Tutorial 4: The BMM-Algorithm: Not a BMW!

Given a finite dimensional vector space V over a field K, we want to turn it into a module over the polynomial ring $P = K[x_1, \ldots, x_n]$. How can we succeed in doing this? One important example is the case $V = P/I$ where $I \subseteq P$ is a zero-dimensional ideal. Here the canonical surjective map $P \longrightarrow P/I$ makes V a cyclic P-module. Are there other examples? How can we define a P-module structure on V? How can we check whether a P-module structure on V yields a cyclic module? These are the questions. Now let us look for answers.

Let us choose a K-basis $B = (v_1, \ldots, v_\mu)$ of V. Thus every endomorphism of V can be represented by a matrix of size $\mu \times \mu$ over K. In particular, when V is a P-module, then $M_1, \ldots, M_n$ denote the matrices corresponding to the multiplication endomorphisms $\mu_{x_i} : V \longrightarrow V$.

Using the following Buchberger-Möller algorithm for matrices, we can calculate the kernel $\operatorname{Ann}_P(V)$ of the composite map

$$\eta : \; P \;\longrightarrow\; \operatorname{End}_K(V) \;\cong\; \operatorname{Mat}_\mu(K)$$

where η is the map which sends a polynomial $f \in P$ to the multiplication map $\mu_f : P \longrightarrow P$. Moreover, the algorithm provides a vector space basis of $P/\operatorname{Ann}_P(V)$. To facilitate the formulation of this algorithm, we use the following convention. Given a matrix $A = (a_{ij}) \in \operatorname{Mat}_\mu(K)$, we order its entries by letting $a_{ij} \prec a_{k\ell}$ if $i < k$, or if $i = k$ and $j < \ell$. In this way we *flatten* the matrix to a vector in K^{μ^2}. Then we can reduce A against a list of matrices by using the usual Gaußian reduction procedure.

a) **(The BMM-Algorithm)**
Let σ be a term ordering on $\mathbb{T}^n$, and let $M_1, \ldots, M_n \in \operatorname{Mat}_\mu(K)$ be pairwise commuting. Consider the following sequence of instructions.

1. Let $G = \emptyset$, $\mathcal{O} = \emptyset$, $S = \emptyset$, $N = \emptyset$, and $L = \{1\}$.
2. If $L = \emptyset$, return the pair $(G, \mathcal{O})$ and stop. Otherwise let $t = \min_\sigma(L)$ and delete it from L.
3. Compute $t(M_1, \ldots, M_n)$ and reduce it against $N = (N_1, \ldots, N_k)$ to obtain
$$R = t(M_1, \ldots, M_n) - \sum_{i=1}^{k} c_i N_i \qquad \text{with} \quad c_i \in K$$
4. If $R = 0$, append the polynomial $t - \sum_i c_i s_i$ to G, where s_i denotes the i^{th} element of S. Remove from L all multiples of t. Continue with step (2).
5. Otherwise, we have $R \neq 0$. Append R to N and $t - \sum_i c_i s_i$ to S. Append the term t to $\mathcal{O}$, and append to L those elements of $\{x_1 t, \ldots, x_n t\}$ which are neither multiples of a term in L nor in $\operatorname{LT}_\sigma(G)$. Continue with step (2).

Prove that this is an algorithm which returns the reduced σ-Gröbner basis G of $\operatorname{Ann}_P(V)$ and a list of terms $\mathcal{O}$ whose residue classes form a K-vector space basis of $P/\operatorname{Ann}_P(V)$.

Hint: You can proceed as follows:

1. To prove termination, use Corollary 1.3.6.
2. Let $I = \operatorname{Ann}_P(V)$, and let H be the reduced σ-Gröbner basis of I. To show correctness, prove by induction that after a term t has been treated by the algorithm, the following holds: the list G contains all elements of H whose leading terms are less than or equal to t, and the list $\mathcal{O}$ contains all elements of $\mathbb{T}^n \setminus \operatorname{LT}_\sigma\{I\}$ which are less than or equal to t.
3. Show that the polynomial $t - \sum_{i=1}^k c_i s_i$ resulting from step (3) of the next iteration has leading term t.
4. Prove that the polynomial $g = t - \sum_{i=1}^k c_i s_i$ is an element of H if $R = 0$ in step (4).
5. Finally, show that the term t is not contained in $\operatorname{LT}_\sigma(I)$ if $R \neq 0$ in step (5).

b) Apply the BMM-Algorithm to the following example. Let $V = \mathbb{Q}^3$, let $B = (e_1, e_2, e_3)$ be its canonical basis, and let V be equipped the the $\mathbb{Q}[x, y]$-module structure defined by

$$M_1 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Compute the reduced `DegLex`-Gröbner basis of $\operatorname{Ann}_P(V)$ and a K-basis of $P/\operatorname{Ann}_P(V)$.

c) Implement the BMM-Algorithm in a CoCoA function `BMM`(...). Apply your function to the example above and compare its result to yours.

Now we are ready for the second algorithm of this tutorial: we can check effectively whether a P-module structure given by commuting matrices defines a cyclic module.

d) **(Cyclicity Test)**
Let V be a finite dimensional K-vector space with basis $B = (v_1, \ldots, v_\mu)$, and let $M_1, \ldots, M_n$ be pairwise commuting matrices. We equip V with the P-module structure defined by $M_1, \ldots, M_n$. Consider the following sequence of instructions.

1. Using the BMM-Algorithm, compute a set of terms $\mathcal{O} = \{t_1, \ldots, t_m\}$ whose residue classes form a K-basis of $P/\operatorname{Ann}_P(V)$.
2. If $m \neq \mu$ then return `"V is not cyclic"` and stop.

3. Let $z_1, \ldots, z_\mu$ be new indeterminates and $A \in \operatorname{Mat}_\mu(K[z_1, \ldots, z_\mu])$ the matrix whose columns are $t_i(M_1, \ldots, M_n) \cdot (z_1, \ldots, z_\mu)^{\mathrm{tr}}$ for $i = 1, \ldots, \mu$. Compute the determinant $d = \det(A) \in K[z_1, \ldots, z_\mu]$.
4. Check if there exists a tuple $(c_1, \ldots, c_\mu) \in K^\mu$ for which the polynomial value $d(c_1, \ldots, c_\mu)$ is non-zero. In this case return `"V is cyclic"` and $w = c_1 v_1 + \cdots + c_\mu v_\mu$. Then stop.
5. Return `"V is not cyclic"` and stop.

Prove that this is an algorithm which checks whether V is cyclic and, in the affirmative case, computes a generator.

Hint: Examine the images of the basis elements $\{\bar{t}_1, \ldots, \bar{t}_\mu\}$ for linear independence.

e) Apply the Cyclicity Test to the example above. Show that V is cyclic and find a generator.

f) Let $V = \mathbb{Q}^3$, let $B = (e_1, e_2, e_3)$ be its canonical basis, and equip V with the $\mathbb{Q}[x, y]$-module structure defined by the commuting matrices

$$\mathcal{M}_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathcal{M}_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Apply the Cyclicity Test and show that V is not cyclic although the dimensions of V and of $P/\operatorname{Ann}_P(V)$ coincide.

g) Write a CoCoA function `CyclTest`$(\ldots)$ which takes a list of n commuting matrices and checks whether they define a cyclic P-module. Apply your function to the above examples.

Hint: If the field K is infinite, the check in step (4) can be simplified to checking $d \neq 0$. For a finite field K, we can, in principle, check all tuples in K^μ.