APPLICATION OF THE NONCOMMUTATIVE GRÖBNER BASES METHOD FOR PROVING GEOMETRICAL STATEMENTS IN COORDINATE-FREE FORM

IRINA J. TCHOUPAEVA

Moscow, MSU, mech-math e-mail: ladyirina@shade.msu.ru

ABSTRACT. In this paper we consider the application of the noncommutative Gröbner bases method for proving theorems in algebraic geometry. Geometrical statements of constructive type should be given in the coordinate-free form.

1. Coordinate-free representation of points and statements

We consider theorems of elementary geometry (two-dimensional and three-dimensional). Let $A_1, A_2, A_3, \ldots, A_n$ be points in a finite-dimensional space. We treat these points as vectors drawn from the origin 0. Then, geometrically, the outer product of two vectors A and B is a bivector corresponding to the parallelogram obtained by sweeping the vector A along the vector B. The parallelogram obtained by sweeping Balong A differs from the parallelogram obtained by sweeping B only in the orientation.

Consider the Grassman algebra generated by points $A_1, A_2, A_3, \ldots, A_n$, i.e., the free algebra with an external product $A \wedge B$, which is associative and anticommutative: $A \wedge B = -B \wedge A$.

Consider a finite-dimensional space and task-space embedded in this space. For example, in the case of a two-dimensional task we consider a plane in the enveloping space.

2. Grassman Algebra

It is known that the Grassman algebra is an associative free algebra with a finite set of relations corresponding to the anticommutativity of multiplication on the generators:

$$Gr = \langle A_1, \ldots, A_n \| A_i \wedge A_j = -A_j \wedge A_i \forall i, j \in \{1, \ldots, n\} \rangle.$$

The conditions of anticommutativity $A_i \wedge A_j = -A_j \wedge A_i \forall i, j \in \{1 \dots n\}$ on the generators allow us to permute the neighboring factors in any product $A_{i_1} \wedge \dots \wedge A_{i_k}$. As a result, the product changes the sign.

So, any of these products in the Grassman algebra is equal up to the sign either to zero or to a product of generators with strictly increasing indices. It follows that any element of the Grassman algebra can be represented as a linear combination of such products

$$X = \sum_{(i_1,\dots,i_k), \quad i_1 < i_2 < \dots < i_k} \alpha^{(i_1,\dots,i_k)} A_{i_1} \wedge \dots \wedge A_{i_k}$$

Then, the dimension of the Grassman algebra is equal to 2^n , where *n* is the number of the generators. Thus, all ideals of this algebra are finite dimensional and have finite Gröbner bases.

3. Statements of the constructive type

In Chou's collection of examples [2] of two-dimensional geometrical tasks, there are a number of statements of the constructive type, which can be written in the coordinate-free form.

The following assertions can be written as some relations in the Grassman algebra:

- (1) three points A_1, A_2, A_3 are collinear iff $(A_1 A_2) \wedge (A_1 A_3) = 0$;
- (2) the lines A_1A_2 and A_3A_4 are parallel iff $(A_1 A_2) \land (A_3 A_4) = 0$;
- (3) a point A_3 divides an interval $[A_1; A_2]$ in the ratio n : m iff $m(A_3 A_1) = n(A_2 A_3) = 0$.

Moreover, some additional relations can be added to this list.

- (1) two points A_1 and A_2 are equal iff $A_1 A_2 = 0$;
- (2) two bivectors $A_1 \wedge A_2$ and $B_1 \wedge B_2$ are collinear iff $\alpha A_1 \wedge A_2 = \beta B_1 \wedge B_2$;
- (3) a point P lies on a plane $\{A_1, A_2, A_3\}$ iff $(A_1 P) \land (A_2 P) \land (A_3 P) = 0$.

etc.

4. Noncommutative Gröbner bases

Let us consider an associative noncommutative free algebra with unit 1 over the field F with generators a_1, \ldots, a_k . Each element of this algebra can be represented in the form $\sum_{(j_1,\ldots,j_l)} k^{(j_1,\ldots,j_l)} a_{j_1} \ldots a_{j_l}$. Introducing an order on the generators and an admissible order on the monomials, we can define the leading monomials $\operatorname{Im}(u) = k_u^{(j_1,\ldots,j_{l_u})} a_{j_1} \ldots a_{j_{l_u}}$ and $\operatorname{Im}(v) = k_v^{(i_1,\ldots,i_{l_v})} a_{i_1} \ldots a_{i_{l_v}}$ for any polynomials $u = \sum_{(j_1,\ldots,j_{l_u})} k_u^{(j_1,\ldots,j_{l_u})} a_{j_1} \ldots a_{j_{l_u}}$ and $v = \sum_{(i_1,\ldots,i_{l_v})} k_v^{(i_1,\ldots,i_{l_v})} a_{i_1} \ldots a_{i_{l_v}}$. Since we consider a free algebra over a field, we can normalize these polynomials

Since we consider a free algebra over a field, we can normalize these polynomials so that the leading coefficients become equal to unit. So, we assume that $\text{Im}(u) = a_{j_1} \dots a_{j_{l_u}}$ and $\text{Im}(v) = a_{i_1} \dots a_{i_{l_v}}$.

Now, we can consider all *compositions* of two monomials lm(u) and lm(v).

Two monomials have a composition f(u, v), iff the end of the first monomial is equal to the beginning of the second one, namely, in our case there exists an integer m > 0 and a set of indices p_1, \ldots, p_m such that $\lim(u) = a_{j_1} \ldots a_{j_{l_u-m}} a_{p_1} \ldots a_{p_m}$ and $\lim(v) = a_{p_1} \ldots a_{p_m} a_{i_{m+1}} \ldots a_{i_{l_v}}$.

Then, the composition is equal to

$$f(u,v) = a_{j_1} \dots a_{j_{l_u}-m} a_{p_1} \dots a_{p_m} a_{i_{m+1}} \dots a_{i_{l_v}} = \operatorname{Im}(u) v_1 = u_1 \operatorname{Im}(v),$$

where $v_1 = a_{i_{m+1}} \dots a_{i_{l_v}}$ and $u_1 = a_{j_1} \dots a_{j_{l_u-m}}$.

Since any monomial can be represented as a finite noncommutative product of the generators, there exist at most a finite set of compositions for each pair of monomials. Having obtained all compositions of leading monomials of two polynomials, one can write a finite number of noncommutative S -polynomials, which can be constructed as $S(u, v) = u_1 v - u v_1$.

A monomial $x = a_{s_1} \dots a_{s_n}$ is divisible by a monomial $y = a_{t_1} \dots a_{t_m}$ iff the monomial y is the substring of the monomial x so that $x = y_{left}yy_{right}$.

A polynomial p_1 with the unit leading coefficient is reducible with respect to a polynomial p_2 with the unit leading coefficient iff the leading monomial $lm(p_1)$ is divided by the leading monomial $lm(p_2)$ so that $lm(p_1) = \alpha lm(p_2)\beta$, where α and β are some monomials. The result of reduction is the polynomial $p'_1 = p_1 - \alpha p_2\beta$.

Noncommutative Gröbner bases of an ideal I are determined by analogy with the commutative case, as a complete system of relations, which generate this ideal.

The Buchberger algorithm is the same, however, the definitions of division, reduction and S -polynomial are changed.

5. Example of a theorem

Example 1. (Gauss' line).

Let A_1, A_2, B_1, B_2 be arbitrary points. Construct the complete quadrilateral $A_1A_2B_1B_2$ and diagonals A_1A_2 , B_1B_2 , A_1B_2 and B_1A_2 . Let A_1A_2 intersect B_1B_2 at A_3 , A_1B_2 intersect B_1A_2 at B_3 . Let M_1 be the midpoint of A_1B_1 , M_2 be the midpoint of A_2B_2 and M_3 be the midpoint of A_3B_3 . Then, the points M_1 , M_2 and M_3 lie on one straight line.

Now, we can formulate the following statements of the constructive type for this theorem:

- (1) $col(A_1, A_2, A_3)$: $(A_1 A_2) \land (A_1 A_3) = 0$
- (2) $col(B_1, B_2, A_3)$: $(B_1 B_2) \land (B_1 A_3) = 0$
- (3) $col(B_1, A_2, B_3)$: $(B_1 A_2) \land (B_1 B_3) = 0$
- (4) $col(A_1, B_2, B_3)$: $(A_1 B_2) \land (A_1 B_3) = 0$
- (5) $midp(A_1, B_1, M_1)$: $(M_1 A_1) = (B_1 M_1) = 0$.
- (6) $midp(A_2, B_2, M_2)$: $(M_2 A_2) = (B_2 M_2) = 0$.
- (7) $midp(A_1, B_1, M_1)$: $(M_3 A_3) = (B_3 M_3) = 0$.

The conclusion is the following: $col(M_1, M_2, M_3)$: $(M_1 - M_2) \wedge (M_1 - M_3) = 0$

6. Description of Gröbner Bases method for the proof of the theorems which are true universally (commutative and anticommutative case)

Some geometrical theorems can be formulated in these terms. To prove these theorems, the theory of noncommutative Gröbner bases can be applied. The system of polynomials corresponding to the hypotheses of the theorem and anticommutativity relations for the generators of the Grassman algebra are considered as generators of an ideal in a free associative algebra. The assertion of the theorem (written as a polynomial in this algebra) is valid if it belongs to this ideal. This is equivalent to zero reducibility of this polynomial.

Implementation of the algorithm for obtaining noncommutative Gröbner bases in the ring of noncommutative polynomials with integer coefficients are being developed.

In the commutative case, we have the same idea, but for the description of hypotheses and conclusions we use the equations for the coordinates of the points.

7. Calculation of Gröbner Bases on a systems with identities. Equivalence of identities on a whole set and relations on bases

ELEMENTS

In the general case, a polynomial identity is not equivalent to a system of equation on generators. However, in our case, the anticommutativity of homogeneous linear polynomials is equivalent to anticommutativity relations on the generators. There is a finite number of such relations.

For example, the property $A \wedge B = -B \wedge A$ for all homogeneous linear polynomials $A, B \in Gr$ is equivalent to the finite set of relations on the generators $A_i \wedge A_j = -A_j \wedge A_i \forall i, j \in \{1, \ldots, n\}$.

The conditions of anticommutativity can also be written as $A \wedge A = 0$ for all homogeneous linear polynomials A from the Grassman algebra. However, in this case the finite system of relations on the generators $A_i \wedge A_i = 0$, $i \in \{1, ..., n\}$ is not equivalent to the previous statement.

8. Description of the implemented algorithm

The algorithm for computing the anticommutative Gröbner bases with integer coefficients has been implemented.

The main algorithm in the program is the following:

- (1) Input the number of the variables and hypotheses.
- (2) Input the name of the variables in the increasing order.
- (3) Input the hypotheses and the conclusion.
- (4) Convert all the statements into the internal format.
- (5) Add the conditions of anticommutativity to the system.
- (6) Calculate the noncommutative Gröbner basis of the system.
- (7) Calculate the normal form of the conclusion of the theorem with respect to the Gröbner basis.
- (8) If the result is equal to zero, then the theorem is true universally, otherwise the theorem is not true universally.

The kernel of the program processes the general case of noncommutative Gröbner bases; however, the current interface is oriented to proving a specific class of geometrical theorems which can be formulated in terms of statements (1)-(3) in the Grassman algebra.

In CAS Maple V, functions which are able to make similar calculations are not revealed.

The program is written in Php 4.0 and uses possibilities of the web interface. Php 4.0 is a platform-free programming language. On the one hand, there is a possibility to include HTML-code into the texts of the programs for simple testing; on the other hand, this language enables us to use its resources as an object-oriented language.

9. An example of calculation of anticommutative Gröbner bases by the program

As an example, consider the operation of the program on the theorem on the Gauss line formulated above.

Determine the noncommutative Gröbner basis and the normal form of the conclusion of the theorem for the reverse lexicographical order on the monomials under the condition $A_1 < A_2 < A_3 < B_1 < B_2 < B_3 < M_1 < M_2 < M_3$.

The hypotheses of the theorem are

$$\begin{split} P[0]: & 1*A_2 \wedge A_3 - 1*A_1 \wedge A_3 - 1*A_2 \wedge A_1 + 1*A_1 \wedge A_1 \\ P[1]: & 1*B_2 \wedge B_1 - 1*B_1 \wedge B_1 - 1*B_2 \wedge A_3 + 1*B_1 \wedge A_3 \\ P[2]: & 1*B_2 \wedge B_3 - 1*A_1 \wedge B_3 - 1*B_2 \wedge A_1 + 1*A_1 \wedge A_3 \\ P[3]: & 1*B_1 \wedge B_3 - 1*A_2 \wedge B_3 - 1*B_1 \wedge B_1 + 1*A_2 \wedge B_1 \\ P[4]: & 2*M_1 - 1*B_1 - 1*A_1 \\ P[5]: & 2*M_2 - 1*B_2 - 1*A_2 \\ P[6]: & 2*M_3 - 1*B_3 - 1*A_3 \end{split}$$

The conclusion of the theorem is

$$1 * M_1 \wedge M_1 - 1 * M_1 \wedge M_3 - 1 * M_2 \wedge M_1 + 1 * M_2 \wedge M_3$$

IRINA J. TCHOUPAEVA

After adding the relations of anticommutativity on the generators of the Grassman algebra to the hypotheses of the theorem, the system of polynomials becomes

 $\mathbf{6}$

P[25]:	$1 * A_3 \wedge B_1 + 1 * B_1 \wedge A_3$
P[26]:	$1 * A_3 \wedge B_2 + 1 * B_2 \wedge A_3$
P[27]:	$1 * A_3 \wedge B_3 + 1 * B_3 \wedge A_3$
P[28]:	$1 * A_3 \wedge M_1 + 1 * M_1 \wedge A_3$
P[29]:	$1 * A_3 \wedge M_2 + 1 * M_2 \wedge A_3$
P[30]:	$1 * A_3 \wedge M_3 + 1 * M_3 \wedge A_3$
P[31]:	$1 * B_1 \wedge B_1$
P[32]:	$1 * B_1 \wedge B_2 + 1 * B_2 \wedge B_1$
P[33]:	$1 * B_1 \wedge B_3 + 1 * B_3 \wedge B_1$
P[34]:	$1 * B_1 \wedge M_1 + 1 * M_1 \wedge B_1$
P[35]:	$1 * B_1 \wedge M_2 + 1 * M_2 \wedge B_1$
P[36]:	$1 * B_1 \wedge M_3 + 1 * M_3 \wedge B_1$
P[37]:	$1 * B_2 \wedge B_2$
P[38]:	$1 * B_2 \wedge B_3 + 1 * B_3 \wedge B_2$
P[39]:	$1 * B_2 \wedge M_1 + 1 * M_1 \wedge B_2$
P[40]:	$1 * B_2 \wedge M_2 + 1 * M_2 \wedge B_2$
P[41]:	$1 * B_2 \wedge M_3 + 1 * M_3 \wedge B_2$
P[42]:	$1 * B_3 \wedge B_3$
P[43]:	$1 * B_3 \wedge M_1 + 1 * M_1 \wedge B_3$
P[44]:	$1 * B_3 \wedge M_2 + 1 * M_2 \wedge B_3$
P[45]:	$1 * B_3 \wedge M_3 + 1 * M_3 \wedge B_3$
P[46]:	$1 * M_1 \wedge M_1$
P[47]:	$1 * M_1 \wedge M_2 + 1 * M_2 \wedge M_1$
P[48]:	$1 * M_1 \wedge M_3 + 1 * M_3 \wedge M_1$
P[49]:	$1 * M_2 \wedge M_2$
P[50]:	$1 * M_2 \wedge M_3 + 1 * M_3 \wedge M_2$
P[51]:	$1 * M_3 \wedge M_3$

The noncommutative Gröbner basis of the ideal generated by relations P[0] - P[51] is

The normal form of the conclusion of the theorem with respect to the Gröbner basis is equal to zero.

Thus, the theorem is true universally.

In the paper [1] Wang considers the same theorem as an example of the use of the coordinate-free technique for automatic proving of theorems. Considering the same

order on the variables and monomials as a hypotheses of the theorem, he takes the same relations P[0] - P[6] of the first system, but from his paper it is not clear which system of relations he considers as relations responsible for the anticommutativity of multiplication.

10. Equations describing the dimension of the task space

It seems that we have to add equations describing the dimension of the task (whether the points are on the same line in the one-dimensional case, or whether the points are on the same plane in the two-dimensional case, etc) to our systems. It is related to the fact that we consider the enveloping space of the task.

Consider the condition that all points of the task lie on the same plane.

If the number n of points is equal to 1, 2 or 3, then all these points are on the same plane, and we need no additional relations.

If the number of points is equal to $n \ge 4$, then the condition that the points belong to the same plane is equivalent to the condition that any four points are on the same plane.

The relation $(A_1 - A_0) \wedge (A_2 - A_0) \wedge (A_3 - A_0) = 0$ formally means that the vectors $(A_3 - A_0)$, $(A_2 - A_0)$ and $(A_1 - A_0)$ are linearly dependent. This condition can be expressed by the formula $0 = (A_1 - A_0) \wedge (A_2 - A_0) \wedge (A_3 - A_0) = A_1 \wedge A_2 \wedge A_3 - A_0 \wedge A_2 \wedge A_3 + A_0 \wedge A_1 \wedge A_3 - A_0 \wedge A_1 \wedge A_2$. Here we take A_0 as a marked point. Actually, as the marked point, we can take any one of these four points.

So, if the number of points $n \ge 4$, the condition all these points belong to one and the same plane if and only if the system of C_n^4 relations $(A_{i_1} - A_{i_0}) \land (A_{i_2} - A_{i_0}) \land$ $(A_{i_3} - A_{i_0}) = 0$ hold, where $i_0, i_1, i_2, i_3 \in \{1, \ldots, n\}$ are any distinct four points.

For example, in the theorem about the Gauss line, we can add the condition that all nine points are on the same plane to the first system. The numbers of the additional relations such as $(X_1 - X_0) \wedge (X_2 - X_0) \wedge (X_3 - X_0) = 0$, where $X_0, X_1, X_2, X_3 \in \{A_1, A_2, A_3, B_1, B_2, B_3, M_1, M_2, M_3\}$ is equal to $C_9^4 = \frac{9!}{4!5!} = 126$. All these relations can be reduced to zero with respect to the Gröbner basis. This means that these polynomials lie in the ideal, generated by hypotheses of the theorem and the anticommutativity relations. Thus, this condition follows from the hypotheses of the theorem and the anticommutativity relations. Using our program, we can verify this fact automatically.

If the polynomials, describing the dimension of the task are not reducible to zero, but the conclusion of the theorem is reducible to zero, then our task is a particular case of another task of a higher dimension.

In the general case, we should consider the condition that all points of the task belong to an m-dimensional space embedded in the enveloping space of a higher dimension. So, we have to consider $C_n^{(m+2)}$ polynomials such as $(A_{i_1} - A_{i_0}) \wedge \cdots \wedge$ $(A_{i_{m+1}} - A_{i_0}) = 0$, where A_{i_0} is one of generators of the Grassman algebra and $i_0, i_1, \ldots, i_{m+1} \in \{1, \ldots, n\}$ is an arbitrary set of m + 2 distinct indices.

IRINA J. TCHOUPAEVA

11. Advantages of the coordinate-free method

- a) If the dimension of the task is m, then max degree of all hypotheses and conclusions will be less than or equal to m
- b) if the conditions of the task are satisfied, then an equation, whose degree is higher than m, cannot be presented in the Gröbner basis (but this is possible in the coordinate case).

12. Acknowledgments

I am grateful to my advisor E.V. Pankratiev for assistance while preparing this paper and for many valuable remarks.

References

- D. Wang, Gröbner Bases Applied to Geometric Theorem Proving and Discovering, Gröbner Bases and Applications, Eds. B. Buchberger and F. Winkler, Cambridge Univ. Press, 1998, pp. 281–302.
- [2] S.C. Chou, Mechanical Geometry Theorem Proving Mathematics and Its Applications, D. Reidel, Dordrecht, 1987.