Assignment 3 M2/Sage Questions

The goal of this assignment will be to implement a primary decomposition algorithm for zero dimensional polynomial ideals over a field of characteristic zero. This is based on an algorithm of Gianni, Trager, and Zacharias [GTZ]. A review of other algorithms for primary decomposition is given in [DGP].

Definitions and Results

Throughout we will let k be a field of characteristic zero and work in the polynomial ring $k[x_1, \ldots, x_n]$.

Definition 1 (Maximal Ideal in General Position)**.** Let $\mathfrak{m}$ be a maximal ideal in $k[x_1, \ldots, x_n]$. We say $\mathfrak{m}$ is *in general position* with respect to the lexicographical order with $x_1 > x_2 > \cdots > x_n$ if the reduced Gröbner basis of $\mathfrak{m}$ is of the form:

$$\{x_1 - f_1(x_n), \ldots, x_{n-1} - f_{n-1}(x_n), f_n(x_n)\}$$

for some *single variable* polynomials $f_i(x_n)$ in $k[x_n]$.

Definition 2 (Change of Coordinates Induced by $\underline{a} \in k^{n-1}$)**.** For any $\underline{a} = (a_1, \ldots, a_{n-1}) \in k^{n-1}$ define an ring automorphism $\varphi_{\underline{a}} : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$ specified by

$$\varphi_{\underline{a}}(x_i) = x_i \text{ for } i < n \text{ and } \varphi_{\underline{a}}(x_n) = x_n + \sum_{i=1}^{n-1} a_i x_i.$$

Note that the inverse map is again the identity on x_i for $i < n$ and $\varphi_{\underline{a}}^{-1}(x_n) = x_n - \sum_{i=1}^{n-1} a_i x_i$. We call *$\varphi_{\underline{a}}$ the change of coordinates induced by $\underline{a} \in k^{n-1}$*.

Proposition 3. *Let $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ be a maximal ideal. Then there exists a Zariski open dense subset $U \subset k^{n-1}$ such that for every $\underline{a} \in U$ the maximal ideal $\varphi_{\underline{a}}(\mathfrak{m})$ is in general position with respect to the lexicographical order with $x_1 > x_2 > \cdots > x_n$.*

Definition 4 (Zero Dimensional Ideal in General Position)**.** Let $I \subset k[x_1, \ldots, x_n]$ be a zero dimensional ideal with minimal primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ and associated primes $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. We say that I *is in general position* with respect to the lexicographical order with $x_1 > x_2 > \cdots > x_n$ if we have that:

- The maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are in general position with respect to the lexicographical order with $x_1 > x_2 > \cdots > x_n$.
- The polynomials $\mathfrak{p}_1 \cap k[x_n], \ldots, \mathfrak{p}_r \cap k[x_n]$ are pairwise coprime (i.e. have greatest common divisor one).

Proposition 5. *Let $I \subset k[x_1, \ldots, x_n]$ be a zero dimensional ideal. Then there exists a Zariski open dense subset $U \subset k^{n-1}$ such that for every $\underline{a} \in U$ the zero dimensional ideal $\varphi_{\underline{a}}(I)$ is in general position with respect to the lexicographical order with $x_1 > x_2 > \cdots > x_n$.*

Theorem 6. *Let $I \subset k[x_1, \ldots, x_n]$ be a zero dimensional ideal in general position with respect to the lexicographical order with $x_1 > x_2 > \cdots > x_n$. Let G be the reduced Gröbner basis of I and let $\{f\} = G \cap k[x_n]$ and let $f = f_1^{c_1} \cdots f_r^{c_r}$ be the unique factorization of f into a product of powers of irreducible polynomials. Then the minimal primary decomposition of I is given by*

$$I = \bigcap_{i=1}^{r} \left(I + \langle f_i^{c_i} \rangle\right).$$

Algorithm

As above we work in the ring $R = k[x_1, \ldots, x_n]$ over a field k of characteristic zero.

Algorithm 1: ZPD
– Computes a minimal primary decomposition of a zero dimensional ideal –

Input: A zero dimensional ideal I in the ring R.
Output: A list of ideals $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$ such that $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ is a minimal primary decomposition of I.

1 Select a random $\underline{a} = (a_1, \ldots, a_{n-1}) \in k^{n-1}$;
2 Set $J = \varphi_{\underline{a}}(I)$;
3 Compute $\langle g \rangle = J \cap k[x_n]$;
4 Compute a factorization $g = g_1^{c_1} \cdots g_r^{c_r}$;
5 **for** i ***from*** 1 **to** r **do**
6 Compute a Gröbner basis G of $J + \langle g_i^{c_i} \rangle$ with respect to the lexicographical order with $x_1 > x_2 > \cdots > x_n$;
7 **if** $g_i^{c_i} \notin G$ **then**
8 RETURN ZPD(I) ;
9 Set $h_n = g_i$;
10 Set $\mathfrak{p}_i = \langle \varphi_{\underline{a}}^{-1}(h_n) \rangle$;
11 **for** j **from** *n-1 to 1* **do**
12 Find a polynomial $v \in G$ such that $v = (x_j - f_j(x_n))^m \mod \langle h_{j+1}, \ldots, h_n \rangle$ for some irreducible polynomial $f_j \in k[x_n]$ and some $m \in \mathbb{N}$;
13 **if** *no such polynomial v exists* **then**
14 RETURN ZPD(I);
15 Set $h_j = x_j - f_j(x_n)$;
16 Set $\mathfrak{p}_i = \mathfrak{p}_i + \langle \varphi_{\underline{a}}^{-1}(h_j) \rangle$;
17 RETURN $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\} = \{\varphi_{\underline{a}}^{-1}(J + \langle g_1^{c_1} \rangle), \ldots, \varphi_{\underline{a}}^{-1}(J + \langle g_r^{c_r} \rangle)\}$;

Questions

1. Implement Algorithm 1 in M2 or Sage. You may (and should) use the built in Gröbner basis and factorization commands. Test your implementation by comparing it to the built-in one (remember that primary decompositions are not unique). If you like, rather than the recursive calls in lines 8 and 14 you may simply return an error if these lines are reached and ask the user to run the code again.

2. Check on an example that the $\mathfrak{p}_i$ computed in Algorithm 1 (see line 16) give a prime decomposition $\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ and $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.

3. Briefly explain using the results and definitions given why this algorithm will correctly compute a minimal primary decomposition. You may also use the fact asserted by item 2 above.

4. Would you expect the algorithm to still work if we omit the changes of coordinates $\varphi_{\underline{a}}$ everywhere they occur above but instead apply $\varphi_{\underline{a}}$ to the ideal I and $\varphi_{\underline{a}}^{-1}$ to the resulting decomposition in lines 8 and 14? Can you think of a reason you may want to do this?

5. If we take $k = \mathbb{Q}$, remove the entire for loop from lines 5–16 of the algorithm, and make the choice of $\underline{a}$ using a uniform distribution on $\mathbb{Q}$ *informally* explain what probability of success you would expect.

6. On an actual computer we cannot sample from a uniform distribution over all of $\mathbb{Q}$. Try some empirical tests using your implementation on an example. How often does the code actually reach the recursive calls in lines 8 and 14?

References

[DGP] W. Decker, G.M. Greuel, and G. Pfister. Primary decomposition: algorithms and comparisons. *Algorithmic algebra and number theory* (pp. 187-220). Springer, Berlin, Heidelberg. 1999.

[GTZ] P. Gianni, B. Trager, G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6(2-3), 149-167, 1988.