the residue class module P^r/M.
   1) $m_1 = (2y, x^2y + x^2 + xy + 2x - 3y, -x + y)$, $m_2 = (-x^2 + y - x, x^3 + 2x^2, x^2 - y)$
   2) $m_1 = (x^3 + x^2 + y - x, x^2 + x, x + y)$, $m_2 = (y, x^3 + 2x^2 - xy - y, 0)$

Tutorial 23: Buchberger's Criterion

In this tutorial we shall implement Buchberger's Criterion 2.5.3 and use it to decide whether certain sets of polynomials are Gröbner bases of the ideals they generate. As in the whole section, we let K be a field, we let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over K, we let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$, where $r \geq 1$, we let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero vectors, and we let $M \subseteq P^r$ be the P-submodule generated by the vectors in $\mathcal{G}$.

a) Write a CoCoA function `CheckGB(...)` which takes $\mathcal{G}$ and uses Buchberger's Criterion 2.5.3 to check whether it forms a σ-Gröbner basis of M. (*Hint:* You may want to use the function `NormalRemainder(...)` from Tutorial 15 or the built-in CoCoA function `NR(...)`.)

b) Let $G = \{x_2 - x_1^2, x_3 - x_1^3\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$. Use the function `CheckGB(...)` to check whether G is a σ-Gröbner basis of the ideal it generates, where σ is one of the following term orderings: `Lex`, `DegLex`, `Ord(`V`)` where $V = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)$ or $V = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$.

c) Use the function `CheckGB(...)` to determine which of the following systems of generators are Gröbner bases with respect to the stated term orderings of the ideals and modules they generate. In the first three cases, try to find a term ordering and a system of generators containing G such that Corollary 2.5.10 can be applied.

1) $G = \{x_1x_2^2 - x_1x_3 + x_2, x_1x_2 - x_3^2, x_1 - x_2x_3^4\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$ with respect to `Lex`
2) $G = \{x_1^4x_2^2 - x_3^5, x_1^3x_2^3 - 1, x_1^2x_2^4 - 2x_3\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$ with respect to `DegLex`
3) $G = \{x_1x_3 - x_2^2, x_1x_4 - x_2x_3, x_2x_4 - x_3^2\} \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]$ with respect to `DegRevLex`
4) $G = \{(x_1^2 - x_2x_3)(e_1 + e_2), (x_1x_3 - x_2x_4)(e_1 - e_2), (x_3^2 - x_1x_4)e_1, (x_3^2 - x_1x_4)e_2\} \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]^2$ with respect to `PosDegRevLex` and `DegRevLexPos`
5) $G = \{(x_1 - x_2^2)e_1, (x_1 - x_3^3)e_1, (x_2 - x_1^2)e_2, (x_2 - x_3^3)e_2, (x_3 - x_1^2)e_3, (x_3 - x_2^3)e_3\} \subseteq \mathbb{Q}[x_1, x_2, x_3]^3$ with respect to `PosDegRevLex` and `DegRevLexPos`

d) Let $n > 1$, and let σ be the lexicographic term ordering on $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ such that $x_1 >_\sigma \cdots >_\sigma x_n >_\sigma y_1 >_\sigma \cdots >_\sigma y_n$. Moreover, for $i = 1, \ldots, n$, let $s_i = \sum_{1 \leq j_1 < \cdots < j_i \leq n} x_{j_1} \cdots x_{j_i}$ be the i^{th} elementary symmetric polynomial in $x_1, \ldots, x_n$ (see also Tutorial 12), and let $h_{i,j} = \sum_{\alpha_j + \cdots + \alpha_n = i} x_j^{\alpha_j} \cdots x_n^{\alpha_n}$ for $i, j = 1, \ldots, n$. Use Buchberger's Criterion to prove that the polynomials

$$g_i = (-1)^i(y_i - s_i) + \sum_{j=1}^{i-1}(-1)^j h_{i-j,i}\,(y_j - s_j)$$

such that $i = 1, \ldots, n$ form a σ-Gröbner basis of the polynomial ideal $I = (y_1 - s_1, \ldots, y_n - s_n)$.

e) Verify the result of d) for $n = 1, \ldots, 5$ by applying your function `CheckGB(...)`. Can you compute this for larger n? How far can you go?

Tutorial 24: Computing Some Gröbner Bases

The purpose of this tutorial is to implement a first version of Buchberger's Algorithm in the case of polynomial ideals, and to use it to study some particular examples. For instance, we will see that the elements of the reduced Gröbner basis of an ideal can have very high degree, even if the generators of the ideals have low degrees.

Then, for the specific ideal $I = (yz - z^2, xz - z^2, xy - z^2)$, you will be guided to find *all* possible reduced Gröbner bases of I, and to give a meaning to the picture on the cover of this book. As usual, we let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K.

a) Write a CoCoA function `SPoly(...)` which takes a tuple of non-zero polynomials $(g_1, \ldots, g_s)$ and indices $i, j \in \{1, \ldots, s\}$ with $i \neq j$ as arguments and returns the S-polynomial S_{ij} of g_i and g_j with respect to the current term ordering.

b) Implement Buchberger's Algorithm 2.5.5 in the case of polynomial ideals. To this end, write a CoCoA program `FirstGB(...)` which takes a tuple of non-zero polynomials generating the ideal and computes a Gröbner basis with respect to the current term ordering. (*Hint:* For step 3), use the built-in function `NR(...)` or `NormalRemainder(...)` of Tutorial 15.)

c) Using `FirstGB(...)`, calculate the Gröbner bases of the following ideals with respect to the stated term orderings.

   1) $I = (x_2^2,\ x_1x_2x_3 + x_3^3) \subseteq \mathbb{Q}[x_1, x_2, x_3]$ with respect to `DegRevLex`
   2) $I = (x_1^2x_2 - 1,\ x_1x_2^2 - x_1) \subseteq \mathbb{Q}[x_1, x_2]$ with respect to `Lex` and `DegLex`
   3) $I = (x_1 - x_3^4,\ x_2 - x_3^5) \subseteq \mathbb{Q}[x_1, x_2, x_3]$ with respect to `Lex` and `DegRevLex`

d) Prove that for every number $m \geq 1$, the reduced Gröbner basis of

$$I_m = (x_1^{m+1} - x_2x_3^{m-1}x_4,\ x_1x_2^{m-1} - x_3^m,\ x_1^m x_3 - x_2^m x_4) \subseteq K[x_1, x_2, x_3, x_4]$$

with respect to `DegRevLex` contains $f_m = x_3^{m^2+1} - x_2^{m^2}x_4$. Note that the degree $m^2 + 1$ of this polynomial is much higher than the degrees of the generators of I_m. Can you write down the whole reduced Gröbner basis of I_m with respect to `DegRevLex`? (Guess it or prove it!)

e) If you couldn't do the second part of d), calculate the reduced Gröbner basis of the ideal I_m with respect to `DegRevLex` using `FirstGB(...)` for $m = 1, \ldots, 100$ and determine its length.

f) Prove that the ideal I_3 of part d) has the same reduced Gröbner bases with respect to `Lex` and `DegRevLex`. Does this hold for all $m \geq 1$?

In the remainder of this tutorial, we want to study the polynomial ideal $I = (xy - z^2, xz - z^2, yz - z^2)$ in $P = K[x, y, z]$. Although we are not going to use it, we mention that I is the ideal of all polynomials which vanish at three lines in $\mathbb{A}^3_K$ passing through the origin, or, equivalently, at three points in $\mathbb{P}^2_K$ (see Tutorials 27 and 35).

g) Let σ be any term ordering such that $x >_\sigma z$ and $y >_\sigma z$. Show that the reduced σ-Gröbner basis of I is $\{xz - z^2, yz - z^2, xy - z^2\}$.

h) Let σ be any term ordering such that $x >_\sigma z$ and $z >_\sigma y$. Show that the reduced σ-Gröbner basis of I is $\{xy - yz, xz - yz, z^2 - yz\}$.

i) Let σ be any term ordering such that $y >_\sigma z$ and $z >_\sigma x$. Show that the reduced σ-Gröbner basis of I is $\{z^2 - xz, yz - xz, xy - xz\}$.

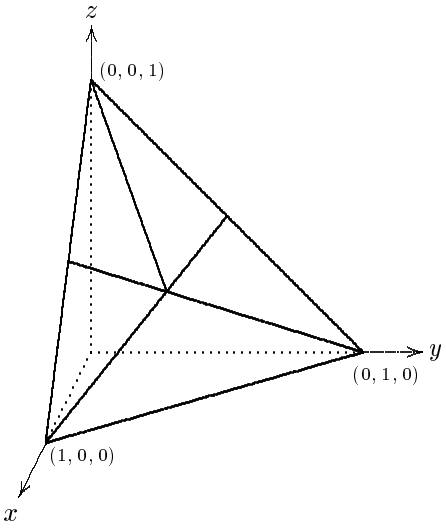
j) Consider the situation where σ is a term ordering such that $z >_\sigma x$ and $z >_\sigma y$. Show that there are only two possible reduced Gröbner bases of I, according as $x >_\sigma y$ or $y >_\sigma x$. Observe that in both cases the number of elements in the reduced Gröbner basis is four.

k) Prove there are exactly five reduced Gröbner bases of I.

l) Group the term orderings in five classes, depending on the inequalities considered before. Then find five term orderings which give rise to the five reduced Gröbner bases you found above.

m) Prove that for each of the five reduced Gröbner bases, there is an infinite set of term orderings σ such that it is the reduced σ-Gröbner basis of I.

n) Consider the description of term orderings by matrices explained in Section 1.4. Try to use it to interpret the following picture.



Tutorial 25: Some Optimizations of Buchberger's Algorithm

The purpose of this tutorial is to find and to implement optimized versions of Buchberger's Algorithm in the case of polynomial ideals. The amount of time consumed by a certain Gröbner basis computation depends largely on the number of pairs which have to be dealt with, and on the number of reduction steps which have to be performed in order to treat each pair. Therefore we will ask you to implement *counters* in your programs which measure these quantities, and we will judge our progress towards our goal of optimizing Buchberger's Algorithm by looking at the numbers returned by those counters.

Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $I \subseteq P$ be an ideal, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero polynomials which generate I. Furthermore, let σ be a term ordering, and let the elements $t_i, t_{ij} \in \mathbb{T}^n$, $\sigma_{ij} \in P^s$, and $S_{ij} \in P$ be defined as at the beginning of this section.

a) Update your CoCoA function `FirstGB(...)` from Tutorial 24 such that it returns not only a σ-Gröbner basis of I, but also the number of pairs (i, j) such that $S_{ij} \neq 0$, i.e. such that the normal remainder had to be computed, and the total number of reduction steps which were necessary to compute all those normal remainders.
Hint: You will have to modify the function `NormalRemainder(...)` from Tutorial 15 suitably.

b) Apply your new function `FirstGB(...)` in the following five cases. Each time, compute a Gröbner basis with respect to `DegRevLex` and one with respect to `Lex`.
1) $I = (x_1^2 - 2x_2^2 + 3x_1,\ x_1^3 - 2x_1x_2)$ in $\mathbb{Q}[x_1, x_2]$
2) $I = (x_1 - 2x_3^4,\ x_2 - 3x_3^5)$ in $\mathbb{Q}[x_1, x_2, x_3]$
3) $I = (x_1^2 - 2x_2^2,\ x_1^3 - 3x_3^3,\ x_1^4 - x_4^4)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$
4) $I = (x_1^3 - 4x_2^3,\ x_1^5 - 7x_3^5,\ x_1^7 - 11x_4^7)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$
5) $I = (x_1^2 + x_2^3 + x_3^3 - 1,\ x_1^3 + x_2^4 + x_3^5 - 1)$ in $\mathbb{Q}[x_1, x_2, x_3]$

c) Implement a CoCoA function `SecondGB(...)` which takes the list $\mathcal{G}$ and computes a σ-Gröbner basis of I via Buchberger's Algorithm 2.5.5, where the pair $(i, j) \in B$ is chosen in step 2) according to the normal selection strategy (see Remark 2.5.6.c), and where the optimization which follows from Proposition 2.5.8 is used.

d) Apply your function `SecondGB(...)` in the cases of b) and compare the results of your counters with those returned by the function `FirstGB(...)`.

e) Given $1 \leq i < j < k \leq s$, find three terms $t, t', t'' \in \mathbb{T}^n$ such that $t\sigma_{ij} + t'\sigma_{jk} + t''\sigma_{ik} = 0$. Prove that one can choose $t'' = 1$ if and only if t_k divides $\mathrm{lcm}(t_i, t_j)$. Give similar criteria for $t = 1$ and $t' = 1$. The triple (i, j, k) is called a **Buchberger triple** if one can choose $t = 1$ or $t' = 1$ or $t'' = 1$.

f) Prove that one can drop a pair (i,j) in the execution of Buchberger's Algorithm if it is contained in a Buchberger triple and if the other two pairs have been treated already. Write a CoCoA function `ThirdGB(...)` which is based on `SecondGB(...)` and adds this new optimization. To make sure that you do not drop more than one pair from a Buchberger triple, implement a list T which keeps track of the pairs which have been treated already.

g) Apply your function `ThirdGB(...)` in the cases of b) and determine the improvement which has been achieved.

h) Start again with your implementation `SecondGB(...)` of Buchberger's Algorithm, and replace step 4) by the following sequence of instructions.

4a) Increase s' by one. Append $g_i = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ to $\mathcal{G}$, and form the set $C = \{(i,s') \mid 1 \leq i < s',\ \gamma_i = \gamma_{s'}\}$.

4b) Delete in C all pairs (j,s') such that there exists an index i in $\{1,\ldots,s'-1\}$ with the properties that $i<j$ and $t_{s'i}$ divides $t_{s'j}$.

4c) Delete in C all pairs (i,s') such that there exists an index j in $\{1,\ldots,s'-1\}$ with the properties that $i<j$ and $t_{s'j}$ properly divides $t_{s'i}$.

4d) Delete in B all pairs (i,j) such that no divisibility occurs between $t_{s'i}$ and $t_{s'j}$ (hence both (i,s') and (j,s') survived the preceding two steps) and we have $\gcd(t_{is'}, t_{js'}) = 1$.

4e) Replace B by $B \cup C$ and continue with step 2).

The fact that this modified algorithm still computes a σ-Gröbner basis of M in finitely many steps will be studied in Volume 2. Implement it in a CoCoA function `GoodGB(...)`, apply this function in the cases of b), and compare the values returned by your counters with the earlier results.