Algebraic Algorithms

mykyta.narusevych@matfyz.cuni.cz

November 2022

1 Theoretical part

1. Let $R = \{r\}$, $r \in T[x]$. Show that the result of applying algorithm A (rewrtiting procedure) onto f is $f \bmod r$. Show that R is a Gröbner basis of the ideal $rT[x]$.

2. Characterize Gröbner bases of $T[x]$. **Hint**: note that all the ideals of $T[x]$ are of the form $rT[x]$.

3. Characterize all admissible (for Gröbner bases method) orderings of $T[x]$.

4. Find normal reduced Gröbner basis of the ideal $< x^3 + x^2 + x + 1, x^4 - 3x^2 - 2x >$ in $\mathbb{Q}[x]$. Using this as a starting point try to derive how does the result of applying Buchberger algorithm on $f, g \in T[x]$ look like and characterize normal reduced Gröbner bases of $T[x]$.

5. Find normal reduced Gröbner basis of the ideal $< 2x+y+4z-1, x-y-z, 2x-y+z+1 >$ in $\mathbb{Q}[x, y, z]$ with the lexicographical ordering given by $x > y > z$. Using this as a starting point show that it is possible to find normal reduced Gröbner basis of the ideal generated by linear polynomials using Gauss-Jordan elimination.

2 Computational part

For all the tasks below we assume that the underlying coefficient field is $\mathbb{Q}$ and the ordering is lexicographical given by $x_1 < x_2 < x_3 < ... < x_n$. You can try to implement all the algorithms in the more general setting, but it is not required. Also, while writing your code you can use sage's representation of polynomials with all the basic operations of the corresponding polynomial ring, although you cannot use procedures and functions related to algorithms we are trying to implement, e.g. you cannot use sage's built-in procedures to directly ask whether given polynomial belongs to the given ideal.

1. Implement Buchberger algorithm.

2. Implement algorithm which transforms given Grönber basis into the normal reduced basis. You can assume that input bases are always Gröbner.

3. Implement algorithm which decides whether given polynomial belongs to the given ideal. You can assume that an ideal is always given by its Gröbner basis.

4. Combine all of the above into a single algorithm solving ideal membership problem.