On Cores of Ideals with Empty Variety

February 21, 2016

Let $F = \{f_1, f_2, \ldots, f_m\}$ be a set of m polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$ and $I = (F)$ the ideal generated by the set F. Assume that our term order is LEX with $x_1 > x_2 > ... > x_n$. Suppose that it is known that $V(I) = \emptyset$.

We can now apply the Buchberger's algorithm [1] to the system of generators F of I.

Next, we will keep track of the S-polynomials that give non-zero remainder when divided by the system of generators of I at that moment.

$$g_{ij} := S(f_i, f_j) - \sum_{k=1}^{l} c_k f_k,$$

where $0 \neq c_k \in \mathbb{F}_2[x_1, \ldots, x_n]$ and $\{f_1, \ldots, f_l\}$ is the current system of generators of I.

For each non-zero g_{ij}, we will record the following data:

$$((g_{ij})(f_i, f_j)(h_{ij}, h_{ji})|(f_1, \ldots, f_l), (c_1, \ldots, c_l))$$

Note that here g_{ij} denotes the remainder of the S-polynomial $S(f_i, f_j)$ modulo the current system of generators $f_1, \ldots, f_l$ of the ideal I and we denote by

$$h_{ij} := \frac{\text{lcm}(\text{in}_<(f_i), \text{in}_<(f_j))}{\text{LT}_<(f_i)}, h_{ji} := \frac{\text{lcm}(\text{in}_<(f_i), \text{in}_<(f_j))}{\text{LT}_<(f_j)}$$

the coefficients of f_i, respectively f_j in the S-polynomial $S(f_i, f_j)$.

I recall that we have

$$S(f_i, f_j) = \frac{\text{lcm}(\text{in}_<(f_i), \text{in}_<(f_j))}{\text{LT}_<(f_i)} f_i - \frac{\text{lcm}(\text{in}_<(f_i), \text{in}_<(f_j))}{\text{LT}_<(f_j)} f_j$$

.

The last part contains the f_i's that appear in the division process and the second parentheses has the corresponding coefficients.

When we obtain 1 as a remainder of a S-polynomial to the current system of generators, we stop.

As an output of the Buckberger's Algorithm, we can obtain not only the Gröbner bases, let's call it $\{g_1, \ldots, g_t\}$, but also a matrix M such that

$$\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_t \end{bmatrix} = M \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{bmatrix} \tag{1}$$

Theorem 0.1. *With the notations above, we have that a core for the system of generators F of the ideal I is given by the union of those f_i's from F that appear in the data recorded above and correspond to the nonzero entries in the matrix M.*

Proof. In our case, $g_1 = 1$ and $t = 1$, since the variety is empty, and hence the ideal is the unit ideal. Say $M = [a_1, \ldots, a_m]$. Then the output of the algorithm gives

$$1 = a_1 f_1 + \cdots + a_m f_m.$$

Clearly, if $a_i = 0$ for some i then f_i does not appear in this equation and should not be included in the core.

□

Our next goal will be to describe an algorithm that allows us to compute a core of the ideal and the matrix M.

INITIAL DATA: $S_0 = \{f_1, \ldots, f_m\}$ system of generators of the ideal I, monomial order $<$ on $\mathbb{F}_2[x_1, \ldots, x_n]$.

STEP 1: We start computing the S-polynomials of the system of generators $\{f_1, \ldots, f_m\}$ as in the Buchberger's algorithm [1]. After computing the first one, we divide it by the system of generators S_0. In this way, we will obtain the following expression

$$g_{i_1 i_2} := h_{i_1 i_2} f_{i_1} - h_{i_2 i_1} f_{i_2} - \sum_{k=1}^{m} c_k f_k$$

If the remainder $g_{i_1 i_2}$ is non-zero, we will denote it by f_{m+1} and we will add it to our initial system of generators. We will also record the data as follows

$$((f_{m+1} := g_{i_1 i_2})(f_{i_1}, f_{i_2})(h_{i_1 i_2}, h_{i_2 i_1})|(f_1, \ldots, f_m), (c_1, \ldots, c_m))$$

Then we will consider $S_1 := \{f_1, \ldots, f_m, f_{m+1}\}$ to be the new system of generators of I.

STEP s: If $S_s := \{f_1, \ldots, f_s\}$ is the current system of generators of I and we have the following relation for f_s

$$f_s = g_{ij} = h_{ij} f_i - h_{ji} f_j - \sum_{k=1}^{s-1} a_k f_k$$

and the recorded data

$$((f_s := g_{ij})(f_i, f_j)(h_{ij}, h_{ji})|(f_1, \ldots, f_{s-1}), (a_1, \ldots, a_{s-1}))$$

We will compute the next S-polynomial which gives a non-zero remainder when divided by our current system of generators S_s

$$f_{s+1} = g_{pq} = h_{pq}f_p - h_{qp}f_q - \sum_{k=1}^{s} b_k f_k$$

By substituting f_s in the expression of f_{s+1} we get

$$f_{s+1} = h_{pq}f_p - h_{qp}f_q - \sum_{k=1}^{s-1} b_k f_k - b_s(h_{ij}f_i - h_{ji}f_j - \sum_{k=1}^{s-1} a_k f_k)$$

$$= h_{pq}f_p - h_{qp}f_q - \sum_{k=1}^{s-1} b_k f_k - b_s h_{ij}f_i + b_s h_{ji}f_j + \sum_{k=1}^{s-1} b_s a_k f_k$$

$$= h_{pq}f_p - h_{qp}f_q - b_s h_{ij}f_i + b_s h_{ji}f_j + \sum_{k=1}^{s-1}(b_s a_k - b_k) f_k$$

Next, we will record the data for f_{s+1}

$$((f_{s+1} := g_{pq})(f_p, f_q)(h_{pq}, h_{qp})|(f_1, \ldots, f_{s-1}, f_i, f_j), (b_s a_1 - b_1, \ldots, b_s a_{s-1} - b_{s-1}, b_s h_{ij}, b_s h_{ji}))$$

The algorithm will stop when we will obtain the last non-zero remainder $f_l = 1$. After using the previous relations, we will have the following

$$1 = f_l = \sum_{k=1}^{m} d_k f_k$$

OUTPUT: the core of the system of generators S_0 is $\{f_k : k \in \overline{1, m}, d_k \neq 0\}$
the matrix with the coefficients

$$M = (d_1, \ldots, d_k)$$

.

Example 0.1.1. *Consider the following set of polynomials:*

$$f_1 : abc + ab + ac + bc + a + b + c + 1$$

$$f_2 : b$$

$$f_3 : ac$$

$$f_4 : ac + a$$

$$f_5 : bc + c$$

$$f_6 : abd + ad + bd + d$$

$$f_7 : cd$$

$$f_8 : abd + ab + ad + bd + a + b + d + 1$$

$$f_9 : abd + ab + bd + b$$

Let $S_0 = \{f_1, \ldots, f_9\}$ *and* $I = (S_0)$ *ideal in* $\mathbb{F}_2[a, b, c, d]$. *Then* $V(I) = \emptyset$ *as* $GB(I) = \{1\}$.

INITIAL DATA: $S_0 = \{f_1, \ldots, f_9\}$ *system of generators of the ideal* I, *monomial order* $<=<_{LEX}$ *on* $\mathbb{F}_2[a, b, c, d]$

STEP 1:

We start computing the S-polynomials and their corresponding remaiders modulo the current system of generators. We keep track of the first non-zero remaider

$$f_{10} = g_{12} = f_1 + acf_2 + af_2 + f_3 + cf_2 + f_2$$

recording the data as follows

$$((f_{10} = g_{12}), (f_1, f_2)(1, ac)|(f_2, f_3, f_2, f_2)(a, 1, c, 1))$$

STEP 2: The second non-zero remainder is given by

$$f_{11} = g_{18} = df_1 + cf_8 + f_1 + adf_2 + af_2 + df_{10} + df_2 + f_7 + f_{10} + f_2$$

and the corresponding recorded data

$$((f_{11} = g_{18}), (f_1, f_8)(d, c)|(f_1, f_2, f_2, f_{10}, f_2, f_7, f_{10}, f_2)(1, ad, a, d, d, 1, 1, 1))$$

Now by substituting f_{10} *in the expression of* f_{11}, *we obtain*

$$f_{11} = (acd + ac + cd + c)f_2 + (d + 1)f_3 + f_7 + cf_8$$

so we have the following data

$$((f_{11} = g_{18}), (f_1, f_8)(0, c)|(f_2, f_3, f_7)(acd + ac + cd + c, d + 1, 1)$$

STEP 3: The last non-zero remaider comes from the S-polynomial of f_3 *and* f_4

$$1 = f_{12} = g_{34} = 1 = f_3 + f_4 + f_{10} + f_{11}$$

so we record the data

$$((f_{12} = g_{34} = 1), (f_3, f_4)(1, 1)|(f_{10}, f_{11})(1, 1))$$

and after making the substitutions we obtain

$$1 = f_1 + (acd + cd + a + 1)f_2 + (d + 1)f_3 + f_4 + f_7 + cf_8$$

OUTPUT:

the core of the S_0 *is given by* $\{f_1, f_2, f_3, f_4, f_7, f_8\}$

the matrix M *is given by*

$$M = (1, acd + cd + a + 1, d + 1, 1, 1, c)$$

References

[1] Jürgen Herzog, Viviana Ene, *Gröbner Bases in Commutative Algebra*, American Mathematical Society, 2012.