Geometry Theorem Proving in Vector Spaces

Sabine Stifter
RISC-Linz
Johannes Kepler University
A-4040 Linz, Austria

ABSTRACT

Within the last few years several approaches to automated geometry theorem proving have been developed and proposed that are based 1) on the formulation of a geometric statement as the implication of a polynomial equation (the "conclusion") from a set of polynomial equations (the "hyptheses"), and 2) the proof of the implication by algebraic methods, namely Gröbner bases and Ritt's bases. All these approaches require the introduction of coordinates for the points involved. Many geometric theorems, however, can be formulated as relations between points directly, without needing coordinates. We present a new method, based on Gröbner bases in vector spaces, that can prove geometric theorems that are formulated as relations between points directly. Our approach has the advantages that theorems can be formulated more naturally and fewer variables are needed for their formulations. This results in shorter and faster proofs.

For this approach to geometry theorem proving it is essential to formulate theorems as relations between points without introducing coordinates. It will be a major topic in this presentation which relations can be formulated and how the formulation can be done best. This envolves considerations of the underlying geometric statements and point configurations.

With our approach to geometry theorem proving it is possible to prove geometric theorems that can be formulated without explicitely introducing coordinates. The method is based on the concept of reduction rings and Gröbner bases computations of modules in rings $(\mathbf{R}[a_1, \ldots, a_m])^d[V_1, \ldots, V_n]$, where $V_1, \ldots, V_n$ stand for points and $a_1, \ldots, a_m$ are variables for scalars that may be needed to formulate the theorem. A vector space R^d can be embedded into a module over the ring R^d with componentwise addition and multipliation. So Gröbner bases of modules in rings $(\mathbf{R}[a_1, \ldots, a_m])^d[V_1, \ldots, V_n]$ can be regarded as Gröbner bases of the respective subsets of the vector space.

Geometry theorems are often described in the following manner: First one has a certain number of points that are arbitrarily positioned in space. Between these points no relations hold; they are "independent" from each other. Starting from these points, other points are defined that are set into relations with each other, originally given or already constructed points. These points are "dependent" from other points. For setting points into relations to each other, certain geometric predicates are used. A few predicates suffice to elegantly formulate various geometric theorems in Euclidean geometry. However, not all geometric relations between points can be formulated without explicitely specifying coordinates for the points. The most important relations that can be formulated on points directly, i.e. within the vector space, are the following:

P is on the line through A and B iff for some a

$$A + a(B - A) - P = 0$$

P is the center of the line segment AB iff

$$\frac{1}{2}(A + B) - P = 0$$

P divides the line segment AB in the ration a to b iff

$$a(P - A) + b(P - B) = 0$$

P is on the plane through points A, B, and C iff for some a, b

$$A + a(B - A) + b(C - A) - P = 0$$

In addition to the variables for the points itself, variables for scalars are needed. We restrict here our considerations to relations that can be written as polynomial equations in the variables for points and additional variables for scalars, but do not need explicit variables for coordinates of points, although one might think of a combination in which for some of the points variables for the coordinates are introduced.

Depending on the context, scalar variables may be bound by "for all" (for example, if one wants to show something for *all* points on a certain line) or may be bound by "there exists" (for example, if one describes a point on the intersection of two lines). From a logical point of view, geometric theorems are described by formulae of the following type:

$$\begin{aligned}(\forall V_1, \ldots, V_n)(\forall a_1, \ldots, a_e)(\exists a_{e+1}, \ldots, a_m):&\\ (h_1(a_1, \ldots, a_m, V_1, \ldots, V_n) &= 0\\ &\vdots\\ h_l(a_1, \ldots, a_m, V_1, \ldots, V_n) &= 0\end{aligned}$$

$$\Rightarrow$$

$$c(a_1, \ldots, a_m, V_1, \ldots, V_n) = 0)$$

where $V_1, \ldots, V_n$ denote points, $a_1, \ldots, a_m$ denote scalars, and $h_1, \ldots, h_l, c$ denote polynomials in $a_1, \ldots, a_m, V_1, \ldots, V_n$. Translating the informal description of a geometric theorem directly, one gets these existential quantifiers for some of the scalar variables. However, the variables that are bound by the existential quantifiers are specified (uniquely) by the hypotheses; i.e. actually the theorem holds for all possible solutions of the hypotheses set of equations for the variables $a_{e+1}, \ldots, a_m$. This means that one can change the existential quantifiers into universal quantifiers without changing the statement. So we can equally well consider theorems of the form

$$(\forall V_1, \ldots, V_n)(\forall a_1, \ldots, a_m):$$

$$(h_1(a_1, \ldots, a_m, V_1, \ldots, V_n) = 0$$

$$\vdots$$

$$h_l(a_1, \ldots, a_m, V_1, \ldots, V_n) = 0$$

$$\Rightarrow$$

$$c(a_1, \ldots, a_m, V_1, \ldots, V_n) = 0)$$

if we keep in mind that there is a distinction between the scalar variables.

For proving statements of this nature it suffices (although it is not necessary) to show c can be written as $c = \sum_i s_i v_i h_i$, where $s_i \in \mathbf{R}[a_1, \ldots, a_m]$, $v_i \in M[V_1, \ldots, V_n]$, $M = \{(a, \ldots, a) | a \in \mathbf{R}\}$. (We also say that c is in the module generated by $h_1, \ldots, h_l$.)

Gröbner bases in "vector spaces" are an appropriate tool for proofing memberships in such modules.