Computing lexicographic Gröbner basis

November 21, 2022

Algorithm 1: Multivariate 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 ← ··· ← q_s ← r ← 0
p ← f
while p ≠ 0 do
    i ← 1
    divisionoccured ← FALSE
    while i ≤ s and divisionoccured = FALSE do
        if LT_≥(f_i) divides LT_≥(p) then
            q_i ← q_i + LT_≥(p) / LT_≥(f_i)
            p ← p − (LT_≥(p) / LT_≥(f_i)) f_i
            divisionoccured ← TRUE
        else
            i ← i + 1
    if divisionoccured = FALSE then
        r ← r + LT_≥(p)
        p ← p − LT_≥(p)
return (q_1, ..., q_s), r
```

Algorithm 2: Buchberger's Algorithm

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

```
t ← s
G ← F
B ← {(i, j) | 1 ≤ i < j ≤ s}
while B ≠ ∅ do
    Select (i, j) ∈ B
    r ← overline(S_≥(f_i, f_j))^(G,≥)
    if r ≠ 0 then
        t ← t + 1
        f_t ← r
        G ← (f_1, ..., f_t)
        B ← B ∪ {(i, t) | 1 ≤ i ≤ t − 1}
    B ← B \ {(i, j)}
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.* $\geq$.

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

Solution: We will 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 $t \leftarrow 2, G \leftarrow (xy-1, x^2-y), B \leftarrow \{(1,2)\}$. We describe what happens to G and B during every iteration of the **while** block.

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

$$S_{\geq_{\mathrm{lex}}}(f_i, f_j) = S_{\geq_{\mathrm{lex}}}(f_1, f_2) = S_{\geq_{\mathrm{lex}}}(xy - 1, x^2 - y) =$$

$$= \frac{\mathrm{LCM}\left(\mathrm{LM}_{\geq_{\mathrm{lex}}}(xy-1), \mathrm{LM}_{\geq_{\mathrm{lex}}}(x^2-y)\right)}{\mathrm{LT}_{\geq_{\mathrm{lex}}}(xy-1)} \cdot (xy-1) - \frac{\mathrm{LCM}\left(\mathrm{LM}_{\geq_{\mathrm{lex}}}(xy-1), \mathrm{LM}_{\geq_{\mathrm{lex}}}(x^2-y)\right)}{\mathrm{LT}_{\geq_{\mathrm{lex}}}(x^2-y)} \cdot (x^2-y) =$$

$$= \frac{\mathrm{LCM}\left(xy, x^2\right)}{xy} \cdot (xy-1) - \frac{\mathrm{LCM}\left(xy, x^2\right)}{x^2} \cdot (x^2-y) = \frac{x^2y}{xy} \cdot (xy-1) - \frac{x^2y}{x^2} \cdot (x^2-y) =$$

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

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

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

Since $r = \overline{S_{\geq_{\mathrm{lex}}}(f_1, f_2)}^{(G,\geq_{\mathrm{lex}})} = y^2 - x \neq 0$, then we set $t \leftarrow 3$, $f_3 \leftarrow r$ and add $f_3 = y^2 - x$ to the sequence G so it becomes $G = (xy - 1, x^2 - y, y^2 - x)$. 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 $\geq_{\mathrm{lex}}$ everywhere for the sake of simplicity, since it is now clear what monomial ordering we are using.

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

$$S(f_1, f_3) = S(xy - 1, y^2 - x) = \frac{\mathrm{LCM}\left(xy, x\right)}{xy} \cdot (xy-1) - \frac{\mathrm{LCM}\left(xy, x\right)}{-x} \cdot (y^2-x) =$$

$$= \frac{xy}{xy} \cdot (xy-1) - \frac{xy}{-x} \cdot (y^2-x) = y^3 - 1$$

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

Since $r \neq 0$, then we set $t \leftarrow 4$, $f_4 \leftarrow r$ and add $f_4 = y^3 - 1$ to the sequence G and it becomes $G = (xy - 1, x^2 - y, y^2 - x, y^3 - 1)$. The set of tuples B at the end of the **while** block becomes $B = \{(2, 3), (1, 4), (2, 4), (3, 4)\}$. Since $B \neq \varnothing$, we repeat the **while** block.

3. $G = (xy-1, x^2-y, y^2-x, y^3-1)$, $B = \{(2,3),(1,4),(2,4),(3,4)\}$. For $(2,3) \in B$ we obtain:

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

$$\begin{aligned} xy^2-y &= \underbrace{xy^2-y}_{p} + \underbrace{0}_{q_1}\cdot(xy-1) + \underbrace{0}_{q_2}\cdot(x^2-y) + \underbrace{0}_{q_3}\cdot(y^2-x) + \underbrace{0}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \\ &= \underbrace{0}_{p} + \underbrace{y}_{q_1}\cdot(xy-1) + \underbrace{0}_{q_2}\cdot(x^2-y) + \underbrace{0}_{q_3}\cdot(y^2-x) + \underbrace{0}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \end{aligned}$$

Since $r=0$, then we update only B and it becomes $B = \{(1,4),(2,4),(3,4)\}$. Since $B \neq \varnothing$, we repeat the **while** block.

4. $G = (xy-1, x^2-y, y^2-x, y^3-1)$, $B = \{(1,4),(2,4),(3,4)\}$. For $(1,4) \in B$ we obtain:

$$S(f_1,f_4) = S(xy-1, y^3-1) = \frac{xy^3}{xy}\cdot(xy-1) - \frac{xy^3}{y^3}\cdot(y^3-1) = y^2\cdot(xy-1) - x\cdot(y^3-1) = x-y^2$$

$$\begin{aligned} x-y^2 &= \underbrace{x-y^2}_{p} + \underbrace{0}_{q_1}\cdot(xy-1) + \underbrace{0}_{q_2}\cdot(x^2-y) + \underbrace{0}_{q_3}\cdot(y^2-x) + \underbrace{0}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \\ &= \underbrace{0}_{p} + \underbrace{y}_{q_1}\cdot(xy-1) + \underbrace{0}_{q_2}\cdot(x^2-y) + \underbrace{(-1)}_{q_3}\cdot(y^2-x) + \underbrace{0}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \end{aligned}$$

Since $r=0$, then we update only B and it becomes $B = \{(2,4),(3,4)\}$. Since $B \neq \varnothing$, we repeat the **while** block.

5. $G = (xy-1, x^2-y, y^2-x, y^3-1)$, $B = \{(2,4),(3,4)\}$. For $(2,4) \in B$ we obtain:

$$S(f_2,f_4) = S(x^2-y, y^3-1) = \frac{x^2y^3}{x^2}\cdot(x^2-y) - \frac{x^2y^3}{y^3}\cdot(y^3-1) = y^3\cdot(x^2-y) - x^2\cdot(y^3-1) = x^2-y^4$$

$$\begin{aligned} x^2-y^4 &= \underbrace{x^2-y^4}_{p} + \underbrace{0}_{q_1}\cdot(xy-1) + \underbrace{0}_{q_2}\cdot(x^2-y) + \underbrace{0}_{q_3}\cdot(y^2-x) + \underbrace{0}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \\ &= \underbrace{y-y^4}_{p} + \underbrace{0}_{q_1}\cdot(xy-1) + \underbrace{1}_{q_2}\cdot(x^2-y) + \underbrace{0}_{q_3}\cdot(y^2-x) + \underbrace{0}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \\ &= \underbrace{0}_{p} + \underbrace{0}_{q_1}\cdot(xy-1) + \underbrace{1}_{q_2}\cdot(x^2-y) + \underbrace{0}_{q_3}\cdot(y^2-x) + \underbrace{(-y)}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \end{aligned}$$

Since $r=0$, then we update only B and it becomes $B = \{(3,4)\}$. Since $B \neq \varnothing$, we repeat the **while** block.

6. $G = (xy-1, x^2-y, y^2-x, y^3-1)$, $B = \{(3,4)\}$. For $(3,4) \in B$ we obtain:

$$S(f_3,f_4) = S(y^2-x, y^3-1) = \frac{xy^3}{-x}\cdot(y^2-x) - \frac{xy^3}{y^3}\cdot(y^3-1) = (-y^3)\cdot(y^2-x) - x\cdot(y^3-1) = -y^5+x$$

$$\begin{aligned} -y^5+x &= \underbrace{-y^5+x}_{p} + \underbrace{0}_{q_1}\cdot(xy-1) + \underbrace{0}_{q_2}\cdot(x^2-y) + \underbrace{0}_{q_3}\cdot(y^2-x) + \underbrace{0}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \\ &= \underbrace{-y^5+y^2}_{p} + \underbrace{0}_{q_1}\cdot(xy-1) + \underbrace{0}_{q_2}\cdot(x^2-y) + \underbrace{(-1)}_{q_3}\cdot(y^2-x) + \underbrace{0}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \\ &= \underbrace{0}_{p} + \underbrace{0}_{q_1}\cdot(xy-1) + \underbrace{0}_{q_2}\cdot(x^2-y) + \underbrace{(-1)}_{q_3}\cdot(y^2-x) + \underbrace{(-y^2)}_{q_4}\cdot(y^3-1) + \underbrace{0}_{r} \end{aligned}$$

Since $r=0$, then we update only B and it becomes $B = \varnothing$. Since $B = \varnothing$, we finish here and return a Gröbner basis $G = (xy-1, x^2-y, y^2-x, y^3-1)$ of F.

We compute the solutions to $G = (xy-1, x^2-y, y^2-x, y^3-1)$ 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 $(xy - 1, x^2 - y, y^2 - x)$ and compute the solutions in x.
   (a) $y = 1$, then we solve
   $$\begin{cases} x - 1 = 0 \\ x^2 - 1 = 0 \\ 1 - x = 0 \end{cases} \iff x = 1.$$
   Hence, we get the solution $(x, y) = (1, 1)$.
   (b) $y = e^{2\pi i \frac{1}{3}}$, then we solve
   $$\begin{cases} e^{2\pi i \frac{1}{3}} x - 1 = 0 \\ x^2 - e^{2\pi i \frac{1}{3}} = 0 \\ e^{2\pi i \frac{2}{3}} - x = 0 \end{cases} \iff x = e^{2\pi i \frac{2}{3}}.$$
   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
   $$\begin{cases} e^{2\pi i \frac{1}{3}} x - 1 = 0 \\ x^2 - e^{2\pi i \frac{2}{3}} = 0 \\ e^{2\pi i \frac{1}{3}} - x = 0 \end{cases} \iff x = e^{2\pi i \frac{1}{3}}.$$
   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

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

$\square$

References

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