PKR Lab-10 Solution

Algorithms

Algorithm 1: Multivariate Polynomial Division Algorithm

Input: $f, F = (f_1, \dots, f_s), \geq$ (monomial ordering)
Output: $(q_1, \dots, q_s), r$ such that $f = \sum_{i=1}^{s} q_i f_i + r$, $\mathrm{LT}_{\geq}(r)$ is not divisible by any of $\mathrm{LT}_{\geq}(f_i)$ or $r = 0$

$q_1 \leftarrow \cdots \leftarrow q_s \leftarrow r \leftarrow 0$
$p \leftarrow f$
while $p \neq 0$ **do**
  $i \leftarrow 1$
  divisionoccured $\leftarrow$ **False**
  while $i \leq s$ **and not** divisionoccured **do**
    if $\mathrm{LT}_{\geq}(f_i)$ divides $\mathrm{LT}_{\geq}(p)$ **then**
      $q_i \leftarrow q_i + \frac{\mathrm{LT}_{\geq}(p)}{\mathrm{LT}_{\geq}(f_i)}$
      $p \leftarrow p - \frac{\mathrm{LT}_{\geq}(p)}{\mathrm{LT}_{\geq}(f_i)} f_i$
      divisionoccured $\leftarrow$ **True**
    else
      $i \leftarrow i + 1$
  if not divisionoccured **then**
    $r \leftarrow r + \mathrm{LT}_{\geq}(p)$
    $p \leftarrow p - \mathrm{LT}_{\geq}(p)$
return $(q_1, \dots, q_s), r$

Algorithm 2: Improved Buchberger's Algorithm

Input: $F = (f_1, \dots, f_s), \geq$ (monomial ordering)
Output: Gröbner basis G of F w.r.t. $\geq$ monomial ordering

$t \leftarrow s$
$G \leftarrow F$
$B \leftarrow \{(i, j) \mid 1 \leq i < j \leq s\}$
while $B \neq \varnothing$ **do**
  Select $(i, j) \in B$
  $B \leftarrow B \setminus \{(i, j)\}$
  $r \leftarrow \overline{S_{\geq}(f_i, f_j)}^{(G, \geq)}$
  if $r \neq 0$ **then**
    $t \leftarrow t + 1$
    $f_t \leftarrow r$
    $G \leftarrow (f_1, \dots, f_t)$
    $B \leftarrow B \cup \{(i, t) \mid 1 \leq i \leq t - 1\}$
return G

Remark. *In the implementation of Buchberger's algorithm the notation $\overline{S_{\geq}(f_i, f_j)}^{(G, \geq)}$ for the monomial ordering $\geq$ is used. It simply denotes the remainder of the division of the S-polynomial of f_i and f_j w.r.t. $\geq$*

$$S_{\geq}(f_i, f_j) = \frac{\mathrm{LCM}\left(\mathrm{LM}_{\geq}(f_i), \mathrm{LM}_{\geq}(f_j)\right)}{\mathrm{LT}_{\geq}(f_i)} \cdot f_i - \frac{\mathrm{LCM}\left(\mathrm{LM}_{\geq}(f_i), \mathrm{LM}_{\geq}(f_j)\right)}{\mathrm{LT}_{\geq}(f_j)} \cdot f_j$$

by the ordered tuple of polynomials G w.r.t. $\geq$. In the expression for the S-polynomial, LCM *denotes the "least common multiple".*

Gröbner Basis Computation

Task 1. *Consider the polynomial system $F = (f_1, f_2) = (x^2 + y^2 - 1, y + x)$. Compute a lexicographic Gröbner basis G of F w.r.t. the variable ordering $x > y$.*

Solution: We apply Algorithm 2 which is a modified version of the improvement [1, Chapter 2, §10, Theorem 9] of the classical Buchberger's algorithm [1, Chapter 2, §7, Theorem 2]. First, we assign

$$t \leftarrow 2, \quad G \leftarrow (x^2 + y^2 - 1, y + x), \quad B \leftarrow \{(1, 2)\}.$$

We describe what happens to G and B during every iteration of the **while** block.

1. $G = (x^2+y^2-1, y+x)$, $B = \{(1, 2)\}$. For the only element $(i, j) = (1, 2) \in B$ we compute the S-polynomial

$$S_{\geq_{\text{lex}}}(f_i, f_j) = S_{\geq_{\text{lex}}}(f_1, f_2) = S_{\geq_{\text{lex}}}(x^2 + y^2 - 1, y + x) =$$
$$= \frac{\text{LCM}\left(\text{LM}_{\geq_{\text{lex}}}(x^2 + y^2 - 1), \text{LM}_{\geq_{\text{lex}}}(y + x)\right)}{\text{LT}_{\geq_{\text{lex}}}(x^2 + y^2 - 1)} \cdot (x^2+y^2-1) - \frac{\text{LCM}\left(\text{LM}_{\geq_{\text{lex}}}(x^2 + y^2 - 1), \text{LM}_{\geq_{\text{lex}}}(y + x)\right)}{\text{LT}_{\geq_{\text{lex}}}(y + x)} \cdot (y+x) =$$
$$= \frac{\text{LCM}\left(x^2, x\right)}{x^2} \cdot (x^2 + y^2 - 1) - \frac{\text{LCM}\left(x^2, x\right)}{x} \cdot (y + x) = \frac{x^2}{x^2} \cdot (x^2 + y^2 - 1) - \frac{x^2}{x} \cdot (y + x) =$$
$$= (x^2 + y^2 - 1) - x \cdot (y + x) = x^2 + y^2 - 1 - xy - x^2 = -xy + y^2 - 1$$

Now we compute the remainder of the division of $-xy + y^2 - 1$ by G w.r.t. $\geq_{\text{lex}}$ monomial ordering (using Algorithm 1):

$$\begin{aligned}
-xy + y^2 - 1 &= \underbrace{-xy + y^2 - 1}_{p} + \underbrace{0}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{0}_{q_2} \cdot (x + y) + \underbrace{0}_{r} \\
&= \underbrace{2y^2 - 1}_{p} + \underbrace{0}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{(-y)}_{q_2} \cdot (x + y) + \underbrace{0}_{r} \\
&= \underbrace{-1}_{p} + \underbrace{0}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{(-y)}_{q_2} \cdot (x + y) + \underbrace{2y^2}_{r} \\
&= \underbrace{0}_{p} + \underbrace{0}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{(-y)}_{q_2} \cdot (x + y) + \underbrace{2y^2 - 1}_{r}
\end{aligned}$$

Since $r = \overline{S_{\geq_{\text{lex}}}(f_1, f_2)}^{(G, \geq_{\text{lex}})} = 2y^2 - 1 \neq 0$, then we set $t \leftarrow 3$, $f_3 \leftarrow r$ and add $f_3 = 2y^2 - 1$ to the sequence G so it becomes $G = (x^2 + y^2 - 1, x + y, 2y^2 - 1)$. The set of tuples B at the end of the **while** block becomes $B = \{(1, 3), (2, 3)\}$. Since $B \neq \varnothing$, we repeat again the **while** block. We will further omit the symbol $\geq_{\text{lex}}$ everywhere for the sake of simplicity, since it is now clear what monomial ordering we are using.

2. $G = (x^2 + y^2 - 1, x + y, 2y^2 - 1)$, $B = \{(1, 3), (2, 3)\}$. We select $(1, 3) \in B$ and apply the same steps as in 1. :

$$S(f_1, f_3) = S(x^2 + y^2 - 1, 2y^2 - 1) = \frac{\text{LCM}\left(x^2, y^2\right)}{x^2} \cdot (x^2 + y^2 - 1) - \frac{\text{LCM}\left(x^2, y^2\right)}{2y^2} \cdot (2y^2 - 1) =$$
$$= \frac{x^2y^2}{x^2} \cdot (x^2 + y^2 - 1) - \frac{x^2y^2}{2y^2} \cdot (2y^2 - 1) = \tfrac{1}{2}x^2 + y^4 - y^2$$

$$\begin{aligned}
\tfrac{1}{2}x^2 + y^4 - y^2 &= \underbrace{\tfrac{1}{2}x^2 + y^4 - y^2}_{p} + \underbrace{0}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{0}_{q_2} \cdot (x + y) + \underbrace{0}_{q_3} \cdot (2y^2 - 1) + \underbrace{0}_{r} \\
&= \underbrace{y^4 - \tfrac{3}{2}y^2 + \tfrac{1}{2}}_{p} + \underbrace{\tfrac{1}{2}}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{0}_{q_2} \cdot (x + y) + \underbrace{0}_{q_3} \cdot (2y^2 - 1) + \underbrace{0}_{r} \\
&= \underbrace{-y^2 + \tfrac{1}{2}}_{p} + \underbrace{\tfrac{1}{2}}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{0}_{q_2} \cdot (x + y) + \underbrace{\left(\tfrac{1}{2}y^2\right)}_{q_3} \cdot (2y^2 - 1) + \underbrace{0}_{r} \\
&= \underbrace{0}_{p} + \underbrace{\tfrac{1}{2}}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{0}_{q_2} \cdot (x + y) + \underbrace{\left(\tfrac{1}{2}y^2 - \tfrac{1}{2}\right)}_{q_3} \cdot (2y^2 - 1) + \underbrace{0}_{r}
\end{aligned}$$

Since $r = 0$, then we update only B and it becomes $B = \{(2,3)\}$. Since $B \neq \varnothing$, we repeat the **while** block.

3. $G = (x^2 + y^2 - 1, x + y, 2y^2 - 1)$, $B = \{(2,3)\}$. For $(2,3) \in B$ we obtain:

$$S(f_2, f_3) = S(x + y, 2y^2 - 1) = \frac{xy^2}{x} \cdot (x + y) - \frac{xy^2}{2y^2} \cdot (2y^2 - 1) = \tfrac{1}{2}x + y^3$$

$$\begin{aligned}
\tfrac{1}{2}x + y^3 &= \underbrace{\tfrac{1}{2}x + y^3}_{p} + \underbrace{0}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{0}_{q_2} \cdot (x + y) + \underbrace{0}_{q_3} \cdot (2y^2 - 1) + \underbrace{0}_{r} \\
&= \underbrace{y^3 - \tfrac{1}{2}y}_{p} + \underbrace{0}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{\tfrac{1}{2}}_{q_2} \cdot (x + y) + \underbrace{0}_{q_3} \cdot (2y^2 - 1) + \underbrace{0}_{r} \\
&= \underbrace{0}_{p} + \underbrace{0}_{q_1} \cdot (x^2 + y^2 - 1) + \underbrace{\tfrac{1}{2}}_{q_2} \cdot (x + y) + \underbrace{\tfrac{1}{2}y}_{q_3} \cdot (2y^2 - 1) + \underbrace{0}_{r}
\end{aligned}$$

Since $r = 0$, then we update only B and it becomes $B = \varnothing$. Since $B = \varnothing$, we finish here and return a Gröbner basis $G = (x^2 + y^2 - 1, x + y, 2y^2 - 1)$ of F.

□

Solving lexicographic GB by back-substitution

Definition 1. *A polynomial system $G = (g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n))$ is said to be* ***triangular*** *w.r.t. a variable ordering $x_1 > \cdots > x_n$ if there exist a partition of G into non-empty blocks $\{B_1, \ldots, B_n\}$ such that*

$$\text{variables}(B_j) = \{x_j, x_{j+1}, \ldots, x_n\}$$

Example 1. *Consider G given by*

$$G = (x_1^2 x_2 + x_3, x_3^2 + x_1, x_2 x_3 + 1, x_2 + x_3, x_3^2 + 1).$$

We can partition G as

$$B_1 = \{x_1^2 x_2 + x_3, x_3^2 + x_1\}, \quad B_2 = \{x_2 x_3 + 1, x_2 + x_3\}, \quad B_3 = \{x_3^2 + 1\}$$

with

$$\text{variables}(B_1) = \{x_1, x_2, x_3\}, \quad \text{variables}(B_2) = \{x_2, x_3\}, \quad \text{variables}(B_3) = \{x_3\}.$$

Such triangular systems can be solved by back-substitution. For the back-substitution we proceed by solving consequtively the blocks B_j starting from B_n according to the following sequence of steps:

1. Find the set of solutions S_n to $B_n = \mathbf{0}$.
2. Set j to n.
3. For every $s = (s_j, \ldots, s_n) \in S_j$ construct a solution set $T_{s,j-1}$ of $C_{j-1} = \{f(x_{j-1}, s) \mid f \in B_{j-1}\}$.
4. Extend $\{T_{s,j-1} \mid s \in S_j\}$ to the solution set of $\cup_{k=j-1}^{n} B_k$:

$$S_{j-1} = \{(s_{j-1}, s) \mid s \in S_j, s_{j-1} \in T_{s,j-1}\}.$$

5. If $j - 1 \geq 2$, go to step 3. for S_{j-1}. Otherwise return the solution set S_{j-1} of G.

Task 2. *Compute the solutions to the lexicographic Gröbner basis $G = (x^2 + y^2 - 1, x + y, 2y^2 - 1)$ from the previous task using back-substitution.*

Solution: We can see that G is triangular w.r.t. a variable ordering $x > y$, since G can be partitioned into blocks as

$$B_1 = \{x^2 + y^2 - 1, x + y\}, \quad B_2 = \{2y^2 - 1\}$$

so that

$$\text{variables}(B_1) = \{x, y\}, \quad \text{variables}(B_2) = \{y\}.$$

Applying the back-substitution we obtain:

1. First, compute the solutions to $2y^2 - 1 = 0$: these are $\pm\frac{1}{\sqrt{2}}$.
2. Substitute every solution of $2y^2 - 1 = 0$ to the system $\{x^2 + y^2 - 1, x + y\}$ and compute the solutions in x.
   (a) $y = \frac{1}{\sqrt{2}}$, then we solve

   $$\begin{cases} x^2 - \frac{1}{2} = 0 \\ x + \frac{1}{\sqrt{2}} = 0 \end{cases} \iff x = -\frac{1}{\sqrt{2}}.$$

   Hence, we get the solution $(x, y) = (-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$.

   (b) $y = -\frac{1}{\sqrt{2}}$, then we solve

   $$\begin{cases} x^2 - \frac{1}{2} = 0 \\ x - \frac{1}{\sqrt{2}} = 0 \end{cases} \iff x = \frac{1}{\sqrt{2}}.$$

   Hence, we get the solution $(x, y) = (\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$.

The set of solutions to G is

$$\left\{(-\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}), (\tfrac{1}{\sqrt{2}}, -\tfrac{1}{\sqrt{2}})\right\}.$$

□

References

[1] David A. Cox, John B. Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, Springer, 2015, Fourth Edition.