ANALYSIS OF GEOMETRICAL THEOREMS IN COORDINATE-FREE FORM BY USING ANTICOMMUTATIVE GRÖBNER BASES METHOD

IRINA J. TCHOUPAEVA

Moscow, MSU, mech-math
e-mail: ladyirina@shade.msu.ru
Proceeding of the Fourth International Workshop on Automated Deduction in Geometry, Johannes Kepler Universität Linz, RISC-Linz, Schloss Hagenberg, Austria, September 4-6, 2002

ABSTRACT. In this paper we consider the Gröbner bases of Grassman algebra and their application to the algebraic geometry. Geometrical statements of constructive type should be given in the coordinate-free form.

1. INTRODUCTION

We consider theorems of elementary geometry. It is well known that it is possible to prove algebraic geometry task using computer algebra methods, such as Wu's method and method of commutative Gröbner bases [?], [?], [?]. Some kind of theorems can be proven using the method of anticommutative Gröbner bases.

Primarily, let us describe objects and tasks which will be regarded. We consider geometrical theorems in m - dimensional space $\mathbb{R}^m$, where $m \in \mathbb{N}_0$.
Let $\{A_1, A_2, A_3, \ldots, A_n\} \in \mathbb{R}^m$ be points of the task. We treat these points as vectors drawn from origin 0. All our theorems deal with statements of constructive type in the coordinate-free form. Data of a theorem contains a finite number of points $A_1, \ldots, A_n$ and finite number of $k_1, \ldots, k_l$ - dimensional subspaces of $\mathbb{R}^m$, $k_1, \ldots, k_l \leq m$ and their properties. Let be $m \geq (n-1)$, because in general case n points define a $(n-1)$ - space, and if we consider a space with $m < (n-1)$, we have some limitations for initial independent points.

Then, geometrically, the outer product of two vectors A and B is the bivector corresponding to the parallelogram obtained by sweeping vector A along vector B. The parallelogram obtained by sweeping B along A differs from the parallelogram obtained by sweeping A along B only in orientation. Let us consider the algebra generated by points $A_1, A_2, A_3, \ldots, A_n$ with an outer product $A \wedge B$, which is associative and anticommutative: $A \wedge B = -B \wedge A$. This algebra is called *Grassman algebra*. It can be proven easily, that the monomial is equal to zero, if it involves a variable in the power of two or more. Dimension of this algebra is equal to 2^n (the number of all non-zero monomials).

In Grassman algebra some geometrical statements may be formulated in these terms as polynomials.

Let the theorem consists of a number of hypotheses of the constructive type $\mathbb{H}_1, \ldots, \mathbb{H}_s$ and a conclusion of the constructive type $\mathbb{C}onc$. Then, these geometrical statements correspond to polynomials $h_1, \ldots, h_s \in Gr$ and $conc \in Gr$.

In commutative Gröbner bases method we have to introduce a coordinate system $(\mathbf{e}_1, \ldots, \mathbf{e}_q)$, then all statements of constructive type are projected to the coordinate subspace $\mathbb{R}^q \subseteq \mathbb{R}^m$:

$$\begin{array}{llll} \mathbf{\Pi}: & \mathbb{R}^m & \longrightarrow & \mathbb{R}^q \\ \mathbf{\Pi}: & \mathbb{H}_i & \longrightarrow & \bar{H}_i, \quad i = 1, \ldots, s \end{array}$$

where $\bar{H}_i$ is the statement in the space $\mathbb{R}^q$. All points $A_1, \ldots, A_n$ are also mapped to the coordinate space:

$$\mathbf{\Pi}: \quad A_i \quad \longrightarrow \quad \bar{A}_i(x_1^i, \ldots, x_q^i), \quad i = 1, \ldots, n$$

and for each point $\bar{A}_j$ in the space $\mathbb{R}^q$, $j = 1, \ldots, s$ in general case of coordinate system we have to introduce q new variables x_i^j, $i = 1, \ldots, q$. So, we will have $s \cdot q$ variables for the task. Moreover, if $q < (n-1) \leq m$ we have an additional limitation for points $A_1, \ldots, A_n$ of the task, but we do not have this limitation in the coordinate-free method.

We can also formulate statements of our task in terms of noncommutative free algebra $F = \langle X_1, \ldots, X_n \rangle$. Let

$$\langle X_1X_2 + X_2X_1, \ldots, X_{n-1}X_n + X_nX_{n-1} \rangle = I_{Ant} \lhd F$$

be a two-side ideal in free algebra F. We will call this ideal *an ideal of relations of anticommutativity.* And let

$$F_{Ant} = \langle X_1, \ldots, X_n | \quad X_1X_2 + X_2X_1, \ldots, X_{n-1}X_n + X_nX_{n-1} \rangle$$

be a free algebra with generators $X_1, \ldots, X_n$ and relations of anticommutativity on the generators. This algebra is isomorphic to the factor-algebra $F_{Ant} \simeq F/I_{Ant}$.

So, we can formulate our statements in terms of algebra F_{Ant}. So, we get $H_1, \ldots, H_s \in F_{Ant}$ and $Conc \in F_{Ant}$.

And some kind of theorems can be proven both in F_{Ant} using noncommutative Gröbner bases method and in terms of Gr using anticommutative Gröbner bases method. But in this paper we are going to show, thatin general noncommutative Gröbner bases in F_{Ant} are not equivalent to anticommutative Gröbner bases in Gr. And we have to use anticommutative Gröbner bases in Gr, but not noncommutative Gröbner bases in F_{Ant} to prove the theorems.

2. Statements of the constructive type in a coordinate-free form

In Chou's collection of examples [**?**] of the two-dimensional geometrical tasks there are some geometrical statements of constructive type, which can be written as polynomials of their coordinates. And the first question is: which of these statements can be rewritten in coordinate free form?

It is easy to check that we get the following:

(1) the 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 $(A_1 - A_2) \wedge (A_3 - A_4) = 0$;
(3) the point A_3 divides the interval $[A_1; A_2]$ in the ratio $n : m$ iff $m(A_3 - A_1) = n(A_2 - A_3) = 0$.

Then, the second question is: which statements of an m - dimensional space can be written as polynomials in Grassman algebra? And the third is: what kind of polynomials of Grassman algebra may be treated as statements of algebraic geometry?

Only the homogeneous polynomials can have geometrical sense in Grassman algebra. Then the third question transforms into question: what kind of homogeneous polynomials can be treated as statements of algebraic geometry?

So, we can formulate the following statements:

(1) $(k + 2)$ points $A_1, \dots, A_{k+2}$, $k + 2 \leq n \leq m + 1$ belong to the same k - dimensional subspace $\mathbb{R}^k$ of $\mathbb{R}^m$: $(A_1 - A_{k+2}) \wedge \cdots \wedge (A_{k+1} - A_{k+2}) = 0$ or in other words point $A_{i_{k+2}}$ belongs to k - subspace defined by the points $A_{i_1}, \dots, A_{i_{k+1}}$:
$$(A_{i_1} - A_{i_{k+2}}) \wedge \cdots \wedge (A_{i_{k+1}} - A_{i_{k+2}}) = 0$$
where $\{i_1, \dots, i_{k+2}\} = \{1, \dots, k+2\}$ as non-ordered sets
(2) two k - dimensional spaces are parallel $S_1 \| S_2 \subset \mathbb{R}^m$, this means that $\forall$ $(k+1)$ points $A_1, \dots, A_{k+1} \in S_1$ and any 2 points $B_1, B_2 \in S_2$:
$$(A_1 - A_{k+1}) \wedge \cdots \wedge (A_k - A_{k+1}) \wedge (B_1 - B_2) = 0$$
(3) $(k + 2)$ points $A_1, \dots, A_{k+2}$, $k + 2 \leq n \leq m + 1$ belong to the same k - dimensional subspace $\mathbb{R}^k$ of $\mathbb{R}^m$ and the proportion is known:
$\alpha_1(A_1 - A_{k+2}) + \cdots + \alpha_{k+1}(A_{k+1} - A_{k+2}) = 0$, where $\alpha_1, \dots, \alpha_{k+1} \in \mathbb{R}$
(4) as the generalization of the previous expressions, that there is a linear dependency among a finite number of k -vectors
$$\sum_{(i_1,\dots,i_k)\in\mathbb{R}^k} \alpha_{(i_1,\dots,i_k)} A_{i_1} \wedge \cdots \wedge A_{i_k} = 0$$

For example, the statement "*two points are equal*" $(A - B = 0)$, meaning that two points belong to the same 0 - dimensional subspace is a particular case of this kind of statements.

Thus, all homogeneous polynomials may be treated as some statements of algebraic geometry.

The outer product of vectors and its properties do not allow formulate conditions concerning angles and circles, thus we are not able to do this in terms of Grassman algebra or in terms of F_{Ant} with operation $\wedge$.

3. Gröbner bases in Grassman algebra

Let Gr be Grassman algebra of the variables $x_1, \dots, x_n$ over the field $K = \mathbb{R}$. This is the associative anticommutative algebra, which consists of Grassman polynomials $\sum_{(i_1,\dots,i_k)} \alpha_{i_1,\dots,i_k} x_{i_1} \wedge \dots \wedge x_{i_k}$. For all homogeneous polynomials $f, g \in Gr$ of degree $\deg(f) = \deg(g) = 1$ we have $f \wedge g = -g \wedge f$ and $f \wedge f = 0$. The maximal degree of monomials in Gr is equal to n and the dimension of this algebra equals 2^n.

So, we have

$$Gr = \langle x_1, x_2, \dots, x_n, x_1 \wedge x_2, \dots, x_{n-1} \wedge x_n, \dots, x_1 \wedge \dots \wedge x_n \rangle.$$

Definition. *Unsigned monomial* in Gr is the combination $u = x_{i_1} \wedge \dots \wedge x_{i_k} = x_1^{u_1} \wedge \dots \wedge x_n^{u_n}$ with $1 \le i_1 < \dots < i_k \le n$, where $i_1, \dots, i_k$ are the indexes of a variable with non-zero power in the product, and $u_j \in \{0, 1\}$, $j = 1, \dots, n$

By analogy with the commutative case, where the monomials can be treated as points in $\mathbb{Z}^n$, unsigned monomials of Gr can be treated as points $(u_1, \dots, u_n) \in \{0, 1\}^n$ with non-zero members on the places $i_1, \dots, i_k$ for $u = x_{i_1} \wedge \dots \wedge x_{i_k} = x_1^{u_1} \wedge \dots \wedge x_n^{u_n}$.

Example. For $Gr = \langle x_1, x_2, x_3, x_4 \rangle$ and $u = x_1 \wedge x_4$ we have $i_1 = 1$, $i_2 = 4$, $(u_1, u_2, u_3, u_4) = (1, 0, 0, 1) \in \{0, 1\}^4$.

Definition. *Term* is product of coefficient and unsigned monomial $t = \alpha \cdot u \in Gr$, $\alpha \in K$.

We can also regard *signed monomials* m as a product of unsigned monomial u and sign of the monomial $(-1)^{\sigma_m}$. Then $m = (-1)^{\sigma_m} \cdot u$ will be a particular case of term. And any term can be regarded as product of signed monomial and a positive coefficient $\alpha > 0$: $t = \alpha \cdot m$, where $m = (-1)^{\sigma} u$, and u is the unsigned monomial.

Each polynomial $p \in Gr$ can be represented as a finite sum of terms:

$$p = \sum_{j=1}^{d_p} t_{j,p}.$$

Definition. *Product* of two terms t_1 and t_2, where $t_1 = \alpha \cdot x_1^{a_1} \wedge \dots \wedge x_n^{a_n}$ with multidegree $(a_1, \dots, a_n) \in \{0, 1\}^n$ with non-zero components on the places $1 \le i_1 < \dots < i_k \le n$ and $t_2 = \beta \cdot x_1^{b_1} \wedge \dots \wedge x_n^{b_n}$ with multidegree $(b_1, \dots, b_n) \in \{0, 1\}^n$ with non-zero components on the places $1 \le j_1 < \dots < j_l \le n$, be the term $t = t_1 \wedge t_2$

$$t = \begin{cases} 0, & \text{if} \quad ((a_1, \dots, a_n) \bigwedge (b_1, \dots, b_n)) \neq (0, \dots, 0) \\ (\alpha \cdot \beta) \cdot (-1)^{\sigma} \cdot x_1^{c_1} \wedge \dots \wedge x_n^{c_n}, & \text{if} \quad ((a_1, \dots, a_n) \bigwedge (b_1, \dots, b_n)) = (0, \dots, 0) \end{cases}$$

where $(c_1, \dots, c_n) \in \{0, 1\}^n$ is a vector with non-zero elements on the places $1 \le h_1 < \dots < h_s \le n$, $s = k + l$ and as non-ordered set $\{h_1, \dots, h_s\}$ is equivalent the union of two non-ordered sets $\{i_1, \dots, i_k\} \cup \{j_1, \dots, j_l\}$, so that $(c_1 \wedge \dots \wedge c_n) = (a_1 \wedge \dots \wedge a_n) \bigvee (b_1, \wedge \dots \wedge b_n)$. And σ is the sign of alternating $(i_1, \dots, i_k, j_1, \dots, j_l)$.

Example. If $t_1 = 5 \cdot x_1 \wedge x_4$ and $t_2 = 3 \cdot x_2$, we have $(a_1, a_2, a_3, a_4) = (1, 0, 0, 1) \in \{0, 1\}^n$, $(b_1, b_2, b_3, b_4) = (0, 1, 0, 0) \in \{0, 1\}^n$, $i_1 = 1$, $i_2 = 4$ and $j_1 = 2$. So, $\deg(t_1) = k = 2$ and $\deg(t_2) = l = 1$, $(a_1, a_2, a_3, a_4) \bigwedge (b_1, b_2, b_3, b_4) = (0, 0, 0, 0)$, $\sigma = \mathrm{sign}(1, 4, 2) = 1$ and $(c_1, c_2, c_3, c_4) = (1, 1, 0, 1)$. Thus $t = t_1 \wedge t_2 = -15 \cdot x_1 \wedge x_2 \wedge x_4$.

Definition. Signed monomial $a = (-1)^{\sigma_a} \cdot x_1^{a_1} \wedge \cdots \wedge x_n^{a_n}$ with non-zero members on the places $1 \leq i_1 < \cdots < i_k \leq n$ *is divisible by* signed monomial $b = (-1)^{\sigma_b} \cdot x_1^{b_1} \wedge \cdots \wedge x_n^{b_n}$ with non-zero members on the places $1 \leq j_1 < \cdots < j_l \leq n$, iff for two vectors $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n) \in \{0,1\}^n$ there are inequality $(a_1, \ldots, a_n) \geq (b_1, \ldots, b_n)$. This means that $\forall i \in \{1, \ldots, n\}$ $a_i \geq b_i$. And so $a = (-1)^{\sigma_u} u \wedge b$, where u is unsigned monomial with multi-degree $(u_1, \ldots, u_n) = (a_1 - b_1, \ldots, a_n - b_n)$ with non-zero members on the places $1 \leq h_1 < \cdots < h_s \leq n$. and σ_u is the sign of alternating $(h_1, \ldots, h_s, j_1, \ldots, j_l)$. Then, *left divisor* of the monomial a by the monomial b is signed monomial $m = (-1)^{\sigma_u} \cdot u$.

Definition. *Term* $t_a = \alpha_a \cdot u_a$ *is divisible by term* $t_b = \alpha_b \cdot u_b$, where u_a, u_b are unsigned monomials, iff $\alpha_b \neq 0$ and signed monomial $m_a = 1 \cdot u_a$ is divisible by signed monomial $m_b = 1 \cdot u_b$. This means, that there is an unsigned monomial u, so that $m_a = (-1)^{\sigma_l} u \wedge m_b$. Then term $t_l = \alpha \cdot u$, $\alpha = (\alpha_a/\alpha_b) \cdot (-1)^{\sigma_l}$ so that $t_a = t_l \wedge t_b$. We say that t_l is left divisor of t_a. It can be seen, that the right divisor of t_a shall be $t_r = (-1)^{\sigma_r} \alpha \cdot u$, where σ_r is the sign of alternating $(j_1, \ldots, j_l, h_1, \ldots, h_s)$ and $t_a = t_b \wedge t_r$.

By definition, it is easy to construct algorithm to find left divisor of term t_a divided by the term t_b: $t_l =$ **LeftDivisor**(term t_a, term t_b) and right divisor of term t_a divided by the term t_b: $t_r =$ **RightDivisor**(term t_a, term t_b).

As in ring of commutative polynomials $k[x_1, \ldots, x_n]$, we consider ideals in Gr and Gröbner bases of the ideals.

Definition. Set $I \lhd Gr$ is an *ideal* in Gr iff:

(1) $0 \in I$
(2) $\forall f \in Gr\ \forall g \in I$, then $f \wedge g \in Gr$ and $g \wedge f \in Gr$
(3) $\forall f, g \in I$, then $(f + g) \in I$

Definition. *Admissible monomial order* $\prec$ on Gr is the order on terms with the properties:

(1) $\prec$ is linear
(2) if $t_1 \neq 0$, $t_2 \neq 0$ and $t_1 \prec t_2$ then $\forall\ t_3, t_4$ so that $t_3 \wedge t_1 \wedge t_4 \neq 0$ and $t_3 \wedge t_2 \wedge t_4 \neq 0$ then $t_3 \wedge t_1 \wedge t_4 \prec t_3 \wedge t_2 \wedge t_4$
(3) if $t \neq 0$, then $0 \prec t$
(4) each non-empty subset of monomials has its minimal element

By analogy with the commutative case, after setting order on all terms in Gr, for each polynomial $Gr \ni p = \sum_{(i_1,\ldots,i_n)} \alpha_{(i_1,\ldots,i_n)} x_1^{i_1} \wedge \cdots \wedge x_n^{i_n}$ we can define the *leader term* $\text{lterm}(p) = \alpha \cdot u$, where u is an unsigned monomial, and define *leader monomial* $\text{lm}(p) = u$ and *leader coefficient* $\text{lcoeff}(p) = \alpha$.

By knowing the leader term in polynomial, we can introduce the result of division of one polynomial by the second.

Definition. Let $p_1, p_2 \in Gr$ and we say, that the polynomial p_1 is right divided by the polynomial p_2 if there exist polynomials $q, r \in Gr$ so that:

$$p_1 = q \wedge p_2 + r, \text{ and } \deg(r) \prec \deg(p_2)$$

and q will be called *left divisor* and polynomial r will be the *reminder* of division polynomial p_1 by the polynomial p_2.

We can introduce the right division algorithm in Gr as a particular case of the following algorithm of obtaining the representation $p_1 = a_1 \wedge p_2 + \cdots + a_k \wedge p_k + r$, where as set $\{p_2, \ldots, p_k\}$ we take the only one polynomial p_2.

Theorem. For polynomials $p, p_1, \ldots p_k \in Gr$ an algorithm of obtaining representation $p = a_1 \wedge p_1 + \cdots + a_k \wedge p_k + r$ can be introduced, where $a_i, r \in Gr$ and $r = 0$ or r is a linear combination of monomials, which are not divisible by any monomials $\mathrm{lm}(p_1), \ldots, \mathrm{lm}(p_k)$.

Algorithm:

Input: $p_1, \ldots, p_k, p \in Gr$
Output: $a_1, \ldots, a_k, r \in Gr$
begin
  $a_1 := 0; \ldots a_k := 0; \quad r := 0$
  $q := p;$
  while $q \neq 0$ **do**
    $i := 1;$
    $IsDividing := false;$
    while $i \leq k$ **and** $IsDividing = false$ **do**
      if $\mathrm{lterm}(p_i)$ divides $\mathrm{lterm}(q)$ **then**
        $t :=$ **LeftDivisor**$(\mathrm{lterm}(q), \mathrm{lterm}(p_i));$
        $a_i := a_i + t;$
        $q := q - t \wedge p_i;$
      else
        $i := i + 1;$
      endif
    endwhile
    if $IsDividing = false$ **then**
      $r := r + \mathrm{lterm}(q);$
      $q := q - \mathrm{lterm}(q);$
    endif
  endwhile
end

Proof. Termination of the algorithm: we have finite number of polynomial $\{p_1, \ldots, p_k\}$ for enumerating, each polynomial has the finite number of terms and at each step in while-loop we have reduction of polynomial q by degree. And it is easy to check, that on the each step the relation $p = a_1 \wedge p_1 + \cdots + a_k \wedge p_k + r$ holds.

Example. For example, using the *lex* order in which
$A_1 < A_2 < A_3 < B_1 < B_2 < B_3 < M_1 < M_2 < M_3$

$$\begin{aligned} p &= 1 \cdot M_3 \wedge M_2 - 1 \cdot M_3 \wedge M_1 + 1 \cdot M_2 \wedge M_1 \\ p_1 &= 2 \cdot M_1 - 1 \cdot B_1 - 1 \cdot A_1 \\ p_2 &= 2 \cdot M_2 - 1 \cdot B_2 - 1 \cdot A_2 \end{aligned}$$

The outcome of the above algorithm is

$$\begin{array}{rcl} a_1 & = & -\frac{1}{2}M_3 + \frac{1}{2}M_2 \\ a_2 & = & \frac{1}{2}M_3 - \frac{1}{4}B_1 - \frac{1}{4}A_1 \\ r & = & \frac{1}{2}M_3 \wedge B_2 - \frac{1}{2}M_3 \wedge B_1 + \frac{1}{2}M_3 \wedge A_2 - \frac{1}{2}M_3 \wedge A_1 + \\ & & +\frac{1}{4}B_2 \wedge B_1 - \frac{1}{4}B_1 \wedge A_2 + \frac{1}{4}B_2 \wedge A_1 + \frac{1}{4}A_2 \wedge A_1 \end{array}$$

So, we have a representation $p = a_1 \wedge p_1 + a_2 \wedge p_2 + r$.

Definition. *Gröbner basis* in Gr of the ideal I is a set of polynomials $g_1, \dots, g_s \in I \lhd Gr$ that

$$\langle \mathrm{lterm}(g_1), \dots, \mathrm{lterm}(g_s) \rangle = \langle \mathrm{lterm}(I) \rangle$$

by analogy with the commutative case. Gr is finite dimensional algebra, so any ideal $I \lhd Gr$ is the finite dimensional, therefore any ideal has a finite Gröbner basis in Gr.

Theorem. If $G = \{g_1, \dots g_s\}$ is Gröbner basis of $I \lhd Gr$ and $f \in Gr$ is any polynomial, then $\exists! r \in Gr$ such that

(1) any monomial of r is not divisible by any monomial from $\mathrm{lm}(g_1), \dots \mathrm{lm}(g_s)$
(2) $\exists g \in I$ so that $f = g + r$

Definition. For each $f, g \in Gr$ we can define *S-polynomial* in Gr as a polynomial:

$$S(f,g) = \mathbf{LeftDivisor}(m, \mathrm{lterm}(f)) \wedge f - \mathbf{LeftDivisor}(m, \mathrm{lterm}(g)) \wedge g$$

where m is signed monomial so that $m = t_l^f \wedge \mathrm{lterm}(f) = t_l^g \wedge \mathrm{lterm}(g)$ is the left least common multiple of the monomials $\mathrm{lterm}(f)$ and $\mathrm{lterm}(g)$.

Proposition. Let a and b be terms in Gr, $a = \alpha \cdot x_1^{a_1} \wedge \dots \wedge x_n^{a_n}$ and $b = \beta \cdot x_1^{b_1} \wedge \dots \wedge x_n^{b_n}$ and $\alpha, \beta \neq 0$, $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \{0,1\}^n$. Then we can find the least common multiple m as a term $m = (-1)^\sigma \gamma \cdot x_1^{m_1} \wedge \dots \wedge x_n^{m_n}$, where vector $(m_1, \dots, m_n) = (a_1, \dots, a_n) \bigvee (b_1, \dots, b_n)$ and coefficient $\gamma = \mathrm{lcm}(\alpha, \beta)$.

Proof. At first, a and b divide m, and second, there is no term m_1 so that m_1 is divisible both by a and by b with the property $m_1 \prec m$.

Buchberger algorithm for finding Gröbner bases in Grassman algebra is very similar to that of the commutative case. For the detailed information see [**?**],[**?**]. But in our case we have another algorithm for finding the least common multiple of two terms and of calculating divisor of the term in the NForm function.

It follows from the theorem, that for polynomial p and set of polynomials $D = \{h_1, \dots, h_s\}$ there exists a representation:

$$p = \sum_{k=1}^{s} a_k \wedge h_k + r$$

where r may be found by the algorithm. So, we will call $r = \mathbf{NForm}(p, D)$ the result of reduction of the polynomial p by the set D.

Algorithm:

Input: $h_1, \dots, h_s, \in Gr$
Output: a Gröbner basis for ideal $G = \{g_1, \dots, g_y\} \subset \langle H \rangle$, where $H = \{h_1, \dots, h_s\}$

begin
  $G := H$
  do
    $G' := G$
    for each pair $p \neq q \in G'$
      $S :=$ **NForm**$(S(p,q), G')$
      if $S \neq 0$
        $G := G \cup \{S\}$
      endif
  while $G = G'$
end

Example. Ideal generated by $h_1, \dots h_7$:

$$\begin{aligned}
h1 :=&\ 1 \cdot A_3 \wedge A_2 - 1 \cdot A_3 \wedge A_1 + 1 \cdot A_2 \wedge A_1 \\
h2 :=&\ 1 \cdot B_2 \wedge B_1 - 1 \cdot B_2 \wedge A_3 + 1 \cdot B_1 \wedge A_3 \\
h3 :=&\ 1 \cdot B_3 \wedge B_2 - 1 \cdot B_3 \wedge A_1 + 1 \cdot B_2 \wedge A_1 \\
h4 :=&\ 1 \cdot B_3 \wedge B_1 - 1 \cdot B_3 \wedge A_2 - 1 \cdot B_1 \wedge A_2 \\
h5 :=&\ 2 \cdot M_1 - 1 \cdot B_1 - 1 \cdot A_1 \\
h6 :=&\ 2 \cdot M_2 - 1 \cdot B_2 - 1 \cdot A_2 \\
h7 :=&\ 2 \cdot M_3 - 1 \cdot B_3 - 1 \cdot A_3
\end{aligned}$$

has the following the Gröbner basis with respect to *lex* monomial order and $A1 < A2 < A3 < B1 < B2 < B3 < M1 < M2 < M3$ order on variables:

$$\begin{aligned}
1 :&\ 1 * M3 - 1/2 * B3 - 1/2 * A3 \\
2 :&\ 1 * M2 - 1/2 * B2 - 1/2 * A2 \\
3 :&\ 1 * M1 - 1/2 * B1 - 1/2 * A1 \\
4 :&\ 1 * B2 \wedge B3 - 1 * A1 \wedge B3 + 1 * A1 \wedge B2 \\
5 :&\ 1 * B1 \wedge B3 + 1 * A1 \wedge B3 - 1 * A3 \wedge B1 + 1 * A1 \wedge A3 \\
6 :&\ 1 * A1 \wedge A3 \wedge B3 \\
7 :&\ 1 * A2 \wedge B3 + 1 * A1 \wedge B3 - 1 * A3 \wedge B1 - 1 * A2 \wedge B1 + 1 * A1 \wedge A3 \\
8 :&\ 1 * B1 \wedge B2 + 1 * A1 \wedge B2 - 1 * A2 \wedge B1 + 1 * A1 \wedge A2 \\
9 :&\ 1 * A3 \wedge B2 + 1 * A1 \wedge B2 - 1 * A3 \wedge B1 - 1 * A2 \wedge B1 + 1 * A1 \wedge A2 \\
10 :&\ 1 * A1 \wedge A2 \wedge B2 \\
11 :&\ 1 * A1 \wedge A3 \wedge B1 \\
12 :&\ 1 * A1 \wedge A2 \wedge B1 \\
13 :&\ 1 * A2 \wedge A3 - 1 * A1 \wedge A3 + 1 * A1 \wedge A2
\end{aligned}$$

and polynomial $f = 1 \cdot M_1 \wedge M_1 - 1 \cdot M_1 \wedge M_3 - 1 \cdot M_2 \wedge M_1 + 1 \cdot M_2 \wedge M_3$ belong to this ideal, and it is easy to verify that $r = 0$ for this polynomial.

4. Noncommutative Gröbner bases in free algebra and relations of anticommutativity

The concept of noncommutative Gröbner bases was studied in works [?],[?],[?], [?].

Let us consider an associative noncommutative free algebra with unit 1 over the field k: $F = k\langle X_1, \ldots, X_n\rangle$. Each element of this algebra can be represented as finite sum in the form

$$\sum_{(j_1,\ldots,j_l)} \alpha^{(j_1,\ldots,j_l)} X_{j_1} \ldots X_{j_l}.$$

Introducing an order on the generators $X_{i_1} < \cdots < X_{i_n}$, where $\{i_1, \ldots, i_n\} = \{1, \ldots, n\}$ as non-ordered sets, and the admissible order on the monomials, for any polynomials

$$u = \sum_{(j_1,\ldots,j_{l_u})} \alpha_u^{(j_1,\ldots,j_{l_u})} X_{j_1} \ldots X_{j_{l_u}}$$

and

$$v = \sum_{(i_1,\ldots,i_{l_v})} \alpha_v^{(i_1,\ldots,i_{l_v})} X_{i_1} \ldots X_{i_{l_v}}.$$

we can define the leading monomials

$$\mathrm{lm}(u) = \alpha_u^{(j_1,\ldots,j_{l_u})} X_{j_1} \ldots X_{j_{l_u}}$$

and

$$\mathrm{lm}(v) = \alpha_v^{(i_1,\ldots,i_{l_v})} X_{i_1} \ldots X_{i_{l_v}}$$

Since we have considered a free algebra over a field, we can normalize these polynomials having the leading coefficients become equal to unit. So, we assume that $\mathrm{lm}(u) = X_{j_1} \ldots X_{j_{l_u}}$ and $\mathrm{lm}(v) = X_{i_1} \ldots X_{i_{l_v}}$.

Definition. We consider all *compositions* of two monomials $\mathrm{lm}(u)$ and $\mathrm{lm}(v)$.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 are an integer $m > 0$ and a set of indexes $p_1, \ldots, p_m$ such that $\mathrm{lm}(u) = X_{j_1} \ldots X_{j_{l_u-m}} X_{p_1} \ldots X_{p_m}$ and $\mathrm{lm}(v) = X_{p_1} \ldots X_{p_m} X_{i_{m+1}} \ldots X_{i_{l_v}}$. Then, the composition is equal to

$$f(u, v) = X_{j_1} \ldots X_{j_{l_u-m}} X_{p_1} \ldots X_{p_m} X_{i_{m+1}} \ldots X_{i_{l_v}} = \mathrm{lm}(u)v_1 = u_1 \,\mathrm{lm}(v),$$

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

Since any monomial can be represented as a finite noncommutative product of the generators, there is at most a finite set of compositions for each pair of monomials.

Example. Let $F = \mathbb{R}\langle X_1, X_2, X_3, X_4\rangle$ be free algebra over $\mathbb{R}$, $M_1 = X_1X_4X_3X_4$ and $M_2 = X_4X_3X_4X_1$ be monomials in F. We can construct the set of all composition of monomials M_1 and M_2: $\{f_i(M_1, M_2)\}$ and find sets $\{(v_1^i, u_1^i)\}$ of left and right multiples:

$$\begin{array}{lllllll} M1: & X_1 & X_4 & X_3 & X_4 & & \\ M2: & & & & X_4 & X_3 & X_4 & X_1 \end{array}$$

Here we have the first composition $f_1(M_1, M_2) = X_1X_4X_3X_4X_3X_4X_1$, $v_1^1 = X_3X_4X_1$, $u_1 = X_1X_4X_3$. For the second composition we can construct the relation:

$$\begin{array}{llllll} M1: & X_1 & X_4 & X_3 & X_4 & \\ M2: & & X_4 & X_3 & X_4 & X_1 \end{array}$$

And we obtain $f_2(M_1, M_2) = X_1X_4X_3X_4X_1$, $v_1^2 = X_1$ and $u_1^2 = X_1$. As we can see, the set of composition $\{f(M_1, M_2)\}$ is not equal to the set $\{f(M_2, M_1)\}$. So, in this case we have only one composition $f_1(M_2, M_1)$:

$$\begin{array}{lllll} M1: & & & X_1 & X_4 \quad X_3 \quad X_4 \\ M2: & X_4 & X_3 & X_4 & X_1 \end{array}$$

Here we have $f_1(M_2, M_1) = X_4X_3X_4X_1X_4X_3X_4$, $v_1^1 = X_4X_3X_4$ and $u_1^1 = X_4X_3X_4$.

Definition. 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

$$S(u, v) = u_1v - uv_1.$$

Note, that this definition depends on the order of polynomials, hence $\{S_i(u, v)\} \neq \{S_j(v, u)\}$.

Definition. The monomial $x = X_{s_1} \dots X_{s_n}$ *is divisible by* the monomial $y = X_{t_1} \dots X_{t_m}$ iff the monomial y is the substring of the monomial x so that

$$x = y_{left}\ y\ y_{right}.$$

Example. In $F = \mathbb{R}\langle X_1, X_2, X_3, X_4\rangle$ monomial $M_1 = X_1X_3X_4X_3$ is divisible by the monomial $M_2 = X_3X_4$, and $y_{left} = X_1$ $y_{right} = X_3$.

Definition. Polynomial p_1 with the unit leading coefficient *is reducible* by a polynomial p_2 with the unit leading coefficient iff the leading monomial $\mathrm{lm}(p_1)$ is divisible by the leading monomial $\mathrm{lm}(p_2)$ so that $\mathrm{lm}(p_1) = \alpha\,\mathrm{lm}(p_2)\beta$, where α and β are some monomials.

Definition. The *result of reduction* shall be 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. But it this case Gröbner basis may be infinite.

The Buchberger algorithm is the same, however, the definitions of division, reduction and S - polynomial are different. And result of division of one monomial by another is not unequivocally defined. Thus, as a result of y_{left} we choose the shortest element of all possible elements in our algorithm, for definiteness. So, we can rewrite the Buchberger algorithm in this case with correction:

Algorithm:

Input: $H_1, \dots, H_s, \in F$

Output: a Gröbner basis for ideal $G = \{g_1, \dots, g_y\} \subset \langle H\rangle$, where $H = \{h_1, \dots, h_s\}$, if there exists finite Gröbner basis for this ideal

begin

  $G := H$

  do

    $G' := G$

    for each pair $p \neq q \in G'$

$\bar{S} := \{S_i(p,q)\} \cup \{S_j(q,p)\}$
foreach $S \in \bar{S}$
$S \in \bar{S}$
$S :=$ **NForm**$(S(p,q), G')$
if $S \neq 0$
$G := G \cup \{S\}$
endif
endforeach
while $G = G'$
end

Theorem. Let $I_{Ant} = \langle X_iX_j + X_jX_i \quad \forall i < j \ \rangle$ be two-side ideal in F of relations of anticommutativity. Let be F/I_{Ant} the factor algebra and free algebra with relations of anticommutativity

$$F_{Ant} = \langle X_1, \dots, X_n | \quad X_1X_2 + X_2X_1, \dots, X_{n-1}X_n + X_nX_{n-1} \rangle$$

This algebra is isomorphic to the factor-algebra $F_{Ant} \simeq F/I_{Ant}$.

Proof. Taking natural mapping

$$\begin{array}{llll} \gamma : & F_{Ant} & \longrightarrow & F/I_{Ant} \\ \gamma : & p & \longrightarrow & \{p + I_{Ant}\} \end{array}$$

and verifying algebra operations on classes of equivalence in F/I_{Ant} and corresponding elements in F_{Ant} we have the isomorphism.

For applying noncommutative Gröbner bases method we consider F_{Ant} and operations on this algebra. But before processing of the theorem $\mathbb{T} = \{[\mathbb{H}_1, \dots, \mathbb{H}_s]; \mathbb{C}onc\}$ we modify set of hypotheses into $\mathbb{T}' = \{[\mathbb{H}_1, \dots, \mathbb{H}_s, X_iX_j + X_jX_i \quad \forall i < j]; \mathbb{C}onc\}$ and apply our algorithm to $\mathbb{T}'$.

5. Noncommutative Gröbner bases for the anticommutative algebra

At the beginning, we tried to apply noncommutative Gröbner bases method to prove this kind of geometrical theorem. But we discovered that some generally true theorems, which can be represented as set of statements of constructive type, can not be proven using this technique. However, they can be proven in the technique of anticommutative Gröbner bases in Gr. In the [**?**] the authors regarded corresponding properties in the free algebra $F = \langle X_1, \dots, X_n \rangle$ and algebra of commutative polynomials $k[x_1, \dots, x_n]$. By analogy, we regard the corresponding properties of F and $Gr = Gr(A_1, \dots, A_n)$ with the anticommutative product $\wedge$.

Let $I \lhd Gr$ be an ideal in Gr and γ be a natural mapping

$$\gamma : F \mapsto Gr$$

taking X_i to A_i for all $1 \leq i \leq n$. Then define $J \subset F$ as the set $J = \gamma^{-1}(I)$. And we obtain

$$F/J \simeq Gr/I.$$

We can define also a map

$$\delta : Gr \mapsto F, \quad A_{i_1} \wedge \dots \wedge A_{i_k} \mapsto X_{i_1} \dots X_{i_k}, \quad \text{if} \quad i_1 \leq \dots \leq i_k$$

Taking as the initial representative of class $\gamma^{-1}(f)$ for $f \in I \subset Gr$ the element $\delta(f)$, it is easy to prove that $J/I_{Ant} \simeq I$, by verifying all operations.

And if $I \lhd Gr$ is generated by the polynomials $h_1, \ldots, h_s$, and relations of anticommutativity $\{X_iX_j + X_jX_i \quad \forall i < j\} \subset F$ and

$$\bar{J} = \langle \delta(h_1), \ldots, \delta(h_s),\ X_iX_j + X_jX_i \quad \forall i < j\ \rangle \lhd F$$

then

$$F/\bar{J} \simeq (F/I_{Ant})/\langle \delta(h_1) \ldots \delta(h_s) \rangle \simeq F_{Ant}/\langle \delta(h_1) \ldots \delta(h_s) \rangle \simeq Gr/I.$$

It can be verified also by checking operations on the corresponging elements.

And we can calculate a noncommutative Gröbner basis for $\bar{J}$. So, if we have hypotheses $H_1, \ldots, H_s \in F$ and conclusion $Cons \in F$ and try to verify if $Conc$ belongs to the ideal $\bar{J}$, by calculate normal form of the conclusion $\mathbf{NForm}(Conc, \bar{J})$ we have

$$\mathbf{NForm}(Conc, \langle H_1, \ldots, H_s,\ X_iX_j + X_jX_i \quad \forall i < j\ \rangle) = 0 \text{ in } F$$
$$\Downarrow$$
$$\mathbf{NForm}(\gamma(Conc), \langle \gamma(H_1), \ldots, \gamma(H_s) \rangle) = 0 \text{ in } Gr$$

but

$$\mathbf{NForm}(conc, \langle h_1, \ldots, h_s \rangle) = 0 \text{ in } Gr$$
$$\not\Downarrow$$
$$\mathbf{NForm}(\delta(conc), \langle \delta(h_1), \ldots, \delta(h_s),\ X_iX_j + X_jX_i \quad \forall i < j\ \rangle) = 0 \text{ in } F$$

Because, conception of division in F and in Gr are not the same and m_1 divide m_2 in Gr do not imply that $M_1 = \delta(m_1)$ divides $M_2 = \delta(m_2)$ in F. Thus, if there exists a reduction

$$p_1 \to_{p_2} p_1' \quad \not\Rightarrow \quad P_1 = \delta(p_1) \to_{\delta(p_2)} P_1'$$

where $\text{lm}(p_1) = m_1$, $\text{lm}(p_2) = m_2$, $\text{lm}(\delta(p_1)) = M_1$ and $\text{lm}(\delta(p_2)) = M_2$.

Example. Let be $m_2 = xz$, and $m_1 = xyz$. In Grassman algebra m_2 divides m_1 and $m_1 = (-1) \cdot y\ m_2$. But in F we obtain $M_2 = XZ$, $M_1 = XYZ$ and M_2 is not substring of M_1, that means that M_2 does not divide M_1 in F. In class of equivalence of M_1 in $F/\langle X_iX_j + X_jX_i,\ \forall i < j\ \rangle$ there exists an element YZX which has the substring M_2, however we can not apply techniques of noncommutative Gröbner bases to our case.

6. Gröbner bases method applied to the coordinate-free geometry

To prove this kind of theorems, which are formulated in the coordinate-free form, the theory of anticommutative Gröbner bases may be applied. The system of polynomials corresponding to the hypotheses of the theorem are considered as generators of an ideal in Grassman algebra.

Let the theorem consist of a number of hypotheses of the constructive type $\mathbb{H}_1, \ldots, \mathbb{H}_s$ and a conclusion of the constructive type $\mathbb{C}onc$. Then, these geometrical statements correspond to polynomials $h_1, \ldots, h_s \in Gr$ and $conc \in Gr$.

Grassman algebra is generated by points of our theorem $A_1, \ldots, A_n$, $Gr = Gr(A_1, \ldots, A_n)$. Geometrical statements (hypotheses of the theorem) are formulated as polynomials in Gr:

$$h_1(A_1, \ldots, A_n) = 0$$
$$\vdots$$
$$h_s(A_1, \ldots, A_n) = 0$$

Let be $G = \{g_1, \ldots, g_q\} \subset I \lhd Gr$ the finite Gröbner basis of the ideal I. We can find it using the previous algorithm.

Definition. Let $\{h_1, \ldots, h_s\} \subset Gr$ be a set of polynomials corresponding to the hypotheses of the theorem and $conc \in Gr$ be a polynomial corresponding to the conclusion of the theorem. We say, that theorem is *generally true* , if for each partial solution $(A_1^0, \ldots, A_n^0)$ of the system $h_1 = 0, \ldots, h_s = 0$, we have $conc(A_1^0, \ldots, A_n^0) = 0$.

Definition. Let $I \lhd Gr$ be an ideal in Grassamn algebra. The *radical* of the ideal be $\sqrt{I} = \{f \in Gr \mid \exists\ m \in \mathbb{N}\ f^m \not\equiv 0,\ f^m \in I\}$.

Definition. Let $\mathrm{Hom}(Gr)$ be a set of all homogeneous polynomials of Gr, and $\mathrm{Hom}_k(Gr)$ be a set of all homogeneous polynomials of Gr of degree k.

Proposition. If k is the field of coefficients of $Gr(A_1, \ldots, A_n)$, then $Gr = \mathbb{R} \bigoplus \mathrm{Hom}_1(Gr) \bigoplus \cdots \bigoplus \mathrm{Hom}_n(Gr)$.

It is easy to check.

Proposition. For each $f \in \mathrm{Hom}_k(Gr)$, $1 \le k \le n$ we have $f^{n+1} \equiv 0$.

Note, that for formulating theorems we use only homogeneous polynomials of Grassman algebra with degree $\deg(f) \ge 1$.

Proposition. Let $I \lhd Gr$, then $\sqrt{I} = \{f \in Gr \mid \exists\ 1 \le m \le n\ f^m \not\equiv 0,\ f^m \in I\}$.

From this proposition we have to check only finite number of property $f \in I, \ldots f^n \in I$ for checking the property if $f \in \sqrt{I}$.

The property $f \in I$ is equivalent to zero reducibility of this polynomial f by G:

$$\mathbf{NForm}(f, G) = 0 \text{ in } Gr.$$

The following algorithm let us to check if $f \in \sqrt{I}$ in Gr:

Algorithm:

Input: $I \lhd Gr$, f
Output: the answer if $f \in \sqrt{I}$
begin
    Calculate Gröbner basis of I: G
    $InRadical = 0$;
    for $k = 1$ **to** n **do**
        $fk = f^k$;
        if $(fk \not\equiv 0)$ **then**
            NF=**Nform** (f, G);
            if $(NF = 0)$ **then**

$InRadical = InRadical + 1;$
endif
else
break;
endif
endfor
if $(InRadical > 0)$ **then**
return $f \in \sqrt{I}$
else
return $f \notin \sqrt{I}$
endif
end

Thus, the idea is to take the theorem of constructive type, reformulate it as a set of polynomials in Gr, calculate Gröbner basis of the ideal generated by these polynomials and verify whether $f \in \sqrt{I}$ in Gr or not. If the result is $f \in \sqrt{I}$, then the theorem is generally true, otherwise we do not know if the theorem is generally true. Most of generally true theorems can be verified by using this method. The hypothesis is that if $f \notin \sqrt{I}$, then the theorem is not generally true. This means that (the theorem is generally true) $\iff$ ($conc \in \sqrt{\langle h_1, \dots, h_s \rangle}$) in Gr, but this fact needs to be proved.

In the commutative case, for the description of hypotheses and conclusions we use the equations for the coordinates of the points, and algorithm for checking $f \in \sqrt{I}$ is much complicated. But in commutative case we have the equivalence (the theorem is generally true) $\iff$ ($conc \in \sqrt{\langle h_1, \dots, h_s \rangle}$) in $k[x_1, \dots, x_n]$.

7. Description of the implemented algorithm

As we can see, we can use noncommutative and anticommutative Gröbner bases method for the geometrical theorems in coordinate-free for, but in CAS Maple V, functions which are able to make similar calculations have yet to be revealed. Thus, the algorithm for computing the noncommutative and anticommutative Gröbner bases and normal form of the polynomial with rational coefficients have been implemented. First, the project **NCBG** (NonCommutative Gröbner Bases) consists of functions which were able to calculate noncommutative Gröbner basis in free algebra with relations of anticommutativity with integer coefficients. Then, on the basis of it K.J.Andreev implemented other project **ncbg** for calculating noncommutative and anticommutative Gröbner bases with rational coefficients. This software includes the interface module, which let us input data of the theorem at the internal metalanguage as a statements of constructive type. And some theorems were proven and analyzed by using this software.

The main algorithm in the program is the following:

Algorithm:

Input: points $A_1, \dots, A_n$, order, hypothesis $\mathbb{H}_1, \dots, \mathbb{H}_s$, conclusion $\mathbb{C}onc$

Output: The answer if the theorem is true in general.
begin
  reformulate statements into polynomials
  $\mathbb{H}_1, \ldots, \mathbb{H}_s, \mathbb{C}onc \to H_1, \ldots, H_s, Conc$
  check if $Conc \in$ by $\sqrt{\langle H_1, \ldots, H_s \rangle}$
  if $(Conc \in \sqrt{\langle H_1, \ldots, H_s \rangle}\ )$
    return "The theorem is generally true";
  else
    return "We have not the answer";
  endif
end

Some theorems can be proved both in noncommutative case with relations of anticommutativity and anticommutative case, but the other theorems can be proved only by using anticommutative Gröbner bases theory.

The project **ncbg** was implemented in C++ and used the main Buchberger algorithm. We are planning to improve strategy of computing Gröbner basis in the future.

8. The dimension of the task

So, we have a comprehensive space $\mathbb{R}^m$, and the task with its n points $A_1, \ldots, A_n \in \mathbb{R}^m$ and its.

Let $\mathbb{S}p_k$ the set of statements defined that all points of the task belong to the same k - dimensional space (for each set of points $\{A_{i_1}, \ldots, A_{i_{k+2}}\} \subset \{A_1, \ldots, A_n\}$ can be constructed a polynomial by using previous rules). We obtain C_n^{k+2} polynomials.

For the fixed $1 \leq k \leq m$ there are two kinds of the theorems, which we consider:

(1) hypotheses of the theorem $\bar{\mathbb{H}} = \{\mathbb{H}_1, \ldots, \mathbb{H}_s\}$ imply the statement, that all points of this theorem lie in the same k - dimensional subspace $\mathbb{R}^k$ of $\mathbb{R}^m$
(2) all other theorem

For the first class of theorem, we obtain the following:

$$\{\mathbb{H}_1, \ldots, \mathbb{H}_s\} \Rightarrow \{\mathbb{S}p_k\}$$
$$\{\mathbb{H}_1, \ldots, \mathbb{H}_s\} \Rightarrow \mathbb{C}onc$$

It would be noticed, that if we have n point $A_1, \ldots, A_n$ in the task, then for any compatible set of hypotheses we have

$$\{\mathbb{H}_1, \ldots, \mathbb{H}_s\} \Rightarrow \{\mathbb{S}p_{n-1}\}$$

because any of n points belong to the same $(n-1)$ - dimensional space. And it easy to verify, by using Gröbner bases method. And we have that for $\forall\, \mathbb{T}\ \exists\, 1 \leq k(\mathbb{T}) \leq m$ so that $\{\mathbb{H}_1, \ldots, \mathbb{H}_s\} \Rightarrow \{\mathbb{S}p_{k(\mathbb{T})}\}$.

From the other hand, for any $1 \leq k \leq m$ we have

$$\{\mathbb{S}p_k\} \Rightarrow \{\mathbb{S}p_{k+1}\}$$

and it can be verified by using Gröbner bases method too.

And we have the following:

$$(\{\mathbb{H}_1,\dots,\mathbb{H}_s\} \Rightarrow \mathbb{C}onc) \Rightarrow (\{\mathbb{H}_1,\dots,\mathbb{H}_s,\mathbb{S}p_k\} \Rightarrow \mathbb{C}onc)$$

It means that theorem is generally true in $\mathbb{R}^m$, then the projection of this theorem to the subspace $\mathbb{R}^k \subset \mathbb{R}^m$ is also generally true in $\mathbb{R}^k$, $\forall 1 \le k \le m$.

So, we obtain, if $\{\mathbb{H}_1,\dots,\mathbb{H}_s\} \Rightarrow \{\mathbb{S}p_k\}$ and the theorem is generally true, then this theorem is generally true in any subspaces Sp_k for $0 \le k \le n-1$.

Definition. *Dimension of the theorem* is a minimal number k: $1 \le k \le m$ so that $\{\mathbb{H}_1,\dots,\mathbb{H}_s\} \Rightarrow \{\mathbb{S}p_k\}$;

For finding the dimension $k(\mathbb{T})$ of the theorems we can use the following algorithm:

Algorithm:

Input: $\mathbb{T} = \{\mathbb{H}_1,\dots,\mathbb{H}_s;\mathbb{C}onc\}$
Output: $k(\mathbb{T})$
begin
  for $i = 0$ **to** $n-1$ **do**
    Prove $(\{\mathbb{H}_1,\dots,\mathbb{H}_s\} \Rightarrow \{\mathbb{S}p_i\})$
    if $(TRUE)$ **then**
      return i
    endif
  endfor
end

We can see, that dimension of the theorem is the property of the hypotheses. And in the other words, dimension of the theorem in the minimum number $1 \le k(\mathbb{T}) \le (n-1)$:

$$\{\mathbb{H}_1,\dots,\mathbb{H}_s\} \Rightarrow \{\mathbb{S}p_{k(\mathbb{T})}\}$$

This number $k(\mathbb{T})$ exists for each theorem, because for any set of hypotheses $\mathbb{H}'_1,\dots,\mathbb{H}'_{s'}$ the theorem $\mathbb{T}' = \{\mathbb{H}'_1,\dots,\mathbb{H}'_{s'};\mathbb{S}p_{n-1}\}$ will be generally true. Note, that if

$$\{\mathbb{H}_,\dots,\mathbb{H}_s,\mathbb{S}p_k\} \Rightarrow \{\mathbb{C}onc\},$$

then

$$\{\mathbb{H}_,\dots,\mathbb{H}_s,\mathbb{S}p_{k-1}\} \Rightarrow \{\mathbb{C}onc\}.$$

We can consider the common property of hypotheses and conclusion of the theorem as the maximum number $1 \le d(\mathbb{T}) \le m$ so that

$$\{\mathbb{H}_1,\dots,\mathbb{H}_s,\mathbb{S}p_{d(\mathbb{T})}\} \Rightarrow \{\mathbb{C}onc\}.$$

Using information about dimension of the theorem, we can make some remarks about finding additional conditions for the data, if the theorem is not generally true in $\mathbb{R}^m$. For example, if we find $1 \le k(\mathbb{T}) \le m$:

$$\{\mathbb{H}_,\dots,\mathbb{H}_s\} \Rightarrow \{\mathbb{S}p_{k(\mathbb{T})}\}$$

but

$$\{\mathbb{H}_,\dots,\mathbb{H}_s\} \not\Rightarrow \{\mathbb{C}onc\}$$

we can try to find the maximum dimension $d(\mathbb{T})$ of the space in which this theorem is generally true :

$$\{\mathbb{H}_, \dots, \mathbb{H}_s, \mathbb{S}p_{d(\mathbb{T})}\} \Rightarrow \{\mathbb{C}onc\}.$$

Additional conditions $\mathbb{S}p_{d(\mathbb{T})}$ will be restrictions for the $A_1, \dots, A_n$, if $1 \leq d(\mathbb{T}) < k(\mathbb{T})$. This number $d(\mathbb{T})$ exists for each theorem, because for any set of hypotheses $\mathbb{H}'_1, \dots, \mathbb{H}'_{s'}$ and any conclusion $\mathbb{C}onc'$ the theorem $\mathbb{T}' = \{\mathbb{H}'_1, \dots, \mathbb{H}'_{s'}, \mathbb{S}p_0; \mathbb{C}onc'\}$ will be generally true.

So, the algorithm for finding $d(\mathbb{T})$ is the following:

Algorithm:

Input: $\mathbb{T} = \{\mathbb{H}_1, \dots, \mathbb{H}_s; \mathbb{C}onc\}$, $k(\mathbb{T})$
Output: $d(\mathbb{T})$
begin
  For $i = k(\mathbb{T})$ **to** 1 **do**
   Prove ($\{\mathbb{H}_1, \dots, \mathbb{H}_s, \mathbb{S}p_i\} \Rightarrow \{\mathbb{C}onc\}$)
   if ($TRUE$) **then**
    return i
   endif
  endfor
end

Example. For example, the Gauss line theorem [**?**] the hypotheses imply that all points belong to the same plane (it is easy to check). So, in this theorem we have $\{\mathbb{H}_1, \dots, \mathbb{H}_7\}$ hypotheses, and $(\{\mathbb{H}_1, \dots, \mathbb{H}_7\} \Rightarrow \{\mathbb{S}p_2\})$. Thus $k(\mathbb{T}) = 2$.

But in the Pappus theorem [**?**] hypotheses of 9 points do not imply this property $\mathbb{S}p_2$. Moreover, this theorem is not generally true in the spaces $\mathbb{R}^f$ with $9 \geq f \geq 3$ and $d(\mathbb{T}) = 2$.

If we use the coordinate method, we add the properties of the q - dimension space, when we introduce the coordinate system $(e_1, \dots, e_q)$. This is equivalent to adding properties $\mathbb{S}p_q$ to the hypotheses. Therefore, in coordinate-free method we have to reformulate all hypotheses, if $q < m$, when we try to find the dimension of the task and the additional conditions.

9. Advantages of the coordinate-free method

- we analyze the dimensional of the theorem $k(\mathbb{T})$ and the maximum size of the space in which the theorem is generally true $d(\mathbb{T})$. We can do it also in the coordinate case. But it is required from us much more efforts. Either we have to take size of coordinate system $q > (n-1)$ or on each step of algorithm reformulate all conditions into new coordinate system with $q' > q$. But, in coordinate-free case we can do it without such efforts
- in coordinate case we have to make the preliminary analysis by choosing the good coordinate system to minimize number of equations. And this analyse we have to do for each theorem before checking it automatically. But in

coordinate-free case we have no coordinate system and do not need to make this analyses

- in general coordinate case without preliminary analysis by choosing the good coordinate system we have $q \cdot n$ variables, but in coordinate-free case we have only n variables, where n is the number of points in the theorem and q is the number of coordinate orts
- it is easier to interpret Grassman polynomials as geometry expressions
- all polynomials in the Buchberger algorithm can not have degree higher than n (where n is number of points in the task), but it is a problem in commutative case

10. Acknowledgments

I am grateful to my advisor E.V. Pankratiev for suggestions while preparing this paper and for many valuable remarks and to K.J.Andreev for the help of implementation the algorithms.

References

[1] B. Buchberger, Gröbner bases: an algorithmic method in polynomial ideal theory, in N.K.Bose (ed.), *Recent trends in multidimensional system theory*, Reidel, 1985 *Mathematics and Its Applications*, D. Reidel, Dordrecht, 1987.

[2] S.C. Chou, Mechanical Geometry Theorem Proving *Mathematics and Its Applications*, D. Reidel, Dordrecht, 1987.

[3] D.Cox, J.Little, D. O'Shea, Using Algebraic Geometry, Springer, New-York, 1998

[4] D.Cox, J.Little, Ideals, Varieties, and Algorithms *An Introduction to Computational Algebraic Geometry and Commutative Algebra*, second edition, Springer, New-York, 1998

[5] D. Eisenbud, I. Peeva, B. Sturmfels, Noncommutative Gröbner Bases for Commutative Ideals. *To appear in Proc. Am. Math. Soc.*

[6] T. Mora, Gröbner bases in noncommutative algebras, *Proc.ISSAC 88, LNCS 358 ,1989*, pp. 150-161

[7] T.Mora : An Introduction to Commutative and Noncommutative Gröbner Bases, *Theoretical Computer Science* vol.134 p131-173, 1994.

[8] I.J. Tchoupaeva, Application of the Noncommutative Gröbner Bases Method for Proving Geometrical Statements in Coordinate Free Form, *Proceeding of the Workshop on Under- and Overdetermined Systems of Algebraic or Differential Equation*, March 18-19, 2002, Karlsruhe, Germany

[9] I.J. Tchoupaeva, Application of Methods of Noncommutative Gröbner Bases to the Proof of Geometrical Statements Given in Noncoordinate Form, *Proceeding of the International Workshop on Computer Algebra and its Application to Physics*, June 28-30, 2001, Dubna, Russia

[10] V.Ufnarovski : Introduction to Noncommutative Gröbner Bases Theory, in Gröbner Bases and Applications, *B.Buchberger and F.Winkler (eds), Proc. London Math. Soc. vol.251* ,1998.

[11] V.W.Vasconcelos, Computational Methods in Commutative Algebra and Algebraic Geometry, Springer Verlag, 1998 Verschelde1999

[12] 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.