Radboud University

Automatic Geometric Theorem Proving using Gröbner Bases

Bachelor's Thesis Mathematics

Author: Ken Madlener (0436798)
Supervisor: Dr. W. Bosma
2nd Reader: Dr. B. Souvignier
Date: October 7, 2008
Version: 1.1

Contents

1 Introduction

A decision method for elementary geometry statements was outlined by Tarski in 1948. This method, however, is impractical for proving non-trivial theorems [3]. In the 1970s W.-T. Wu developed a powerful algebraic method which can prove a large number of non-trivial theorems [2, p. 298]. His method is based on a technique called "pseudo-division". It was subsequently demonstrated by Chou and others that Gröbner bases, invented by Buchberger in the 1960s, can be applied to prove the same class of geometric theorems [2, pp. 298–299]. In this text we shall demonstrate the Gröbner basis method and explain the necessary theory behind it. We have used the Magma algebra system [1] to do our computations.

2 Gröbner Bases

In this section we shall explain the rudimentary machinery used by the methods presented in Section 3. We follow [4] in our notations and refer to [2] for an elaborate treatment of Gröbner bases.

2.1 Definitions

Throughout this text, let K be an arbitrary field. In polynomial rings in one variable, one defines the leading term of a polynomial $f = a_n x^n + \ldots + a_0 \in K[x]$, where $a_n \neq 0$, as $\mathrm{LT}(f) = a_n x^n$. Because we will be working with rings in more than one variable, we can not give this a useful analogue without first defining an ordering on the monomials. We assign to each monomial $x_1^{\alpha(1)} x_2^{\alpha(2)} \cdots x_n^{\alpha(n)}$ in $K[x_1, \ldots, x_n]$ an n-tuple α.

Definition 2.1. A **monomial ordering** on $K[x_1, \ldots, x_n]$ is a relation $\prec$ on $\mathbb{N}^n$ such that

- $\prec$ is a total ordering;
- $\prec$ is a well-ordering;
- If $p \prec q$, then $p + \beta \prec q + \beta$ (for all $\beta \in \mathbb{N}^n$).

We can now give a sensible definition of the leading term of a polynomial in $K[x_1, \ldots, x_n]$.

Definition 2.2. Let $\prec$ be a monomial order and f a nonzero polynomial in $K[x_1, \ldots, x_n]$. The **leading term** of f is the term $a_\alpha x^\alpha$ (this is a multi-exponent notation) for which $a_\alpha \neq 0$ and α is the maximum among the n-tuples. The **leading coefficient** is then a_α.

As an example, let $f = 8x^2y^3z^6 + 5x^7y^4z^5 + 3xy^2$. Then with respect to the lexicographic monomial ordering, which says that $\beta \prec \alpha$ iff $\alpha - \beta$ has a positive leftmost nonzero entry, $\mathrm{LT}(f) = 5x^7y^4z^5$.

From now on, fix an order on the variables. Being able to test whether a polynomial is a member of an ideal plays a key role in proving geometric theorems. In the case of a polynomial ring in one variable this problem is readily solved by the highschool long division method, the resulting remainder is reduced modulo the set of input polynomials. A natural generalization would be the following algorithm.

Algorithm GeneralizedDivision
Input $(f_1, \ldots, f_n)$, f
Output r and optionally $(q_1, \ldots, q_n)$

$q := (\underbrace{0, 0, \ldots, 0}_{n})$
$r := 0$
$p := f$
repeat
  $i := 1$
  dividing := false
  while $i \leq n$ and not dividing **do**
    if $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ **then**
      $u := \mathrm{LT}(p)/\mathrm{LT}(f_i)$
      $q_i := q_i + u$
      $p := p - f_i u$
      dividing := true
    else
      $i := i + 1$
    end if
  end while
  if not dividing **then**
    $r := r + \mathrm{LT}(p)$
    $p := p - \mathrm{LT}(p)$
  end if
until $p = 0$

An implementation of this algorithm in Magma can be found in Appendix A.1. The correctness proofs can be found in [4, pp. 63-64]. Unfortunately,

the resulting remainder depends on the order of the f_i. We have encountered this problem with the polynomials when working out Example 3.2. This problem does not arise when the f_i form a Gröbner basis, as we shall see in Proposition 2.1.

Definition 2.3. Fix a monomial order $\prec$. A **Gröbner basis for an ideal** I **w.r.t.** $\prec$ is a finite subset $G = \{g_1, \ldots, g_n\}$ of I such that

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_n) \rangle = \langle \mathrm{LT}(I) \rangle.$$

In Section 2.3 we explain Buchberger's algorithm to compute a Gröbner basis of I.

2.2 Some properties of Gröbner bases

Proposition 2.1. *Let $G = \{g_1, \ldots, g_n\}$ be a Gröbner basis for the ideal $I \subset K[x_1, \ldots x_m]$ and let $f \in K[x_1, \ldots, x_m]$. Then there exists a unique $r \in K[x_1, \ldots, x_m]$ satisfying the following properties:*

- *No term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_n)$;*
- *There exists $g \in I$ such that $f = g + r$.*

Proof. We let r be the remainder of GeneralizedDivision(G, f), of which the output is of the form $f = c_1 g_1 + c_2 g_2 + \ldots + c_n g_n + r$.

Now suppose r is not unique. Then there exists g', r' such that $f = g + r = g' + r'$. Then $r - r' = g - g' \in I$, so that $r \neq r'$ implies that $\mathrm{LT}(r' - r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_n) \rangle$. We can expand $\mathrm{LT}(r' - r)$ as $\sum_i f_i \mathrm{LT}(g_i)$, where $f_i \in K[x_1, \ldots, x_m]$. It is then clear that since $\mathrm{LT}(r' - r)$ is a monomial, there must be some $\mathrm{LT}(g_i)$ that divides it. This contradicts the first property of r. Hence, $r' - r = 0$, and uniqueness is proved. For the second property, set $g = c_1 g_1 + c_2 g_2 + \ldots + c_n g_n \in I$. □

The above proposition gives rise to a method to determine whether a given $f \in K[x_1, \ldots, x_n]$ is a member of the ideal I. One first computes a Gröbner basis G of I and subsequently computes the remainder r of f divided by G. Then $r = 0$ iff $f \in I$.

Definition 2.4. A **reduced Gröbner basis** G is a Gröbner basis satisfying the following properties:

- Every $f \in G$ has leading coefficient 1;
- For every $f \in G$, no monomial of f lies in $\langle \mathrm{LT}(G - \{f\}) \rangle$.

A reduced Gröbner basis $G = \{h_1, \ldots, h_m\}$ has the particular property that any proper subset of G is not a Gröbner basis (w.r.t. the chosen monomial ordering). In Section 2.3 we shall demonstrate how to find the c_i if it is known that $f \in I$.

Proposition 2.2. *Given an ideal I, there exists a unique reduced Gröbner basis.*

Proof. See [4, pp. 91–92]. □

Proposition 2.2 exhibits yet another useful application of Gröbner bases. It is possible to determine whether two ideals are equal.

2.3 Computing a Gröbner basis

Definition 2.5. Let $f, g \in K[x_1, \ldots, x_n]$ be two nonzero polynomials. The **S-polynomial** of f and g is

$$S(f, g) = \frac{\mathrm{LT}(g)f - \mathrm{LT}(f)g}{\mathrm{GCD}(\mathrm{LT}(f), \mathrm{LT}(g))}.$$

We now state without proof the main theorem of Gröbner bases:

Theorem 2.1. *Let $I = \langle g_1, \ldots, g_n \rangle$ and fix a monomial ordering $\prec$. The set $G = \{g_1, \ldots, g_n\}$ is a Gröbner basis for I w.r.t. $\prec$ if and only if*

$$\mathrm{GeneralizedDivision}(G, S(f, g)) = 0$$

for all $f, g \in G$.

Proof. See [2, pp. 19-21] or [4, pp. 84-86]. □

We can devise an algorithm based on this theorem to compute a Gröbner basis. The algorithm takes F as input, a basis of an ideal I (i.e. a finite set of polynomials that generate I).

Algorithm Buchberger
Input $F := (f_1, \ldots, f_n)$
Output $G := (g_1, \ldots, g_m)$

$G := F$
$P := \{(a, b) \mid a, b \in F\}$
while $|P| > 0$ **do**

```
    Choose a pair (a, b) ∈ P
    P := P − {(a, b)}
    (r, q) := GeneralizedDivision(G, S(a, b))
    if r ≠ 0 then
      P := P ∪ {(h, r) | h ∈ G}
      G := G ∪ {r}
    end if
  end while
```

Because the algorithm only enlarges G, the output is a basis of I. It is also clear that in any stage $G \subset I$, because $S(f,g) \in I$ and the remainder on division by G is also in I. The algorithm terminates when GeneralizedDivision$(G, S(f,g)) = (0,q)$ for every $f, g \in G$. Theorem 2.1 then guarantees that the resulting G is a Gröbner basis.

It remains to show that the algorithm actually halts. Suppose that $r \neq 0$. Because r is the remainder on division by G, $\mathrm{LT}(r)$ is not divisible by the leading terms of the elements of G, hence $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G) \rangle$. So adding r to the new set G strictly increases the ideal generated by its leading terms. By the ascending chain condition (see [4, pp. 77-78]), this process must halt, because every strictly increasing chain of ideals of $K[x_1, \ldots, x_p]$ is finite.

Example 2.1. We compute a Gröbner basis w.r.t. the lexicographic order for $\langle x + y^2, xy + 1 \rangle \subset \mathbb{Q}[x, y]$. The S-polynomial of $x + y^2$ and $xy + 1$ is

$$S(x + y^2, xy + 1) = y(x + y^2) - 1(xy + 1) = y^3 - 1.$$

This polynomial can not be reduced modulo $x + y^2, xy + 1$, so it is added to G. In the next phase, we have two new S-polynomials:

$$S(x + y^2, y^3 - 1) = y^3(x + y^2) - x(y^3 - 1) = y^5 + x,$$

$$S(xy + 1, y^3 - 1) = y^2(xy + 1) - x(y^3 - 1) = x + y^2.$$

Both polynomials can be reduced modulo $x + y^2, xy + 1, y^3 - 1$, so $\{x + y^2, xy + 1, y^3 - 1\}$ is a Gröbner basis.

By Proposition 2.1 we can find a complete decomposition of a polynomial $f = \sum_i c_i g_i$ in terms of a Gröbner basis $G = \{g_1, \ldots, g_n\}$ using the GeneralizedDivision algorithm. In Section 3.2, we will need a decomposition of f in terms of the original basis $\{h_1, \ldots, h_m\}$. This can be achieved by computing the matrix N such that $N_{i,j} = (\mathrm{GD}(G, h_i))_j$, where $\mathrm{GD}(G, h_i)$

is the row with q_j's of GeneralizedDivision(G, h_i). Then $N \cdot (g_1 \ \cdots \ g_n)^{\mathsf{T}} = (h_1 \ \cdots \ h_m)^{\mathsf{T}}$. A left-inverse M of N (if it exists) has the property that

$$R \cdot M \cdot (h_1 \ \cdots \ h_m)^{\mathsf{T}} = R \cdot (g_1 \ \cdots \ g_n)^{\mathsf{T}},$$

where R is the "coefficient" row GD(G, h_i). We call a matrix M with this property a **transformation matrix**.

We can also arrive at a transformation matrix by using the information that is readily available in Buchberger's algorithm. This amounts to keeping track of a "coefficient" row V attached to each polynomial in G such that $g_i = \sum_j V_j f_j$. These V_j's have to be updated accordingly during execution of the algorithm. Because this involves a lot of bookkeeping, we do not give the pseudocode here, but a Magma implementation can be found in Appendix A.1.

3 Geometric Theorem Proving

3.1 Translating geometry into algebra

A thesis consists of a bunch of hypotheses and one or more conclusions. When doing elementary geometry, one may think of the hypotheses as a configuration of points, lines and circles. By introducing cartesian coordinates in the Euclidean plane, it is possible to define a corresponding set of polynomials $h_1, \ldots, h_n$ in unknowns $x_1, \ldots, x_m$, such that $h_1(x_1, \ldots, x_m) = \ldots = h_n(x_1, \ldots, x_m) = 0$ precisely if the conditions of the thesis in question are met.

Example 3.1. Let $O = (0,0), A = (a_1, a_2), B = (b_1, b_2)$. The statement "the point B lies on OA" corresponds to the equation $a_2 b_1 - b_2 a_1 = 0$.

It will always be so that some coordinates in a geometric configuration are arbitrary, whereas the other coordinates are fixed. As a convention, we will denote the arbitrary unknowns by u_i and the other coordinates by x_j.

Definition 3.1. We say that the conclusion g **follows** from the hypotheses $h_1, \ldots, h_n$ if $\forall (u_1, \ldots, u_p, x_1, \ldots, x_m) \in \mathbb{R}^{p+m}$ it holds that

$$\left.\begin{array}{c} h_1(u_1, \ldots, u_p, x_1, \ldots, x_m) = 0 \\ \vdots \\ h_n(u_1, \ldots, u_p, x_1, \ldots, x_m) = 0 \end{array}\right\} \Rightarrow \ g(u_1, \ldots, u_p, x_1, \ldots, x_m) = 0.$$

Suppose that the assumption in the above definition holds. Then $\sum_i f_i h_i = 0$, where $f_i \in \mathbb{R}[u_1, \ldots, u_p, x_1, \ldots, x_m]$, for every choice of the x_i. Thus, if there exists a decomposition of the conclusion $g = \sum_i f_i h_i$, we may conclude that the thesis holds. The Gröbner basis techniques from Section 2 give us an algorithmic way to determine whether $g \in I = \langle h_1, \ldots, h_n \rangle$, in other words, we are able to algorithmically verify some theses. Unfortunately, the converse does not hold, i.e. there exist theses which can not be proven this way. See [4, pp. 286,291] for more details.

Example 3.2. This theorem is taken from [5, 3.4]. Without loss of generality, fix $C = (0,0)$, $B = (b_1, 0)$, $A = (a_1, a_2)$. Let $K = (k_1, k_2), L = (l_1, l_2), G = (g_1, 0)$ be the feet of the altitudes BK, CL, AG respectively of ABC. Then BK, CL and AG intersect in the point H. The hypothesis polynomials are:

$H_1 = a_2k_2 - a_1b_1 + a_1k_1$	$AC \perp BK$
$H_2 = a_1k_2 - a_2k_1$	K is on AC
$H_3 = l_2a_2 - l_1b_1 + l_1a_1$	$AB \perp CL$
$H_4 = -a_2l_1 + a_2(b_1 - a_1) + a_2a_1 - l_2(b_1 - a_1)$	L is on AB
$H_5 = l_2h_1 - l_1h_2$	H is on CL
$H_6 = h_1 - g_1 = h_1 - a_1$	H is on AG

Note that for perpendicularity, we have used that two lines are perpendicular if and only if for their slopes s_1, s_2 it holds that $s_1 s_2 = -1$. The thesis is that CL, AG, BK intersect in H, i.e. $g = -k_2h_1 + k_2b_1 - h_2(b_1 - k_1)$. The configuration is as in Figure 1 on page 12.

If we use Magma to check whether

$$g \in I = \langle H_1, \ldots, H_6 \rangle \subseteq \mathbb{Q}[a_1, a_2, b_1, k_1, k_2, l_1, l_2, h_1],$$

it will unfortunately answer `false`.[1] This is due to so-called degenerate cases. For example, if A coincides with C, the coordinates of K are undefined. We can try asking Magma whether for example $ga_1a_2b_1 \in I$. This means that if $g \neq 0$, then $a_1 = 0$ or $a_2 = 0$ or $b_1 = 0$, thereby ignoring problematic configurations. This time Magma answers `true`. The Magma commands can be found in Appendix A.2. In Section 3.2 we will use Gröbner bases to automatically derive degenerate cases. In fact, we shall see that there exists a weaker assumption that leads to the conclusion, in Example 3.3.

[1] We use the rationals here, because it is impossible in Magma to compute a Gröbner basis in a polynomial ring with base field $\mathbb{R}$.

We have to remark that some intuition was involved in defining the polynomials representing the hypotheses of the above example. We used the knowledge that G is on BC, and therefore, that if the three altitudes coincide in one point, this point must have a_1 as its x-coordinate.

3.2 Degenerate cases

Sometimes geometric statements are not very precise. They make implicit assumptions about the figures involved. We have already encountered this problem in Example 3.2, where problems occur when certain coordinates are zero. The conclusions of these theorems are said to be generically true. In the present section we shall make this notion of genericity formal and demonstrate a remarkable application of Gröbner bases to discover these degenerate hypotheses.

A conclusion g is to hold for any choice of the unknowns u_i. Therefore, we want to exclude the degenerate cases in which the u_i actually depend on each other.

Definition 3.2. Let V be an irreducible variety[2] in the affine space $\mathbb{R}^{p+m}$ with coordinates $u_1, \ldots, u_p, x_1, \ldots, x_m$. We say that the $u_1, \ldots, u_p$ are **algebraically independent on** V if no nonzero polynomial in the u_i alone vanishes on V.

Definition 3.3. The conclusion g **follows generically** from the hypotheses $h_1, \ldots, h_m$ if $g \in \mathrm{I}(V') \subset \mathbb{R}[u_1, \ldots, u_p, x_1, \ldots, x_m]$, where V' is the union of the irreducible components of the variety $\mathrm{V}(h_1, \ldots, h_n)$ on which the u_i are algebraically independent.

Proposition 3.1. *The conclusion g follows generically from $h_1, \ldots, h_m$ if there exists a nonzero polynomial $d \in \mathbb{R}[u_1, \ldots, u_p]$ such that $d \cdot g \in \sqrt{H}$ (see footnote [3]), where $H = \langle h_1, \ldots, h_m \rangle$ and $h_i \in \mathbb{R}[u_1, \ldots, u_p, x_1, \ldots, x_n]$.*

Proof. Let V_i be one of the irreducible components of V'. Since $d \cdot g \in \sqrt{H}$, $(d \cdot g)^k \in H$ for some $k \geq 1$ and therefore $(d \cdot g)^k$ vanishes on V and hence $d \cdot g$ vanishes on V. Since V_i is a component of V, $d \cdot g$ also vanishes on V_i. Therefore, $d \cdot g \in \mathrm{I}(V_i)$. But since V_i is irreducible, $\mathrm{I}(V_i)$ is by Proposition 3 on p. 197 of [4] a prime ideal and thus $d \in \mathrm{I}(V_i)$ or $g \in \mathrm{I}(V_i)$. Since the u_i are algebraically independent on V_i, d does not vanish on V_i and is therefore

[2] We use irreducible varieties in a non-essential way in this text. The reader is referred to [4, p. 196] for background. We denote the ideal corresponding to variety V as $\mathrm{I}(V)$.

[3] The **radical** $\sqrt{I}$ of an ideal I is the set $\{f \mid f^n \in I \text{ for some } n \geq 1\}$.

not a member of $\mathrm{I}(V_i)$. Thus $g \in \mathrm{I}(V_i)$. Since this holds for every irreducible component V_i of V', it follows that $g \in \mathrm{I}(V')$. □

The polynomial d encodes information about the degenerate cases. The following proposition gives rise to a straightforward method to actually find d.

Proposition 3.2. *The polynomial d of Proposition 3.1 exists if and only if $g \in \sqrt{\widetilde{H}}$, where $\widetilde{H}$ is the ideal generated by $h_i \in \mathbb{R}(u_1, \ldots, u_p)[x_1, \ldots, x_n]$.*

Proof. ($\Rightarrow$) Suppose d as in Proposition 3.1 exists. Then $d \cdot g \in \sqrt{H}$, which means that $(d \cdot g)^k = \sum_i c_i h_i$ for some $k \geq 1$. Dividing both sides by d^k yields $g^k = \sum_i \frac{c_i}{d^k} h_i$, which shows that g is in the radical $\sqrt{\widetilde{H}}$.

($\Leftarrow$) Suppose $g \in \sqrt{\widetilde{H}}$. Then $g^k = \sum_i A_i h_i$, where $A_i = \frac{p_i}{q_i}$ such that $p_i \in \mathbb{R}[u_1, \ldots, u_p, x_1, \ldots, x_n]$ and $q_i \in \mathbb{R}(u_1, \ldots, u_p) - \{0\}$. Set $d = \prod_i q_i$. Then $(d \cdot g)^k = \sum_i A'_i h_i$, where $A'_i \in \mathbb{R}[u_1, \ldots, u_p, x_1, \ldots, x_n]$. Hence, $d \cdot g \in \sqrt{H}$. □

We can now present a method to obtain d, given that g is generically true. Given an ideal $I = \langle h_1, \ldots, h_n \rangle$, compute the reduced Gröbner basis $G = \{g_1, \ldots, g_l\}$ and corresponding transformation matrix M using the ExtendedBuchberger algorithm. Recall that $M \cdot (h_1 \ \cdots \ h_n)^\mathsf{T} = (g_1 \ \cdots \ g_l)^\mathsf{T}$. Repeatedly run GeneralizedDivision(G, g^k) and increment k (starting from $k = 1$) until the remainder is zero. This results in the row $R = (A_1 \ \cdots \ A_m)$ such that $R \cdot (g_1 \ \cdots \ g_l)^\mathsf{T} = g^k$. Next, compute RM in order to obtain the row with "coefficients" in the original basis $\{h_1, \ldots, h_n\}$ of I. Note that the $(RM)_i$ are members of the ring $\mathbb{R}(u_1, \ldots, u_p)[x_1, \ldots, x_n]$. Therefore, rewrite the $(RM)_i$ as $\frac{p_i}{q_i}$ and finally compute $d = \prod_i q_i$ as in the proof.

If the conclusion does not hold generically, this procedure does obviously not halt. The following proposition gives a sufficient criterion to decide whether g is generically true:

Proposition 3.3. $\{1\}$ *is the reduced Gröbner basis of the ideal*

$$\langle h_1, \ldots, h_m, 1 - yg \rangle \subset \mathbb{R}(u1, \ldots, u_p)[x_1, \ldots, x_n, y]$$

if and only if g follows generically from $\{h_1, \ldots, h_m\}$.

Proof. See [4, p. 177]. □

Example 3.3. We derive the degenerate cases of Example 3.2. A computation of RM in the ring $\mathbb{Q}(a1, a2, b1)[k_1, k_2, l_1, l_2, h_1]$ yields

$$\left(\begin{array}{c} \frac{a_1h_2 - a_1a_2 + a_2b_1}{a_1^2 + a_2^2} \\ \\ \frac{-a_2h_2 - a_1^2 + a_1b_1}{a_1^2 + a_2^2} \\ \\ \frac{a_1 - b_1}{a_1^2 + a_2^2}h_2 - \frac{a_1a_2}{a_1^2 + a_2^2} \\ \\ \frac{-a_2h_2 - a_1^2 + a_1b_1}{a_1^2 + a_2^2} \\ \\ \frac{a_1^2 - 2a_1b_1 + a_2^2 + b_1^2}{a_1^3 + a_1a_2^2}h_1 \\ \\ k_2 + \frac{-a_1^2 + 2a_1b_1 - a_2^2 - b_1^2}{a_1^3 + a_1a_2^2}l_1h_2 + \frac{a_1^2 - 2a_1b_1 + a_2^2 + b_1^2}{a_1^3 + a_1a_2^2}l_2h_1 + \frac{a_1^2 - 2a_1b_1 + a_2^2 + b_1^2}{a_1^2 + a_2^2}l_2 \end{array}\right)^{\mathsf{T}}$$

A simple calculation reveals that $d = a_1^2(a_1^2 + a_2^2)^6$ is admissible, i.e. it is a product of the q_i. Indeed, Magma tells us that $d \cdot g$ is in I in the ring $\mathbb{Q}[a1, a2, b1, k_1, k_2, l_1, l_2, h_1]$. Note that if $g \neq 0$, then $a_1^2 + a_2^2 = 0$ which means that $a_1 = 0$ and $a_2 = 0$. It turns out that setting $d = a_1^2 + a_2^2$ is sufficient. The degenerate case is therefore only the one in which A coincides with C. The Magma commands required to arrive at these results can be found in Appendix A.2.

Example 3.4. We consider the "Nine Point Circle" theorem of Brianchon and Poncelet (1820). A geometric proof can be found in [5, 3.6]. The construction is as follows (see Figure 1). The points A, B, C, G, K, L are constructed as in Example 3.2. The points D, E, F, P, Q, R are the midpoints of the segments BC, AB, AC, AH, CH, BH respectively. The theorem says

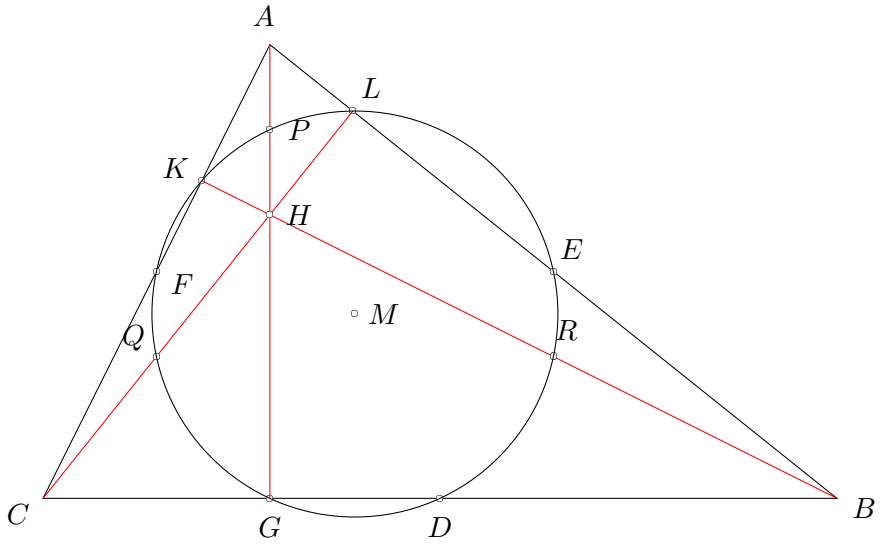

Figure 1: The nine point circle

that the points $D, E, F, G, K, L, P, Q, R$ lie on one circle.

$H_1 = 2d_1 - b_1$	D midpoint of BC
$H_2 = b_1 + a_1 - 2e_1$	E midpoint of AB
$H_3 = 2e_2 - a_2$	
$H_4 = 2f_1 - a_1$	F midpoint of AC
$H_5 = 2f_2 - a_2$	
$H_6 = g1 - a_1$	$AG \perp BC$
$H_7 = a_2k_2 - a_1(b_1 - k_1)$	$BK \perp AC$
$H_8 = a_2k_1 - a_1k_2$	K is on AC
$H_9 = l_2a_2 - l_1(b_1 - a_1)$	$CL \perp AB$
$H_{10} = -a_2l_1 + a_2b_1 - l_2(b_1 - a_1)$	L is on AB
$H_{11} = h_1 - a_1$	H is on AG
$H_{12} = l_2h_1 - h_2l_1$	H is on CL
$H_{13} = p1 - a_1$	P midpoint of AH
$H_{14} = h_2 + a_2 - 2p2$	
$H_{15} = 2q_1 - h_1$	Q midpoint of CH
$H_{16} = 2q_2 - h_2$	
$H_{17} = b_1 + h_1 - 2r_1$	R midpoint of BH
$H_{18} = 2r_2 - h_2$	
$H_{19} = (m_1 - d_1)^2 + m_2^2 - (m_1 - e_1)^2 - (m_2 - e_2)^2$	$MD = ME$
$H_{20} = (m_1 - d_1)^2 + m_2^2 - (m_1 - f_1)^2 - (m_2 - f_2)^2$	$MD = MF$

The conclusion polynomials $G_1, \ldots, G_6$ are of the form of H_{20}, but the coor-

dinates of F replaced with the coordinates of G, K, L, P, Q, R respectively. Using the techniques demonstrated in Example 3.3, we obtain the nondegeneracy condition $a_2^2 b_1 \neq 0$. It is well-known that $a_2 \neq 0$ iff $a_2^2 \neq 0$. However, Magma returns `false` when we ask whether $G_4 a_2 b_1 \in I$. We have to admit that we do not precisely know why this is so, but we expect that this happens because the hypothesis polynomials are irredicuble and of quadratic degree.

4 Conclusions

We have applied Gröbner bases to prove a theorem of elementary geometry in Example 3.2. It turns out that theorems stated textbooks often implicitly assume nondegeneracy conditions about the figures involved. For example, when talking about a triangle ABC, one often assumes that no pair of A, B, C coincides. It is possible to automatically find these degenerate cases using Gröbner bases. We have illustrated this in Example 3.3. In fact, the condition derived by means of Gröbner bases was weaker than our own temporary condition, in Example 3.2. We end our discussion with a treatment of the Nine Point Circle theorem in Exampe 3.4.

References

[1] W. Bosma, J. Cannon, C. Playoust. *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24(3-4):235-265, 1997.

[2] B. Buchberger, F. Winkler. *Gröbner Bases and Applications*, Cambridge, 1998.

[3] S.-C. Chou. *Automated reasoning in geometries using the characteristic set method and Gröbner basis method*, ISSAC '90, pp. 255–260, 1990.

[4] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties and Algorithms*, Springer-Verlag, 1992.

[5] W. Veldman. *Euclidische Meetkunde*, Nijmegen University, Lecture notes.

A Appendix

A.1 Magma Code

```
GeneralizedDivision := function(ring, F, f)
  if #F lt 1 then
    return f;
  end if;

  q := [ ring!0 : i in [1..#F] ];
  r := 0;
  p := f;
  repeat
    i := 1;
dividing := false;
while i le #q and not dividing do
  Q := quo<Parent(f)|LeadingTerm(F[i])>;
  if Q!LeadingTerm(p) eq 0 then
    u := ring!(LeadingTerm(p) / LeadingTerm(F[i])); // division possible, so u is in the ring
            q[i] := q[i] + u;
            p := p - u*F[i];
            dividing := true;
  else
    i := i + 1;
  end if;
end while;
if not dividing then
  r := r + LeadingTerm(p);
  p := p - LeadingTerm(p);
end if;
  until p eq 0;
  return r, q;
end function;

//-------------------------------------

ExtendedReduce := function(ring, F, G)
  D_ := []; N_ := G;
  k := #N_;

  while N_ ne [] do
    g_ := N_[k];
    g := g_[1][1];
    Prune(~N_);

    polys := [ (D_ cat N_)[i][1][1] : i in [1..#(D_ cat N_)] ];

    g,coeff_row := GeneralizedDivision(ring, polys, g);
```

```
    // mimic
    g_[1][1] := g;
    for i in [1..#F] do
      for j in [1..#(D_ cat N_)] do
        g_[2][i] := g_[2][i] - coeff_row[j]*(D_ cat N_)[j][2][i];
      end for;
    end for;

    if g ne 0 then
      LC := LeadingCoefficient(g);

      g_[1][1] := ring!g_[1][1]/LC;
      // mimic
      for i in [1..#F] do
        g_[2][i] := ring!g_[2][i]/LC;
      end for;
      D_ := D_ cat [g_];

    end if;

    k := k - 1;
  end while;

  D := [ D_[i][1][1] : i in [1..#D_] ];
  return D,D_;
end function;

//-------------------------------------

ExtendedBuchberger := function(F)
  if #F lt 1 then
    return [];
  end if;

  ring := Parent(F[1]);

  G := [ [ [F[i]], [ 0 : j in [1..#F] ] ] : i in [1..#F] ];
  for i in [1..#F] do
    G[i][2][i] := 1;
  end for;

  Pairs := [ [f, g] : f in G, g in G | f ne g ];

  while #Pairs gt 0 do
    pair := Pairs[#Pairs];
    Prune(~Pairs);
    f := pair[1]; g := pair[2];
```

```
    f_poly := f[1][1]; g_poly := g[1][1];
    f_row := f[2]; g_row := g[2];

    d := GCD(LeadingTerm(f_poly), LeadingTerm(g_poly));

    SPoly_poly := ring!((LeadingTerm(g_poly)*f_poly - LeadingTerm(f_poly)*g_poly)/d);
    SPoly_row := [ ring!((LeadingTerm(g_poly)*f_row[i] - LeadingTerm(f_poly)*g_row[i])/d) : i in [1..#F] ];

    SPoly := [[SPoly_poly], SPoly_row];

    r_poly,coeff_row := GeneralizedDivision(ring, [ g[1][1] : g in G ], SPoly_poly); // rest

    for i in [1..#F] do
      for j in [1..#G] do
        SPoly_row[i] := SPoly_row[i] - coeff_row[j]*G[j][2][i];
      end for;
    end for;

    r := [ [r_poly], SPoly_row ];

    if r_poly ne 0 then
      Pairs := Pairs cat [ [h,r] : h in G ];
      _,G := ExtendedReduce(ring, F, G cat [r]); // simplify the multiplication matrix
    end if;
  end while;

  GB_list := [ G[i][1][1] : i in [1..#G] ];

  GB_list,G := ExtendedReduce(ring, F, G);

  GB := Matrix(ring, #GB_list, 1, GB_list);
  M := Matrix(ring, #G, #F, [ [ g : g in G[i][2] ] : i in [1..#G] ] );

  return GB,GB_list,M;
end function;
```

A.2 Magma Commands

```
// configuration
// points (w.l.o.g.) C=(0,0), B=(b1,0), A=(a1,a2)
B<a1,a2,b1,k1,k2,l1,l2,h1,h2> := PolynomialRing(RationalField(), 9);
hypotheses := [
  a2*k2-a1*b1+a1*k1,
  a1*k2-a2*k1,
  l2*a2-l1*b1+l1*a1,
  -a2*l1+a2*(b1-a1)+a2*a1-l2*(b1-a1),
  l2*h1 - l1*h2,
```

```
  a1-h1
];
I := ideal< B | hypotheses >;
concl := -k2*h1+k2*(b1-k1)+k2*k1-h2*(b1-k1);

// try it; maybe there are no degenerate cases?
concl in I;

// apparently there are degenerate cases.
// a first guess is that A,B,C must not coincide, hence try a_1,a_2,b_1 \neq 0
concl*a1*a2*b1 in I;

// this worked, but can we also derive the degenerate cases automatically?

// we now work in the base field of rational functions in the unknowns a_1,a_2,b_1
A<a1,a2,b1> := FieldOfFractions(PolynomialRing(RationalField(), 3));
B<k1,k2,l1,l2,h1,h2> := PolynomialRing(A, 6);
hypotheses := [
  a2*k2-a1*b1+a1*k1,
  a1*k2-a2*k1,
  l2*a2-l1*b1+l1*a1,
  -a2*l1+a2*(b1-a1)+a2*a1-l2*(b1-a1),
  l2*h1 - l1*h2,
  a1-h1
];
I := ideal< B | hypotheses >;
concl := -k2*h1+k2*(b1-k1)+k2*k1-h2*(b1-k1);

// compute Groebner basis and transformation matrix using ExtendedBuchberger
GB,GB_list,M := ExtendedBuchberger(hypotheses);
OB := Matrix(B, #hypotheses, 1, hypotheses);

// verify that M*OB=GB;
M*OB eq GB;

// compute row of coefficients in terms of the GB
_,q := GeneralizedDivision(B, GB_list, concl);
R := Matrix(B, 1, #GB_list, q);

// verify
(R*M*OB)[1][1] eq concl;

// R*M is a row with of rational functions. The divisors of these functions form d
R*M;

// a_1^2+a_2^2 \neq 0 seems to be a sufficient condition, try it
B<a1,a2,b1,k1,k2,l1,l2,h1,h2> := PolynomialRing(RationalField(), 9);
hypotheses := [
  a2*k2-a1*b1+a1*k1,
```

```
  a1*k2-a2*k1,
  l2*a2-l1*b1+l1*a1,
  -a2*l1+a2*(b1-a1)+a2*a1-l2*(b1-a1),
  l2*h1 - l1*h2,
  a1-h1
];
I := ideal< B | hypotheses >;
concl := -k2*h1+k2*(b1-k1)+k2*k1-h2*(b1-k1);

concl*(a1^2+a2^2) in I;
```