Computing lexicographic groebner basis

December 5, 2021

Algorithm 1: Polynomial Division Algorithm

Input: $f, F = (f_1, \ldots, f_s), \geq$ (monomial ordering)
Output: $(q_1, \ldots, q_s), r$ 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** divisionoccured $= FALSE$ **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 divisionoccured $= FALSE$ **then**
    $r \leftarrow r + \mathrm{LT}_{\geq}(p)$
    $p \leftarrow p - \mathrm{LT}_{\geq}(p)$
return $(q_1, \ldots, q_s), r$

Algorithm 2: Buchberger Algorithm

Input: $F = (f_1, \ldots, f_s), \geq$ (monomial ordering)
Output: Groebner basis $G = (g_1, \ldots, g_t)$ w.r.t. $\geq$ monomial ordering

$G \leftarrow F$
repeat
  $G' \leftarrow G$
  foreach $\{p, q\} \subseteq G',\ p \neq q$ **do**
    $S \leftarrow \overline{S(p,q)}^{G'}_{\geq}$
    if $S \neq 0$ **then**
      $G \leftarrow G \cup \{S\}$
until $G \neq G'$
return G

Task 1. *Consider the polynomial system $F = (xy - 1, x^2 - y)$. Compute a lexicographic groebner basis G of F w.r.t. the variable ordering $x > y$ and retrieve the solutions to F from G.*

Solution: We will apply (a little bit modified version of) Buchberger algorithm. First, we assign $(xy-1, x^2-y)$ to G. I will describe what happens to G and G' during every iteration of the **repeat** block.

1. $G' = (xy - 1, x^2 - y)$. For the only subset $\{p, q\} = \{xy - 1, x^2 - y\} \subseteq G'$ with $p \neq q$ we compute the S-polynomial

$$S(p,q) = S(xy-1, x^2-y) =$$
$$= \frac{\text{LCM}\left(\text{LM}(xy-1), \text{LM}(x^2-y)\right)}{\text{LT}(xy-1)} \cdot (xy-1) - \frac{\text{LCM}\left(\text{LM}(xy-1), \text{LM}(x^2-y)\right)}{\text{LT}(x^2-y)} \cdot (x^2-y) =$$
$$= \frac{\text{LCM}\left(xy, x^2\right)}{xy} \cdot (xy-1) - \frac{\text{LCM}\left(xy, x^2\right)}{x^2} \cdot (x^2-y) = \frac{x^2y}{xy} \cdot (xy-1) - \frac{x^2y}{x^2} \cdot (x^2-y) =$$
$$= x \cdot (xy-1) - y \cdot (x^2-y) = x^2y - x - x^2y + y^2 = y^2 - x$$

   Now we reduce $y^2 - x$ by the sequence G' (using the algorithm of polynomial division):

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

   Since $S = \overline{S(p,q)}^{G'}_{\geq} = y^2 - x \neq 0$, then we add it to the sequence G and it becomes $G = (xy - 1, x^2 - y, y^2 - x)$. Further, since

$$(xy - 1, x^2 - y, y^2 - x) = G \neq G' = (xy - 1, x^2 - y)$$

   we repeat again the **repeat** block.

2. $G' = (xy - 1, x^2 - y, y^2 - x)$. There are in total $\binom{3}{2} = \frac{3!}{2!1!} = 3$ different subsets $\{p, q\} \subseteq G'$ with $p \neq q$. We take the first one $\{p, q\} = \{xy - 1, x^2 - y\} \subseteq G'$ and apply the same steps as in 1. :

$$S(p,q) = y^2 - x$$
$$y^2 - x = \underbrace{y^2 - x}_{p} + \underbrace{0}_{q_1} \cdot (xy-1) + \underbrace{0}_{q_2} \cdot (x^2-y) + \underbrace{0}_{q_3} \cdot (y^2-x) + \underbrace{0}_{r}$$
$$= \underbrace{0}_{p} + \underbrace{0}_{q_1} \cdot (xy-1) + \underbrace{0}_{q_2} \cdot (x^2-y) + \underbrace{1}_{q_3} \cdot (y^2-x) + \underbrace{0}_{r}$$

   Since $S = \overline{S(p,q)}^{G'}_{\geq} = 0$, then we don't add it to the sequence G.

   We now take the second pair $\{p, q\} = \{xy - 1, y^2 - x\} \subseteq G'$:

$$S(p,q) = S(xy-1, y^2-x) = \frac{xy}{xy} \cdot (xy-1) - \frac{xy}{-x} \cdot (y^2-x) = xy - 1 + y^3 - xy = y^3 - 1$$
$$y^3 - 1 = \underbrace{y^3 - 1}_{p} + \underbrace{0}_{q_1} \cdot (xy-1) + \underbrace{0}_{q_2} \cdot (x^2-y) + \underbrace{0}_{q_3} \cdot (y^2-x) + \underbrace{0}_{r}$$
$$= \underbrace{0}_{p} + \underbrace{0}_{q_1} \cdot (xy-1) + \underbrace{0}_{q_2} \cdot (x^2-y) + \underbrace{0}_{q_3} \cdot (y^2-x) + \underbrace{y^3 - 1}_{r}$$

   Since $S = \overline{S(p,q)}^{G'}_{\geq} = y^3 - 1 \neq 0$, then we add it to the sequence G and it becomes $G = (xy - 1, x^2 - y, y^2 - x, y^3 - 1)$.

   We now take the last pair $\{p, q\} = \{x^2 - y, y^2 - x\} \subseteq G'$:

$$S(p,q) = S(x^2-y, y^2-x) = \frac{x^2}{x^2} \cdot (x^2-y) - \frac{x^2}{-x} \cdot (y^2-x) = x^2 - y - x^2 + xy^2 = xy^2 - y$$

$$xy^2 - y = \underbrace{xy^2 - y}_{p} + \underbrace{0}_{q_1} \cdot (xy - 1) + \underbrace{0}_{q_2} \cdot (x^2 - y) + \underbrace{0}_{q_3} \cdot (y^2 - x) + \underbrace{0}_{r}$$
$$= \underbrace{0}_{p} + \underbrace{y}_{q_1} \cdot (xy - 1) + \underbrace{0}_{q_2} \cdot (x^2 - y) + \underbrace{0}_{q_3} \cdot (y^2 - x) + \underbrace{0}_{r}$$

Since $S = \overline{S(p,q)}_{\geq}^{G'} = 0$, then we don't add it to the sequence G.

Finally, we are at the end of the **repeat** block and since

$$(xy - 1, x^2 - y, y^2 - x, y^3 - 1) = G \neq G' = (xy - 1, x^2 - y, y^2 - x)$$

we need to repeat again the **repeat** block.

3. $G' = (xy - 1, x^2 - y, y^2 - x, y^3 - 1)$. There are in total $\binom{4}{2} = \frac{4!}{2!2!} = 6$ different subsets $\{p, q\} \subseteq G'$ with $p \neq q$, i.e. the computations by hand are becoming already time-consuming. We will use the following modification of the Buchberger algorithm in order to simplify the computations. We can notice that

$$xy - 1 = (-y) \cdot (y^2 - x) + 1 \cdot (y^3 - 1),$$

i.e. $xy - 1 \in G'$ is a polynomial combination of another two polynomials $y^2 - x, y^3 - 1$ from G'. That's why if we remove $xy - 1$ from G', then the resulting polynomial system $(x^2 - y, y^2 - x, y^3 - 1)$ defines the same ideal as G' (the set of solutions to those 2 polynomial systems is the same) and hence it will be sufficient to find a Groebner basis for $(x^2 - y, y^2 - x, y^3 - 1)$ and it will also be a Groebner basis for G'.

Hence we go through the **repeat** block for $G = G' = (x^2 - y, y^2 - x, y^3 - 1)$. There are in total $\binom{3}{2} = \frac{3!}{2!1!} = 3$ different subsets $\{p, q\} \subseteq G'$ with $p \neq q$.

We take the first one $\{p, q\} = \{x^2 - y, y^2 - x\} \subseteq G'$:

$$S(p,q) = S(x^2 - y, y^2 - x) = xy^2 - y$$
$$xy^2 - y = \underbrace{xy^2 - y}_{p} + \underbrace{0}_{q_1} \cdot (x^2 - y) + \underbrace{0}_{q_2} \cdot (y^2 - x) + \underbrace{0}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r}$$
$$= \underbrace{y^4 - y}_{p} + \underbrace{0}_{q_1} \cdot (x^2 - y) + \underbrace{(-y^2)}_{q_2} \cdot (y^2 - x) + \underbrace{0}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r}$$
$$= \underbrace{0}_{p} + \underbrace{0}_{q_1} \cdot (x^2 - y) + \underbrace{(-y^2)}_{q_2} \cdot (y^2 - x) + \underbrace{y}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r}$$

Since $S = \overline{S(p,q)}_{\geq}^{G'} = 0$, then we don't add it to the sequence G.

We take the second pair $\{p, q\} = \{x^2 - y, y^3 - 1\} \subseteq G'$:

$$S(p,q) = S(x^2 - y, y^3 - 1) = \frac{x^2y^3}{x^2} \cdot (x^2 - y) - \frac{x^2y^3}{y^3} \cdot (y^3 - 1) = x^2y^3 - y^4 - x^2y^3 + x^2 = x^2 - y^4$$
$$x^2 - y^4 = \underbrace{x^2 - y^4}_{p} + \underbrace{0}_{q_1} \cdot (x^2 - y) + \underbrace{0}_{q_2} \cdot (y^2 - x) + \underbrace{0}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r}$$
$$= \underbrace{-y^4 + y}_{p} + \underbrace{1}_{q_1} \cdot (x^2 - y) + \underbrace{0}_{q_2} \cdot (y^2 - x) + \underbrace{0}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r}$$
$$= \underbrace{0}_{p} + \underbrace{1}_{q_1} \cdot (x^2 - y) + \underbrace{0}_{q_2} \cdot (y^2 - x) + \underbrace{(-y)}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r}$$

Since $S = \overline{S(p,q)}_{\geq}^{G'} = 0$, then we don't add it to the sequence G.

We take the last pair $\{p, q\} = \{y^2 - x, y^3 - 1\} \subseteq G'$:

$$S(p,q) = S(y^2 - x, y^3 - 1) = \frac{xy^3}{-x} \cdot (y^2 - x) - \frac{xy^3}{y^3} \cdot (y^3 - 1) = -y^5 + xy^3 - xy^3 + x = x - y^5$$

$$\begin{aligned} x - y^5 &= \underbrace{x - y^5}_{p} + \underbrace{0}_{q_1} \cdot (x^2 - y) + \underbrace{0}_{q_2} \cdot (y^2 - x) + \underbrace{0}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r} \\ &= \underbrace{-y^5 + y^2}_{p} + \underbrace{0}_{q_1} \cdot (x^2 - y) + \underbrace{(-1)}_{q_2} \cdot (y^2 - x) + \underbrace{0}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r} \\ &= \underbrace{0}_{p} + \underbrace{0}_{q_1} \cdot (x^2 - y) + \underbrace{(-1)}_{q_2} \cdot (y^2 - x) + \underbrace{(-y^2)}_{q_3} \cdot (y^3 - 1) + \underbrace{0}_{r} \end{aligned}$$

Since $S = \overline{S(p,q)}_{\geq}^{G'} = 0$, then we don't add it to the sequence G.

We are now at the end of the **repeat** block and since

$$(x^2 - y, y^2 - x, y^3 - 1) = G = G' = (x^2 - y, y^2 - x, y^3 - 1)$$

we finish here and return a Groebner basis $G = (x^2 - y, y^2 - x, y^3 - 1)$ of $F = (xy - 1, x^2 - y)$.

We compute the solutions to $G = (x^2 - y, y^2 - x, y^3 - 1)$ as follows:

1. First, compute the solutions to $y^3 - 1 = 0$: these are the cubic roots of unity $1, e^{2\pi i \frac{1}{3}}, e^{2\pi i \frac{2}{3}}$.
2. Substitute every solution of $y^3 - 1 = 0$ to the system $(x^2 - y, y^2 - x)$ and compute the solutions in x.
   (a) $y = 1$, then we solve
   $$\begin{cases} x^2 - 1 \\ 1 - x \end{cases} \iff x = 1.$$
   Hence, we get the solution $(x, y) = (1, 1)$.
   (b) $y = e^{2\pi i \frac{1}{3}}$, then we solve
   $$\begin{cases} x^2 - e^{2\pi i \frac{1}{3}} \\ e^{2\pi i \frac{2}{3}} - x \end{cases} \iff x = e^{2\pi i \frac{2}{3}}.$$
   Hence, we get the solution $(x, y) = (e^{2\pi i \frac{2}{3}}, e^{2\pi i \frac{1}{3}})$.
   (c) $y = e^{2\pi i \frac{2}{3}}$, then we solve
   $$\begin{cases} x^2 - e^{2\pi i \frac{2}{3}} \\ e^{2\pi i \frac{1}{3}} - x \end{cases} \iff x = e^{2\pi i \frac{1}{3}}.$$
   Hence, we get the solution $(x, y) = (e^{2\pi i \frac{1}{3}}, e^{2\pi i \frac{2}{3}})$.

The set of complex solutions to F is

$$\left\{(1,1), (e^{2\pi i \frac{2}{3}}, e^{2\pi i \frac{1}{3}}), (e^{2\pi i \frac{1}{3}}, e^{2\pi i \frac{2}{3}})\right\}.$$

The set of real solutions to F is

$$\{(1,1)\}.$$

□