Automatic Discovery of Geometry Theorems Using Minimal Canonical Comprehensive Gröbner Systems

Antonio Montes[1,⋆] and Tomás Recio[2,⋆⋆]

[1] Dep. Matemàtica Aplicada 2, Universitat Politècnica de Catalunya, Spain
antonio.montes@upc.edu
http://www-ma2.upc.edu/∼montes
[2] Dep. Matemáticas, Estadística y Computación, Universidad de Cantabria, Spain
tomas.recio@unican.es
http://www.recio.tk

Abstract. The main proposal in this paper is the merging of two techniques that have been recently developed. On the one hand, we consider a new approach for computing some specializable Gröbner basis, the so called Minimal Canonical Comprehensive Gröbner Systems (MCCGS) that is -roughly speaking- a computational procedure yielding "good" bases for ideals of polynomials over a field, depending on several parameters, that specialize "well", for instance, regarding the number of solutions for the given ideal, for different values of the parameters. The second ingredient is related to automatic theorem discovery in elementary geometry. Automatic discovery aims to obtain complementary (equality and inequality type) hypotheses for a (generally false) geometric statement to become true. The paper shows how to use MCCGS for automatic discovering of theorems and gives relevant examples.

Keywords: automatic discovering, comprehensive Gröbner system, automatic theorem proving, canonical Gröbner system.

MSC: 13P10, 68T15.

1 Introduction

1.1 Overview of Goals

The main idea in this paper is that of merging two recent techniques. On the one hand, we will consider a method (named *MCCGS*, standing for *minimal canonical comprehensive Gröbner systems*) [MaMo06], that is –roughly speaking– a

⋆ Work partially supported by the Spanish Ministerio de Ciencia y Tecnología under project MTM 2006-01267, and by the Generalitat de Catalunya under project 2005 SGR 00692.

⋆⋆ Work partially supported by the Spanish Ministerio de Educación y Ciencia under project GARACS, MTM2005-08690-C02-02.

F. Botana and T. Recio (Eds.): ADG 2006, LNAI 4869, pp. 113–138, 2007.

computational approach yielding "good" bases for ideals of polynomials over a field depending on several parameters, where "good" means that the obtained bases should specialize (and specialize "well", for instance, regarding the number of solutions for the given ideal) for different values of the parameters.

Briefly, in order to understand what kind of problem *MCCGS* addresses, let us consider the ideal $(ax, x + y)K[a][x, y]$, where a is taken as a parameter and K is a field. Then it is clear that there will be, for different values of $a = a_0 \in K$, essentially two different types of bases for the specialized ideal $(a_0x, x+y)K[x, y]$. In fact, for $a_0 = 0$ we will get $(x + y)$ as a Gröbner-basis (in short, a G-basis) for the specialized ideal; and for any other rational value of a such that $a = a_0 \neq 0$, we will get a G-basis with two elements, (x, y). Thus, the given G-basis $(ax, x + y)K[a, x, y]$ does not specialize well to a G-basis of every specialized ideal. On the other hand, let us consider $(ax - b)K[a, b][x]$, where a, b are taken as free parameters and x is the only variable. Then, no matter which rational values a_0, b_0 are assigned to a, b, it happens that $\{a_0x - b_0\}$ remains a Gröbner basis for the ideal $(a_0x - b_0)K[x]$. Still, there is a need for a case-distinction if we focus on the cardinal of the solutions for the specialized ideal. Namely, for $a_0 \neq 0$ there is a unique solution $x = -b_0/a_0$; for $a_0 = 0$ and $b_0 \neq 0$ there is no solution at all; and for $a_0 = b_0 = 0$ a solution can be any value of x (no restriction, one degree of freedom).

The goal of *MCCGS* is to describe, in a compact and canonical form, the discussion, depending on the different values of the parameters specializing a given parametric system, of the different basis for the resulting specialized systems and on their solutions.

The second ingredient of our contribution is about automatic theorem discovery in elementary geometry. Automatic discovery aims to obtain complementary hypotheses for a (generally false) geometric statement to become true. For instance, we can consider an arbitrary triangle and the feet on each sides of the three altitudes. These three feet give us another triangle, and now we want to conclude that such triangle is equilateral. This is generally false, but, under what extra hypotheses (of equality type) on the given triangle will it become generally true?

Finding, in an automatic way, the necessary and sufficient conditions for this statement to become a theorem, is the task of automatic discovery. A protocol for automatic discovery is presented in [RV99] and a detailed discussion of the method appears in [DR]. The protocol proceeds requiring some computations (contraction, saturation, etc.) about certain ideals built up from the given statement, but does not state any preference about how to perform such computations (although the computed examples in both papers rely on straightforward Gröbner bases computations for ideal elimination).

Our goal in this paper is to show how we can improve the automatic discovery of geometry theorems, by performing a *MCCGS* procedure on an ideal built up from the given hypotheses and theses, considering as parameters the free coordinates of some elements of the geometric setting,

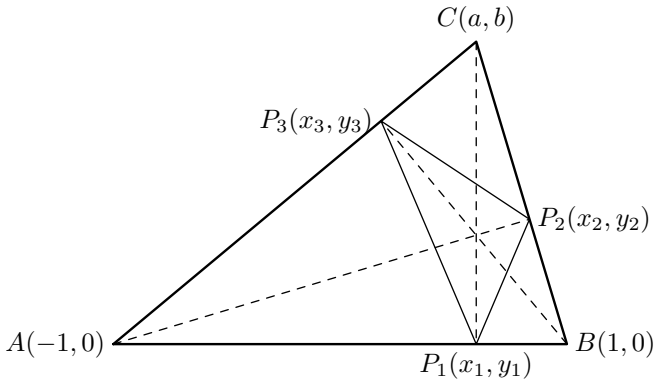

Fig. 1. Orthic triangle

1.2 Related Work

This idea has a close precedent in the work[1] of [CLLW], directly inspired by [K95] and, to a lesser extent, by [Weis92]. In [CLLW], a parametric radical membership test is presented for a mathematical construct the authors introduce, called "partitioned parametric Gröbner basis" (PPGB). Suppose we are given a statement $H := \{h_1 = 0, \ldots, h_r = 0\} \Rightarrow T := \{g = 0\}$, expressed in terms of polynomial equations –usually over some computable field– and their solutions over some extension field K –that we can assume, in order to simplify the exposition, to be algebraically closed. Roughly speaking, the method behind [CLLW] starts by computing the "partitioned basis" (with respect to a given subset of variables, here denoted by $\mathbf{u}$) of an ideal $I \subseteq K[\mathbf{u}, \mathbf{x}, y]$, (for instance, $I = (h_1(\mathbf{u}, \mathbf{x}) \ldots h_r(\mathbf{u}, \mathbf{x}), g(\mathbf{u}, \mathbf{x})\, y - 1)$), ie. a finite collection of couples (C_i, F_i), where the C_i's are constructible sets described as $\{c_1 = 0, \ldots, c_m = 0, q_1 \neq 0, \ldots, q_s \neq 0\}$ on the parameter space, and the F_i's are some collections of polynomials in $K[\mathbf{u}, \mathbf{x}, y]$. Moreover, it is required (among other conditions) that the C_i's conform a partition of the parameter space and, also, that for every element $\mathbf{u_0}$ in each C_i, the (reduced) G-basis of $(h_1(\mathbf{u_0}, \mathbf{x}) \ldots h_r, (\mathbf{u_0}, \mathbf{x}), g(\mathbf{u_0}, \mathbf{x})\, y - 1)$ is precisely $F_i(\mathbf{u_0}, \mathbf{x})$. It is well known (e.g. [K86] or [Ch88]) that, in this context, a statement $\{h_1 = 0 \ldots h_r = 0\} \Rightarrow \{g = 0\}$ is to be considered true if $1 \in (h_1 \ldots h_r, g\, y - 1)$; thus, the extra hypotheses that [CLLW] proposes to add for the statement to become a theorem are precisely those expressed by any of the C_i's such that the corresponding $F_i = \{1\}$, since this is the only case F_i can specialize to $\{1\}$.

We must remark that, simply testing for $1 \in (h_1 \ldots h_r, g\, y - 1)$, as in the method above, can yield to theorems that hold just because the hypotheses are not consistent (i.e. such that already $1 \in (h_1 \ldots h_r)$). This cannot happen with our approach to automatic discovery: if a new statement is discovered, then the obtained hypotheses will be necessarily consistent.

[1] But notice the authors of [CLLW] already mention the paper of Montes [Mo02] as a predecessor on this particular kind of discussion of Gröbner basis with parameters.

Although our approach stems from the same basic ideas, our contribution differs from [CLLW] in some respects: first, we focus on automatic discovery, and not in automatic proving. Moreover, we are able to specifically describe the capability and limitations of the method (while in [CLLW] it is only mentioned that, in the reducible case, their "method ... cannot determine if the conclusion of the geometric statement is true on some components of the hypotheses"). Second, even for proving, the use of *MCCGS* provides not only the specialization property (which is the key for the application of partitioned parametric bases in [CLLW]) but also an automatic case distinction, that allows a richer understanding of the underlying geometry for the considered situation. In fact, it seems that the partitioned parametric G-Basis (PPGB) algorithm from [CLLW] is close to the algorithm DISPGB considered in [Mo02], both sharing that their output requires collecting by hand multiple cases (and then having to manually express in some simplified way the union of the corresponding conditions on the parameters). Actually, the motivation for *MCCGS* was, precisely, improving DISPGB.

Our approach has also an evident connection (since [Weis92] is the common origin of all posterior developments on parametric Gröbner basis) to the work of several members of Prof. Weispfenning's group, regarding generic quantifier elimination (Q. E.) and its application to automatic theorem proving (as, for example, in [DG], [DSW], [SS], [St]). In particular we remark the strong relation of our work with that of [DG], that approaches theorem proving via a restricted (generically valid) Q.E. method, relying on generic Gröbner systems computations. The set of restrictions Θ provided by this method, besides speeding up the Q.E. computations, can be interpreted in the context of theorem proving, roughly speaking, as a collection of new (sufficient) non-degeneracy conditions for an statement to hold true.

Again, the difference between our contribution here and theirs is, first, that we address problems requiring, in general, parameter restrictions that go beyond "a conjunction Θ of negated equations in the parameters" ([DG], first paragraph in Section 3). That is, we deal with formulas that are almost always false (see below for a more detailed explanation of the difference between automatic derivation and automatic discovery) and require non-negated (ie. equality) parameter restrictions; they can not be directly approached via generic Q.E. since our formulas are, quite often, generically false. Moreover, our approach is limited to this specific kind of generically false problems and we do not intend to provide a general method for Q.E. A second difference is that, for our very particular kind of problems, *MCCGS* formulates parameter restrictions in a compact and canonical way, a goal that is not specifically intended concerning the description of Θ in [DG]. For these reasons we can not include performance comparisons to these Q.E. methods and we do not consider relevant (although we provide some basic information) giving hardware details, computing times, etc. on the performance of our method running on the examples described in the last section of this paper. We are not proposing something better, but something different in a different context.

Next Section includes a short introduction to the basics on automatic discovery, which could be of interest even for automatic proving practitioners. Section 3 provides some bibliographic references for the problem of the G-basis specialization and summarizes the main features of the *MCCGS* algorithm, including an example of its output. Section 4 describes the application of *MCCGS* to automatic discovery, while Section 5 works in detail a collection of curious examples, including the solution of a pastime from *Le Monde* and the simpler solution (via this new method) of one example also solved by a more traditional method.

2 A Digest on Automatic Discovery

Although less popular than automatic proving, automatic discovery of elementary geometry theorems is not new. It can be traced back to the work of Chou (see [Ch84], [Ch87] and [ChG90]), regarding the "automatic derivation of formulas", a particular variant of automatic discovery where the goal consists in deriving results that always occur under some given hypotheses but that can be formulated in terms of some specific set of variables (such as expressing the area of a triangle in terms of the lengths of its sides). Finding the geometric locus of a point defined through some geometric constraints (say, finding the locus of a point when its projection on the three sides of a given triangle form a triangle of given constant area [Ch88], Example 5.8) can be considered as another variant of this "automatic derivation" approach.

Although "automatic derivation" (or locus finding) aims to discover some new geometric statements (without modifying the given hypotheses), it is not exactly the same as "automatic discovery" (in the sense we have presented it in the previous section), that searches for complementary hypotheses for a (generally false) geometric statement to become true (such as stating that the three feet of the altitudes for a given triangle form an equilateral triangle and finding what kind of triangles verify it). Again, automatic discovery in this precise sense appears in the early work of Chou (whose thesis [Ch85] deals with "Proving and discovering theorems in elementary geometries using Wu's method") and Kapur [K89] (where it is explicitly stated that "... the objective here is to find the missing hypotheses so that a given conclusion follows from a given incomplete set of hypotheses...").

Further specific contributions to automatic discovery appear in [Wa98], [R98] (a book written in Spanish for secondary education teachers, with circa one hundred pages devoted to this topic and with many worked out examples), [RV99], [Ko] or [CW]. Examples of automatic derivation, locus finding and discovery, achieved through a specific software named *GDI* (the initials of *Geometría Dinámica Inteligente*), of Botana-Valcarce, appear in [BR05] or [RB] (and the references thereof), such as the automatic derivation of the thesis for the celebrated Maclane 8_3-Theorem, or the automatic answer to some items on a test posed by Richard [Ri], on proof strategies in mathematics courses, for students 14-16 years old.

The simple idea behind the different approaches is[2], essentially, that of adding the conjectural theses to the collection of hypotheses, and then deriving, from this new ideal of theses plus hypotheses, some new constraints in terms of the free parameters ruling the geometric situation. For a toy example, consider that $x - a = 0$ is the only hypothesis, that the set of points (x, a) in this hypothesis variety is determined by the value of the parameter a, and that $x = 0$ is the (generally false) thesis. Then we add the thesis to the hypothesis, getting the new ideal $(x - a, x)$, and we observe that the elimination of x in this ideal yields the constraint $a = 0$, which is indeed the extra hypothesis we have to add to the given one $x - a = 0$, in order to have a correct statement $[x - a = 0 \wedge a = 0] \Rightarrow [x = 0]$.

With this simple idea as starting point[3], an elaborated discovery procedure, with several non trivial examples, is presented in [RV99]. It has been recently revised in [BDR] and [DR], showing that, in some precise sense, the idea of considering $H + T$ for discovering is intrinsically unique (see Section 4 for a short introduction, leading to the use of *MCCGS* in this context).

3 Overwiew on the *MCCGS* Algorithm

As mentioned in the introduction, specializing the basis of an ideal with parameters does not yield, in general, a basis of the specialized ideal.

This phenomenon –in the context of Gröbner basis– has been known for over fifteen years now, yielding to a rich variety of attempts towards a solution (we refer the interested reader to the bibliographic references in [MaMo06] or in [Wib06]). Finding a specializable basis (ie. providing a single basis that collects all possible bases, together with the corresponding relations among the parameters) is –more or less– the task of the different comprehensive G-Basis proposals. Although the first global solution was that of Weispfenning, as early as 1992 (see [Weis92]), the topic is quite active nowadays, as exemplified in the above quoted recent papers. The *MCCGS* procedure, that is, computing the *minimal canonical comprehensive Gröbner system* of a given parametric ideal, is one of the approaches we are interested in. Let us describe briefly the goals and output of the *MCCGS* algorithm.

[2] Already present in the well known book of [Ch88], page 72: "... The method developed here can be modified for the purpose of finding new geometry theorems... Suppose that we are trying to prove a theorem... and the final remainder... R_0 is nonzero. If we add a new hypotheses $R_0 = 0$, then we have a theorem...". Here Chou proposes adding as new hypotheses the pseudoremainder of the thesis by the ideal of hypotheses, a mathematical object which should be zero if the theorem was generally true.

[3] Indeed, things are not so trivial. Consider, for instance, $H \Rightarrow T$, where $H = (a + 1)(a + 2)(b + 1) \subset K[a, b, c]$ and $T = (a + b + 1, c) \subset K[a, b, c]$. Take as parameters $U = \{b, c\}$, a set of $\dim(H)$-variables, independent over H. Then the elimination of the remaining variables over $H + T$ yields $H' = (c, b^3 - b)$. But $H + H' = (a + 1, b, c) \cap (a + 2, b, c) \cap (a + 1, b - 1, c) \cap (a + 2, b - 1, c) \cap (b + 1, c)$ does not imply T, even if we add some non-degeneracy conditions expressed in terms of the free parameters U, since T vanishes over some components, such as $(a + 2, b - 1, c)$ (and does not vanish over some other ones, such as $(a + 1, b - 1, c)$).

Given a parametric polynomial system of equations over some computable field, such as the rational numbers, our interest focuses on discussing the type of solutions over some algebraically closed extension, such as the complex numbers, depending on the values of the parameters. Let $\mathbf{x} = (x_1, \ldots, x_n)$ be the set of variables, $\mathbf{u} = (u_1, \ldots, u_m)$ the set of parameters and $I \subset K[\mathbf{u}][\mathbf{x}]$ the parametric ideal we want to discuss, where, in order to simplify the exposition, a single field K, algebraically closed, is considered both for the coefficients and the solutions. We want to study how the solutions over K^n of the equation system defined by I vary when we specialize the values of the parameters $\mathbf{u}$ to concrete values $\mathbf{u_0} \in K$. Denote by $A = K[\mathbf{u}]$, and by $\sigma_{\mathbf{u_0}} : A[\mathbf{x}] \to K[\mathbf{x}]$ the homomorphism corresponding to the specialization (substitution of $\mathbf{u}$ by some $\mathbf{u_0} \in K$).

A Gröbner System $GS(I, \succ_{\mathbf{x}})$ of the ideal $I \subset A[\mathbf{x}]$ wrt (with respect to) the termorder $\succ_{\mathbf{x}}$ is a set of pairs (S_i, B_i), where each couple consists of a constructible set (called segment) and of a collection of polynomials, such that

$$\begin{aligned}\mathrm{GS}(I, \succ_{\mathbf{x}}) = \{(S_i, B_i) \ : \ 1 \leq i \leq s, \ S_i \subset K^m, \ B_i \subset A[\mathbf{x}], \ \textstyle\bigcup_i S_i = K^m, \\ \forall \mathbf{u_0} \in S_i, \ \sigma_{\mathbf{u_0}}(B_i) \text{ is a Gröbner basis of } \sigma_{\mathbf{u_0}}(I) \text{ wrt } \succ_{\mathbf{x}}\}.\end{aligned}$$

The algorithm *MCCGS* (Minimal Canonical Comprehensive Gröbner System) [Mo06],[MaMo06] of the ideal $I \subset A[\mathbf{x}]$ wrt the monomial order $\succ_{\mathbf{x}}$ for the variables, builds up the unique Gröbner System having the following properties:

1. The segments S_i form a partition $\mathcal{S} = \{S_1, \ldots, S_s\}$ of the parameter space K^m.
2. The polynomials in B_i are normalized to have content 1 wrt $\mathbf{x}$ over $K[\mathbf{u}]$ (in order to work with polynomials instead of with rational functions). The B_i specialize to the reduced Gröbner basis of $\sigma_{\mathbf{u_0}}(I)$, keeping the same *lpp* (leading power products set) for each $\mathbf{u_0} \in S_i$, i.e. the leading coefficients are different from zero on every point of S_i. [4]. Thus a concrete set of *lpp* can be associated to a given S_i. Often it exists a unique segment corresponding to each particular *lpp*, although in some cases several such segments can occur. In any case, when a segment with the reduced basis [1] exists, then it is unique. When two segments S_i, S_j share the same *lpp*, then there is not a common reduced basis B specializing to both B_i, B_j [5].

   Moreover, there exists a unique segment S_1 (called the *generic segment*), containing a Zariski-open set, whose associated basis B_1 is called the *generic basis* and coincides with the Gröbner basis of I considered in $K(\mathbf{u})[\mathbf{x}]$ conveniently normalized without denominators and content 1 wrt $\mathbf{x}$.
3. The partition $\mathcal{S}$ is canonical (unique for a given I and monomial order).
4. The partition is minimal, in the sense it does not exists another partition having property 2 with less sets S_i.
5. The segments S_i are described in a canonical form.

[4] The polynomials in the B_i's are not faithful (they do not belong to I), as they are reduced wrt to the null conditions in S_i. By abuse of language we call them *reduced bases* (i.e. not-faithful, in the terminology of Weispfenning).

[5] M. Wibmer [Wib06] has proved that for homogeneous ideals in the projective space there is at most a unique reduced basis and segment corresponding to a given *lpp*.

As it is known, the *lpp* of the reduced Gröbner basis of an ideal determine the cardinal or dimension of the solution set over an algebraically closed field. This makes the *MCCGS* algorithm very useful for applications as it identifies canonically the different kind of solutions for every value of the parameters. This is particularly suitable for automatic theorem proving and automatic theorem predicting, as we will show in the following sections.

Let us give an example of the output of *MCCGS*.

Example 1. Consider the system described by the following parametric ideal (here the parameters are a, b, c, d):

$$I = (x^2 + by^2 + 2cxy + 2dx, 2x + 2cy + 2d, 2by + 2cx),$$

arising in the context of finding all possible singular conics and their singularities. Calling to the Maple implementation of *MCCGS* yields a graphical and an algebraic output. The graphical output is shown in Figure 2. It contains the basic information that is to be read as follows. At the root there is the given ideal (in red). The second level (also in red) contains the *lpp* of the bases of the three different possible cases. These are [1], corresponding to the no solution (no singular points) case; $[x, y]$, corresponding to the one solution (one singular point) case; and $[x]$, corresponding to the case of one dimensional solution (ie. when the conic is a double line). Below each case there is a subtree (in blue) describing the corresponding S_i, with the following conventions:

- at the nodes there are ideals of $K[\mathbf{u}]$, prime in the field of definition (generated over the prime field by the coefficients of a reduced G-Basis) of the given ideal $I \subset A[\mathbf{x}]$
- a descending edge means the set theoretic "difference" of the set defined by the node above minus the set defined at the node below,
- nodes at the same level, hanging from a common node, are to be interpreted as yielding the set theoretic "union" of the corresponding sets; they form the irredundant prime decomposition of a radical ideal of $K[\mathbf{u}]$.
- every branch contains a strictly ascending chain of prime ideals.

So, in the example above, the three cases, their *lpp* and the corresponding S_i's are to be read as shown in the following table:

lpp	Basis B_i	Description of S_i
$[1]$	$[1]$	$K^3 \setminus ((\mathbb{V}(b) \setminus (\mathbb{V}(c, b) \setminus \mathbb{V}(d, c, b))) \cup \mathbb{V}(d))$
$[y, x]$	$[2cy + d, x]$	$(\mathbb{V}(b) \setminus \mathbb{V}(c, b)) \cup \left(\mathbb{V}(d) \setminus \mathbb{V}(d, b - c^2)\right)$
$[x]$	$[x + cy]$	$\mathbb{V}(d, b - c^2)$

We remark that the B_i's do not appear in the Figure 2, since –in order to simplify the display– the complete bases are only given by the algebraic output of *MCCGS* and are not shown by the graphic output.

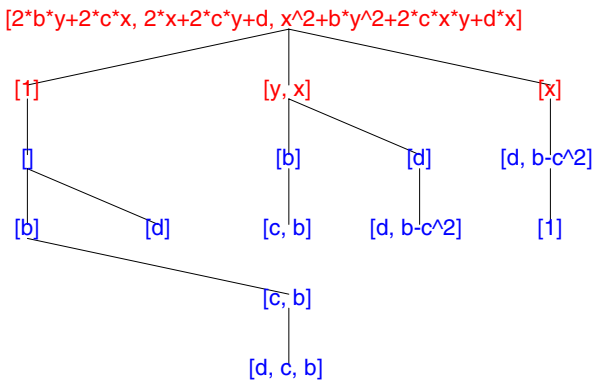

Fig. 2. *MCCGS* for the singular points of a conic

4 Using *MCCGS* for Automatic Theorem Discovering

Once we have briefly described the context for *MCCGS* and for automatic discovery, we are prepared to describe the basic idea in this paper. We can say that our goal is to show how performing a *MCCGS* procedure can improve the automatic discovery of geometry theorems.

Example 1 can be seen as a very simple example of theorem discovering. We could formulate the statement *a conic has one singular point* and try to find the conditions for the statement to be true. Without loss of generality we express the equation of the conic and its partial derivatives as

$$I = (x^2 + by^2 + 2cxy + 2dx, 2x + 2cy + 2d, 2by + 2cx),$$

and search for the values of the parameters where this system has a single solution. As shown above, we have found that the statement is true if and only if $\{b = 0, c \neq 0\}$ or if $\{d = 0, b - c^2 \neq 0\}$, since in the first segment of the table there is no solution ($B_1 = (1)$), while the third segment yields a 1-dimensional set of solutions.

In general, let $H \Rightarrow T$ be a statement expressed in terms of polynomial equations, where the ideals H, $T \subseteq K[x_1, \ldots, x_n]$ will be the corresponding hypotheses ideal and theses ideal (both, possibly, with several generators). In this context [DR] sets, as discovery goal, finding a couple of subsets of variables $U \supseteq U'$, with $X \supseteq U \supseteq U'$, and a couple of ideals $R' \subset K[U], R'' \subset K[U']$, so that the following properties hold for the associated algebraic varieties (over K^n, with K algebraically closed):

1. $\mathbb{V}(H + R'^e) \backslash \mathbb{V}(R''^e) \subseteq \mathbb{V}(T)$ (where the ^{e} stands for the extension of the ideal from its defining ring, say, $K[U]$ or $K[U']$, to $K[X]$);
2. $\mathbb{V}(H + T) \subseteq \mathbb{V}(R'^e)$;
3. $\mathbb{V}(H + R'^e) \backslash \mathbb{V}(R''^e) \neq \emptyset$.

The rationale behind such a definition is that such a couple (R', R'') is supposed to provide

- some necessary (as expressed by item 2) above)
- and sufficient (as expressed by item 1) above)

non trivial (as expressed by item 3)) complementary conditions of equality kind (given by R') and of non-degeneracy type (given by the negation of R'') for the given theses to hold under the given hypotheses.

Then it is shown in [DR] that, for a given couple of subsets of variables $U \supseteq U'$, with $X \supseteq U \supseteq U'$, there is a couple of ideals $R' \subset K[U], R'' \subset K[U']$ verifying properties 1), 2) and 3) above if and only if the couple of ideals $H' = (H+T) \cap K[U]$ and[6] $H'' = ((H + H'^e) : T^\infty) \cap K[U']$ also verify these three conditions. Moreover, Theorem 2 in [DR] shows these conditions hold if and only if $1 \notin (H')^c : H''^\infty$ (equivalently, iff $H'' \not\subseteq \sqrt{(H')^c}$), where ^{c} stands for the contraction ideal, so there is an algorithmic way of solving the posed discovery problem for a given statement and choice of variables.

Now we remark the following:

Proposition 1. *If there is a couple R', R'' verifying the above conditions, then*

$$\mathbb{V}(H + R'^e) \backslash \mathbb{V}(R''^e) = \mathbb{V}(H + H'^e) \backslash \mathbb{V}(R''^e)$$

Proof. First notice that $\mathbb{V}(H+H'^e) \subseteq \mathbb{V}(H+R'^e)$, since, by property 2), $\mathbb{V}(H+T) \subseteq \mathbb{V}(R'^e)$, thus $R'^e \subseteq \sqrt{H+T}$ and so $R' = R'^{ec} \subseteq \sqrt{H+T}^c = \sqrt{H'}$ and this implies that $\mathbb{V}(H'^e) \subseteq \mathbb{V}(R'^e)$.

Moreover, we have also that $\mathbb{V}(H + R'^e) \backslash \mathbb{V}(R''^e) \subseteq \mathbb{V}(T) \cap \mathbb{V}(H)$, by property 1), and $\mathbb{V}(T) \cap \mathbb{V}(H) \subseteq \mathbb{V}(H'^e)$, where the last inclusion follows from the definition of H'^e. We conclude that $\mathbb{V}(H + R'^e) \backslash \mathbb{V}(R''^e) \subseteq \mathbb{V}(H + H'^e) \backslash \mathbb{V}(R''^e)$.

This means that the search for candidates R' for complementary hypotheses of equality type, can be reduced to computing $\mathbb{V}(H')$. This is, precisely, the (Zariski closure of the) projection, over the parameter space of the U-variables, of $\mathbb{V}(H+T)$, and this can be computed through *MCCGS*, providing as well some other useful information (as in Corollary 1).

Proposition 2. *The projection of $\mathbb{V}(H+T)$ over the U-variables can be computed by performing a MCCGS for $I = H+T$ and $X \supset U$, discarding, if it exists, the unique segment S_i's with B_i equal to 1 and keeping the remaining S_i's.*

Proof. Since the segments of a *MCCGS* partition the parameter space U, it is enough to show that a point (u_0) is not in the projection if and only if it belongs to the S_i with associated $B_i = 1$. Now we recall that a reduced Gröbner basis is 1 if and only if the corresponding ideal is (1). Then, the ideal $H+T$ specialized at u_0 will be (1) if and only if its reduced G-basis is 1. Since we work over an algebraically closed field, this is the only case the system $H+T$, specialized at u_0,

[6] Let I, J be ideals of $K[X]$. Recall that $I : J = \{x, xJ \subset I\}$. Then, the *saturation of I by J* is defined as $I : J^\infty = \cup_n (I : J^n)$, cf. [KR00].

has no solution, ie. u_0 is not in the projection of $\mathbb{V}(H+T)$. But, by construction, a B_i specializes to 1 if and only if $B_i = 1$ (since the specialization must be a reduced G-basis and has the same *lpp* as B_i).

Corollary 1. *The union of these S_i's with associated $B_i \neq 1$ (ie. the complement of the only possible segment with $B_i = 1$) partitions the projection of $\mathbb{V}(H+T)$; that is, it holds $H \wedge T \Rightarrow \{\cup S_i\}$. Thus, the union of these S_i's provide complementary necessary conditions for the theses T to hold over H.*

We will see below (Remark 2) that, when the given statement does not hold over any geometrically meaningful component of the hypotheses variety – ie. in the automatic discovery situation– the segment with $B_i = 1$ is the generic one, so its complement provides necessary conditions for the theses T to hold over H.

Next we must study if some of these S_i's provide sufficient conditions, analyzing the behavior of each statement $H \wedge S_i \Rightarrow T$, for every segment S_i with lpp $\neq 1$. Some –perhaps all, perhaps none– of them could be true. Remark that, anyway, $H \wedge S_i \neq \emptyset$, since the associated basis in not 1. Remark, also, that *MCCGS* allows to obtain supplementary conditions S_i of the more general form (not every constructible set is the difference of two closed sets of the form $\mathbb{V}(H + R'^e)\backslash\mathbb{V}(R''^e)$, as in the previous approach).

There are some special easy cases, as shown in the next result.

Corollary 2. *For every segment S_i such that the corresponding lpp of the associated basis is, precisely, the collection of variables $\{x_1, \ldots, x_n\}$, we have that $\mathbb{V}(H) \cap S_i \subseteq \mathbb{V}(T)$, ie. $H \wedge S_i \Rightarrow T$ holds, and S_i provides sufficient conditions for T to hold over H.*

Proof. In fact, the condition on the associated *lpp* means that for every u_0 in S_i, the system $H(u_0, x) = 0, T(u_0, x) = 0$ has a unique solution, and it belongs to $\mathbb{V}(T)$. Thus $\mathbb{V}(H) \cap S_i \subseteq \mathbb{V}(T)$.

Otherwise, we should analyze, for each i with S_i involved in the projection of $\mathbb{V}(H + T)$, the validity of $H \wedge S_i \Rightarrow T$. This is a straightforward "automatic proving" step, and not of "automatic discovery", since adding again T to the collection of hypotheses $H \wedge S_i$ will not change the situation, as the projection of $\mathbb{V}(H) \cap \mathbb{V}(T) \cap S_i$ equals the projection of $\mathbb{V}(H) \cap S_i$, both being S_i.

Yet, *MCCGS* can provide a method for checking the truth of such statement $H \wedge S_i \Rightarrow T$. As it is well known, we can reformulate the hypotheses $H \wedge S_i$ as a collection of equality hypotheses H, since S_i is constructible and, then, the union of intersections of closed and open sets (in the Zariski topology). And open sets can be expressed through equalities by means of saturation techniques (such as $x \neq 0 \Leftrightarrow xy - 1 = 0$, etc.). So let us state the following propositions (adapting to the *MCCGS* context some results from [RV99], [DR]) in all generality.

Proposition 3. *Let $H \Rightarrow T$ be a statement and let U be a collection of variables independent for H. Then T vanishes identically on all the components of H where U remain independent if and only if, performing a MCCGS for $\{H, Tz-1\}$ with respect to U, the generic basis is 1.*

Proof. Notice the stated condition on the segments of the *MCCGS* is equivalent to the fact that the contraction $(H, Tz-1) \cap K[U] \neq (0)$. In fact, this contraction is zero if and only if the projection of $\mathbb{V}(H + (Tz - 1))$ contains an open set. And this is equivalent to the fact that the generic segment has lpp $\neq 1$.

Now, if $(H, Tz - 1) \cap K[U] \neq (0)$, take some $0 \neq g \in (H, Tz - 1) \cap K[U]$. Remark that, by construction, $g\,T = 0$ over $\mathbb{V}(H)$. If $T \neq 0$ at some point over some component of $\mathbb{V}(H)$, then $g = 0$ over such component; so it cannot be a component where the U are independent, since $g \in K[U]$.

Conversely, if T vanishes identically over all the independent components, then we can compute an element $g \in K[U]$ vanishing over the remaining components (because U' is dependent over them). So $g\,T$ vanishes all over $\mathbb{V}(H)$, and thus $(H, Tz - 1) \cap K[U'] \neq (0)$.

Remark 1. In fact, as in [CLLW], it is easy to show that the segment with associated *lpp* equal to 1 provides complementary sufficient conditions for $H \Rightarrow T$ to hold. In fact, for every $\mathbf{u_0}$ in such segment, $\mathbb{V}(H(\mathbf{u_0}, \mathbf{x}), T(\mathbf{u_0}, \mathbf{x})z - 1) = \emptyset$, so $\mathbb{V}(H(\mathbf{u_0}, \mathbf{x}) \subseteq T(\mathbf{u_0}, \mathbf{x})$. But it can happen there is no such segment.

Proposition 4. *Let $H \Rightarrow T$ be a statement and let U be a collection of variables independent for H and of dimension equal to* $\dim(H)$*. Then T vanishes identically on some components of H where U remains independent if and only if, performing a MCCGS for $\{H, T\}$ with respect to U, the reduced basis of the generic segment is different from 1.*

Proof. As above, the stated condition on the segments of the *MCCGS* is equivalent to the fact that the contraction $(H, T) \cap K[U'] = (0)$.

Now, if T does not vanish identically over any component of $\mathbb{V}(H)$ independent over U', the projection of $\mathbb{V}(H, T)$ over U will be a proper closed subset (since the dimension of the projection is less or equal than the dimension of the components of $\mathbb{V}(H)$ contained in $\mathbb{V}(T)$, the maximum dimension of all components of $\mathbb{V}(H)$ equals the maximum dimension of the independent components, and the dimension of the U-space equals the maximum dimension of the components of $\mathbb{V}(H)$). This contradicts the assumption $(H, T) \cap K[U] = (0)$, which implies the closure of the projection is the whole U-space.

Conversely, if T vanishes identically over some independent component (say, C) and $(H, T) \cap K[U] \neq (0)$, then we can choose an element $0 \neq g \in (H, T) \cap K[U]$. This element vanishes over any component of $\mathbb{V}(H)$ where T vanishes, in particular over C, contradicting its independence over U.

Remark 2. The last proposition can be also read in a different way: T does not vanish identically on any independent component of H if and only if the reduced basis of the generic segment is 1.

Corollary 3. *Let $H \Rightarrow T$ be a statement and let U be a collection of variables independent for H and of dimension equal to* $\dim(H)$*. Then T vanishes*

identically on some components of H where U remains independent and also T does not vanish identically on some other components of H where U remains independent if and only if

- *performing a MCCGS for $\{H, Tz-1\}$ with respect to U, the generic segment dos not have reduced basis 1, and*
- *performing a MCCGS for $\{H, T\}$ with respect to U, the reduced basis of the generic segment is also different from 1.*

In conclusion, using *MCCGS* one can determine, for a given statement, whether it is generally true (over all independent components, using Proposition 3, generally false (over all independent components, using Remark 2), or partially true and false (using Corollary 3). Let us call this last situation the "undecidable" case.

In fact, unfortunately, in this circumstance it is not possible, using only data on the U variables, to determine the components of H where T vanishes identically. Consider $H = b(b+1) \subseteq K[a,b]$, $T = (b)$ and take $U = \{a\}$. Here the projection of $\mathbb{V}(H, Tz-1)$ over the U-variables is the whole a-line, so does not have any segment with *lpp* equal to 1, and we know the thesis does not hold over all independent components. Moreover the projection of $\mathbb{V}(H+T)$ over the U-space is again the whole a-line, so there is no segment with *lpp* 1, and we can conclude T holds over a component, but there is no way of separating the component $b = 0$, by manipulating H, T in terms of polynomials in the variable a.

This discussion applies to the situation described above, when considering statements $H \wedge S_i \Rightarrow T$, where segment S_i belongs to a *MCCGS* for $\{H, T\}$ with respect to a collection U of variables and has lpp $\neq 1$. Let HH be the reformulation of $H \wedge S_i$ in terms of equalities and let (if possible) $U' \subseteq U$ be a new collection of variables, such that they are independent for HH and of dimension equal to $\dim(HH)$.

Then, as remarked above, $HH \Rightarrow T$ will be true on the segment SS_i of a *MCCGS* with respect to $HH, Tz-1$, with *lpp* 1. If it is is an open segment, then the statement $H \wedge S_i \Rightarrow T$ will be generally true (over all the components independent over U'). If it is not open segment, but there is at least one such segment, the statement will hold true under the new restrictions.

But if there is no segment at all with lpp $= 1$, then and only then we are in the undecidable case. In fact, over all points in the U'-projection of $\mathbb{V}(HH, Tz-1)$ we will have points of $\mathbb{V}(H)$ not in $\mathbb{V}(T)$ (because all the segments will have lpp $\neq 1$ in the *MCCGS* for $HH, Tz-1$) and also points of $\mathbb{V}(H)$ and $\mathbb{V}(T)$ (since we are also in the projection of S_i over U', and S_i corresponds to a segment of lpp $\neq 1$ for a *MCCGS* with respect to H, T).

In this case, since the projection over U' of $\mathbb{V}(HH, T)$ will be same as the projection of $\mathbb{V}(HH)$ (both being equal to the projection of S_i), it is of no use to go further with a new discovery procedure, computing a *MCCSG* for HH, T over U'. We know beforehand that all its segments will have lpp $\neq 1$, since over any point in the projection of S_i there will be always points on $\mathbb{V}(HH) \cap \mathbb{V}(T)$, confirming, again, that we are in the undecidable situation.

5 Examples

Let us see how this works in a collection of examples, where we have just detailed the discovery step (ie. computing the *MCCGS* of $\{H, T\}$ with respect to a collection of maximal independent variables for H, and then collecting the potentially true statements $H \wedge S_i \Rightarrow T$, where segment S_i has lpp $\neq 1$) in the procedure outlined in the previous Section. That is, we have not included here the formal automatic verification in each case that the newly found hypotheses actually lead to a true statement (the "proving step").

Example 2. (See also [DR]). Next, we will develop the above introduced notions considering a statement from [Ch88] (Example 91 in his book), suitably adapted to the discovery framework. The example here is taken from [DR].

Let us consider as given data a circle and two diametral opposed points on it (say, take a circle centered at $(1, 0)$ with radius 1, and let $C = (0, 0), D = (2, 0)$ the two ends of a diameter), plus an arbitrary point $A = (u_1, u_2)$. See Figure 3. Then trace a tangent from A to the circle and let $E = (x_1, x_2)$ be the tangency point. Let $F = (x_3, x_4)$ be the intersection of DE and CA. Then we claim that $AE = AF$. Moreover, in order to be able to define the lines DE, CA, we require, as hypotheses, that $D \neq E$ (ie. $u_1 \neq 2$) and that $C \neq A$ (ie. $u_1 \neq 0$ or $u_2 \neq 0$).

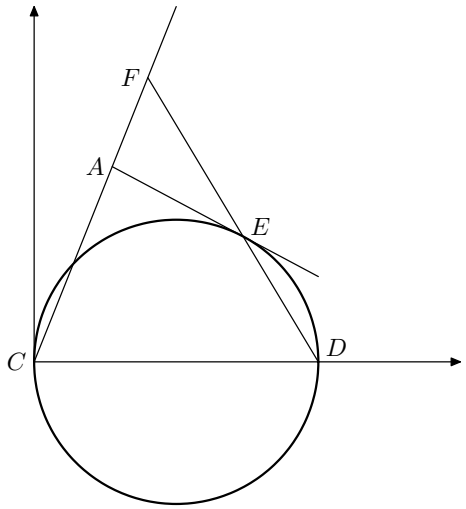

Fig. 3. Problem of Example 2

Now, using CoCoA [CNR99] and its package TP (for Theorem Proving), we translate the given situation as follows

```
Alias  TP   := $contrib/thmproving;

Use R::=Q[x[1..4],u[1..2]];
```

```
A:=[u[1],u[2]];
E:=[x[1],x[2]];
D:=[2,0];
F:=[x[3],x[4]];
C:=[0,0];

Ip1:=TP.Perpendicular([E,A],[E,[1,0]]);
Ip2:=TP.LenSquare([E,[1,0]])-1;
Ip3:=TP.Collinear([0,0],A,F);
Ip4:=TP.Collinear(D,E,F);

H:=Saturation(Ideal(Ip1,Ip2,Ip3,Ip4),Ideal(u[1]-2)*
                                    Ideal(u[1], u[2]));

T:=Ideal(TP.LenSquare([A,E])-TP.LenSquare([A,F]));
```

where T is the thesis and H describes the hypothesis ideal. Notice that $Ip1$ expresses that the segments $[E, A], [E, (1, 0)]$ are perpendicular; $Ip2$ states that the square of the length of $[E, (1, 0)]$ is 1 (so $Ip1, Ip2$ imply E is the tangency point from A); and the next two hypotheses express that the corresponding three points are collinear. The hypothesis ideal H is here constructed by using the *saturation* command, since it is a standard way of stating that the hypothesis variety is the (Zariski) closure of the set defined by all the conditions $Ip[i] = 0, i = 1 \dots 4$ minus the union $\{u[1] = 2\} \cup \{u[1] = 0, u[2] = 0\}$, as declared in the formulation of this example (but we refer to [DR] for a discussion on the two possible ways of introducing inequalities as hypotheses). Finally, the thesis expresses that the two segments $[AE], [AF]$ have equal non oriented length.

Now, let us use in this, clearly false, statement the approach of [RV99] or [DR] to discovery. First we check that the statement $H \to T$ is not algebraically true in any conceivable way. For instance, it turns that

```
Saturation(H, Saturation(H,T));
Ideal(1)
--------------------------------
```

and this computation shows that all possible non-degeneracy conditions (those polynomials $p(\mathbf{u}, \mathbf{x})$ that could be added to the hypotheses as conditions of the kind $p(\mathbf{u}, \mathbf{x}) \neq \mathbf{0}$) lie in the hypotheses ideal, yielding, therefore to an empty set of conditions of the kind $p \neq 0 \wedge p = 0$. This implies, in particular, that the same negative result would be obtained if we restrict the computations to some subset of variables, since the thesis does not vanish on any irreducible component of the hypotheses variety.

Thus we must switch on to the discovery protocol, checking before hand that $u[1], u[2]$ actually is a (maximal) set of independent variables –the parameters– for our construction:

```
Dim(R/H);
2
--------------------------------
```

```
Elim([x[1],x[2],x[3],x[4]],H);
Ideal(0)
------------------------------
```

Then we add the thesis to the hypotheses ideal and we eliminate all variables except $u[1], u[2]$

```
H':=Elim([x[1],x[2],x[3],x[4]],H+T);
H';
Ideal(-1/2u[1]^5 - 1/2u[1]^3u[2]^2 + u[1]^4)
------------------------------
Factor(-1/2u[1]^5 - 1/2u[1]^3u[2]^2 + u[1]^4);
[[u[1]^2 + u[2]^2 - 2u[1], 1], [u[1], 3], [-1/2, 1]]
------------------------------
```

yielding as complementary hypotheses the conditions $u[1]^2 + u[2]^2 - 2u[1] = 0 \vee u[1] = 0$ that can be interpreted by saying that either point A lies on the given circle or (when $u[1] = 0$) triangle $\Delta(A, C, D)$ is rectangle at C. In the next step of the discovery procedure we consider as new hypotheses ideal the set $H + H'$, which is of dimension 1 and where both $u[2]$ or $u[1]$ can be taken as independent variables ruling the new construction.

```
Dim(R/(H+H'));
1
------------------------------
Elim([x[1],x[2],x[3],x[4],u[1]],H+H');
Ideal(0)
------------------------------
Elim([x[1],x[2],x[3],x[4],u[2]],H+H');
Ideal(0)
```

Choosing, for example, $u[2]$ as relevant variable, we check –applying the usual automatic proving scheme– that the new statement $H \wedge H' \rightarrow T$ is correct under the non-degeneracy condition $u[2] \neq 0$:

```
H'':=Elim([x[1],x[2],x[3],x[4],u[1]], Saturation(H+H',T));
H'';
Ideal(u[2]^3)
------------------------------
```

Thus we have arrived to the following statement: Given a circle of radius 1 and centered at $(1, 0)$, and a point A not in the X-axis and lying either on the Y axis or in the circle, it holds that the segments AE, AF (where E is a tangency point from A to the circle and F is the intersection of the lines passing by $(2, 0), E$ and $A, (0, 0)$) are of equal length.

Let us now review Example 2 using *MCCGS*. As above, the hypotheses are the union of $H := H_1 \cup S$, where H_1 expresses the equality type constraints:

$$H_1 = [(x_1 - 1)(u_1 - x_1) + x_2(u_2 - x_2), (x_1 - 1)^2 + x_2^2 - 1, \\ u_1x_4 - u_2x_3, x_3x_2 - x_4x_1 - 2x_2 + 2x_4]$$

to which we have to add the saturation ideal expressing the inequality constraints:

$$\begin{aligned} S = [&u_1x_4 - u_2x_3, x_1u_1 - u_1 - x_1 + x_2u_2, x_4x_2 - 2x_2u_2 - x_3u_1 + 2u_1,\\ &x_4x_1 - 2x_1u_2 + u_2x_3, x_3x_2 - 2x_1u_2 + u_2x_3 - 2x_2 + 2x_4,\\ &x_1x_3 + x_3u_1 + 2x_2u_2 - 2x_1 - 2u_1, x_1^2 - 2x_1 + x_2^2,\\ &x_3u_1^2 + 2x_2u_2u_1 - 2u_2^2x_1 + u_2^2x_3 - 2u_1^2 - 2x_2u_2 + 2u_2x_4,\\ &x_3^2u_1 + x_4u_2x_3 + 2x_4^2 - 4x_3u_1 - 4u_2x_4 + 4u_1,\\ &u_1x_2^2 - x_1x_2u_2 - x_2^2 + x_2u_2 + x_1 - u_1,\\ &u_2x_3^3 + u_2x_4^2x_3 + 2x_4^3 - 4u_2x_3^2 - 4u_2x_4^2 + 4u_2x_3]. \end{aligned}$$

The thesis is

$$T = (u_1 - x_1)^2 + (u_2 - x_2)^2 - (u_1 - x_3)^2 - (u_2 - x_4)^2.$$

Calling now $\mathrm{mccgs}(H_1 \cup S \cup T, \mathrm{lex}(x_1, x_2, x_3, x_4), \mathrm{lex}(u_1, u_2))$ one obtains the following segments:

Segment	lpp	Description of S_i
1	$[1]$	$K^2 \setminus (\mathbb{V}(u_1^2 + u_2^2 - 2u_1) \cup \mathbb{V}(u_1))$
2	$[x_4^2, x_3, x_2, x_1]$	$\mathbb{V}(u_1^2 + u_2^2 - 2u_1) \setminus (\mathbb{V}(u_1 - 2, u_2) \cup \mathbb{V}(u_1, u_2))$
3	$[x_4^2, x_3, x_2, x_1]$	$\mathbb{V}(u_1) \setminus (\mathbb{V}(u_1, u_2^2 + 1) \cup \mathbb{V}(u_1, u_2))$
4	$[x_4, x_3, x_2, x_1]$	$\mathbb{V}(u_1, u_2^2 + 1)$
5	$[x_4^2, x_3, x_2^2, x_1]$	$\mathbb{V}(u_1 - 2, u_2)$
6	$[x_4^2, x_3^2, x_2, x_1]$	$\mathbb{V}(u_2, u_1)$

Segment S_1 states that point $A(u_1, u_2)$ must lie either in the Y-axis or on the circle, as a necessary condition in the parameter space $\mathbf{u} = (u_1, u_2)$ for the existence of solutions, in the hypotheses plus thesis variety, lying over $\mathbf{u}$. This essentially agrees with the result obtained in [DR].

A detailed analysis of the remaining segments show a variety of formulas for determining the (sometimes not unique) values of points $E(x_1, x_2)$ and $F(x_3, x_4)$ –verifying the theorem– over the corresponding parameter values.

For completeness we give the different bases associated, in the different segments, to the above ideal of thesis plus hypotheses

$$\begin{aligned} B_1 &= [1]\\ B_2 &= [u_2^2 + x_4^2 - 2u_2x_4, -u_1x_4 + u_2x_3, u_2^3 - 2u_2u_1 + x_2u_2^2 + (-2u_2^2 + 2u_1)x_4,\\ &\quad u_2u_1 + x_1u_2 - 2u_1x_4]\\ B_3 &= [-2u_2x_4 + x_4^2, x_3, (u_2^2 + 1)x_2 - x_4, (u_2^2 + 1)x_1 - u_2x_4]\\ B_4 &= [x_4, x_3, x_2, x_1]\\ B_5 &= [x_4, -4 + 2x_3, x_2^2, -2 + x_1]\\ B_6 &= [x_4^2, x_3^2, -x_3x_4 + 2x_2 - 2x_4, 2x_1] \end{aligned}$$

Example 3. Next we consider the problem[7] described in Figure 4. Take a circle $\mathcal{C}$ with center at $O(0, 0)$ and radius 1 and let us denote points $A = (-1, 0)$ and

[7] We thankfully acknowledge here that this problem was suggested by a colleague, Manel Udina.

$B = (0, 1)$. Let D be an arbitrary point with coordinates $D = (1 + a, b)$ and let $C = (1 + a, 0)$ be another point in the X-axis, lying under point D. Then trace the line BC. Assume this line intersects the circle $\mathcal{C}$ at point $P(x, y)$.

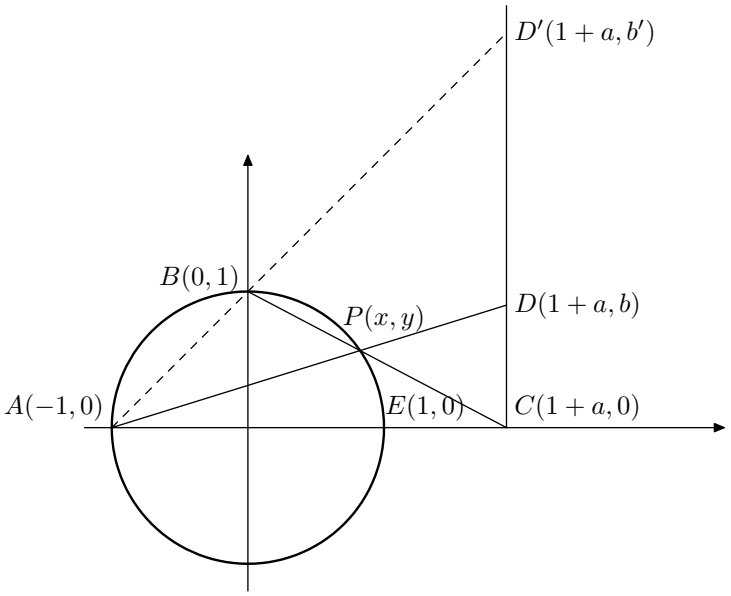

Fig. 4. Example 3

Consider now the, in general false, statement *"the points A, P, D are aligned"*. We want to discover the conditions on the parameters a, b for the statement to be true. The set of hypotheses plus thesis equations are very simple:

$$HT = [x^2 + y^2 - 1, -x + 1 - y + a - ay, -2y + b + xb - ay]$$

Take x, y as variables and a, b as parameters and call mccgs(HT, lex(x, y), lex(a, b)). The graphical output of the algorithm can be seen in Figure 5, and the algebraic description appears in the following table.

lpp	Basis B_i	Description of S_i
$[1]$	$[1]$	$(K^2 \setminus (\mathbb{V}(a-b) \setminus \mathbb{V}(a-b, (b+1)^2+1)))$ $\cup\ (K^2 \setminus \mathbb{V}(2+a))$ $\cup\ (K^2 \setminus \mathbb{V}(a-b+2))$
$[y, x]$	$[x^2 + y^2 - 1,$ $x + (a+1)(y-1),$ $b(x+1) - (a+2)y]$	$(\mathbb{V}(a-b) \setminus \mathbb{V}(a-b, (b+1)^2+1))$ $\cup\ (\mathbb{V}(2+a) \setminus \mathbb{V}(b, 2+a))$ $\cup\ (\mathbb{V}(a-b+2) \setminus \mathbb{V}(b, 2+a))$
$[y^2, x]$	$[y(y-1), 1+x-y]$	$\mathbb{V}(b, 2+a)$

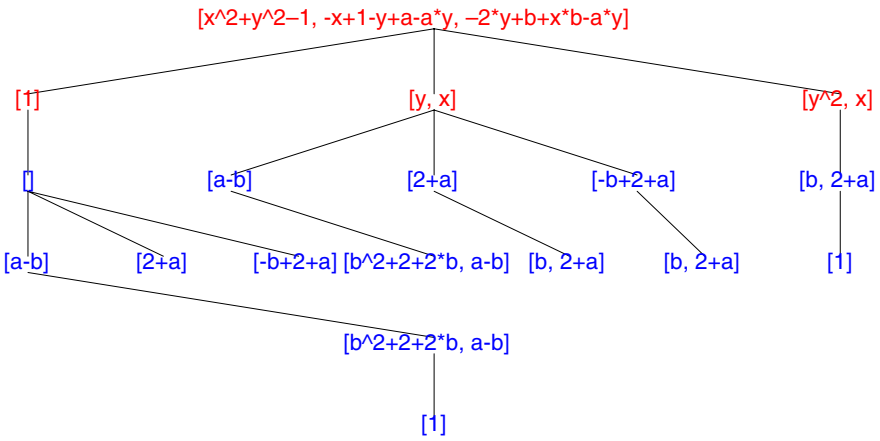

Fig. 5. Canonical tree for Example 3

As we see, the generic case has basis [1] showing that the statement is false in general. The interesting case corresponds, as it is usually expected, to the case with lpp $= [x, y]$, providing a unique solution for P. The description of the parameter set associated to this basis gives the union of three different locally closed sets, namely $\mathbb{V}(a-b) \setminus \mathbb{V}(a-b, (b+1)^2+1)$, $\mathbb{V}(2+a) \setminus \mathbb{V}(b, 2+a)$ and $\mathbb{V}(a-b+2) \setminus \mathbb{V}(b, 2+a)$, expressing complementary hypotheses for the statement to hold.

The first set is (perhaps) the expected one, corresponding to the case $a = b$ (except for the degenerate complex point (b, b) with $(b+1)^2+1 = 0$, without interest from the real point of view). Thus we can say that the statement holds if point C is equidistant from point D and point E.

The second set yields $a = -2$ and corresponds to the situation where point D is on the tangent to the circle trough the point $(-1, 0)$ (except for the degenerate case $b = 0$). In this case $P = A$ and, obviously, A, P, D are aligned (even in the degenerate case, as stated in the third segment, corresponding to the lpp $= [y^2, x]$).

Finally, the third set gives the condition $b = a + 2$ and it is also interesting, since it corresponds to the case where the intersecting point of the line BC with the circle is taken to be B instead of P, and then point D' should be in the vertical of C and at distance $D'C$ equal to distance EC plus two.

Example 4. [Isosceles orthic triangle]

In [DR] the conditions for the orthic triangle of a given triangle (that is, the triangle built up by the feet of the altitudes of the given triangle over each side) to the equilateral have been discovered. Next example aims to discover conditions for a given triangle in order to have an isosceles orthic triangle.

Consider the triangle of Figure 1 with vertices $A(-1, 0)$, $B(1, 0)$ and $C(a, b)$, corresponding to a generic triangle having one side of length 2. Denote by

$P_1(a,0)$, $P_2(x_2,y_2)$, $P_3(x_3,y_3)$ the feet of the altitudes of the given triangle, ie. the vertices of the orthic triangle. The equations defining these vertices are:

$$H = \left.\begin{array}{r} (a-1)\,y_2 - b\,(x_2-1) = 0, \\ (a-1)\,(x_2+1) + b\,y_2 = 0, \\ (a+1)\,y_3 - b\,(x_3+1) = 0, \\ (a+1)\,(x_3-1) + b\,y_3 = 0, \end{array}\right\}$$

Now let us add the condition $\overline{P_1P_3} = \overline{P_1P_2}$.

$$T = (x_3-a)^2 + y_3^2 - (x_2-a)^2 - y_2^2 = 0.$$

Take x_2, x_3, y_2, y_3 as variables and a, b as free parameters and call

$$\mathrm{mccgs}(H \cup T, \mathrm{lex}(x_2,x_3,y_2,y_3), \mathrm{lex}(a,b)).$$

The output has now four segments. The generic case, with lpp = [1], meaning that the orthic triangle is, in general, not isosceles; one interesting case with lpp = $[y_3, y_2, x_3, x_2]$; and two more cases we can call degenerate, with *lpp*'s $[y_2, x_3^2, x_2]$ and $[y_2, x_3, x_2^2]$, respectively. For the interesting case we show the graphic output in Figure 6. Its basis is

$$B_2 = [(a^2+b^2+2a+1)y_3 - 2ab - 2b, (a^2+b^2-2a+1)y_2 + 2ab - 2b,$$
$$(a^2+b^2+2a+1)x_3 - a^2 + b^2 - 2a - 1, (a^2+b^2-2a+1)x_2 + a^2 - b^2 - 2a + 1].$$

Next table shows the description of the *lpp* and the S_i's for the the four cases:

lpp	Description of S_i
[1]	$K^2 \setminus ((\mathbb{V}(a) \setminus \mathbb{V}(b^2+1,a))$ $\cup\ (\mathbb{V}(a^2-b^2-1) \setminus \mathbb{V}(b^2+1,a))$ $\cup\ \mathbb{V}(a^2+b^2-1))$
$[y_3, y_2, x_3, x_2]$	$\mathbb{V}(a) \setminus \mathbb{V}(b^2+1,a)$ $\cup\ \mathbb{V}(a^2+b^2-1) \setminus (\mathbb{V}(b,a-1) \cup \mathbb{V}(b,a+1))$ $\cup\ (\mathbb{V}(a^2-b^2-1) \setminus (\mathbb{V}(b^2+1,a) \cup \mathbb{V}(b,a-1) \cup \mathbb{V}(b,a+1))$
$[y_2, x_3^2, x_2]$	$\mathbb{V}(b,a+1)$
$[y_2, x_3, x_2^2]$	$\mathbb{V}(b,a-1)$

The description of the parameter set (over the reals) for which the theorem is potentially true and no degenerate can be phrased as follows:

1) $a = 0$
2) $a^2 + b^2 = 1$ except the points $(1,0)$ and $(-1,0)$
3) $a^2 - b^2 = 1$ except the points $(1,0)$ and $(-1,0)$

This set is represented in Figure 7. and corresponds to

1) The given triangle is itself isosceles ($a = 0$);
2) The given triangle is rectangular at vertex C (with vertices $A(-1,0)$, $B(1,0)$ and the vertex $C(a,b)$ inscribed in the circle $a^2 + b^2 = 1$,

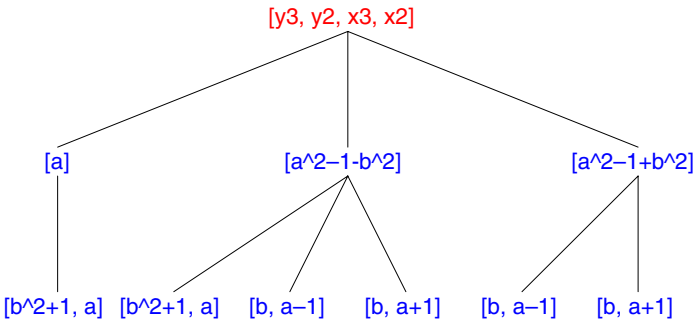

Fig. 6. Canonical tree branch for lpp $= [y_3, y_2, x_3, x_2]$ in Example 4

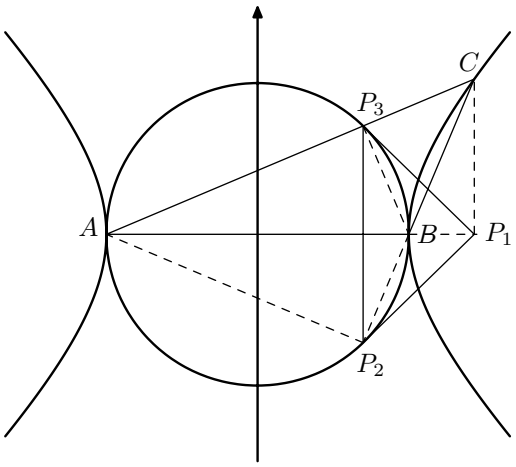

Fig. 7. Solutions of Example 4

3) The given triangle has vertices $A(-1,0)$, $B(1,0)$ and vertex $C(a,b)$ lies on the hyperbola $a^2 - b^2 = 1$.

Solution 1) is, perhaps, not surprising. Solution 2) corresponds to rectangular triangles for which the orthic triangle reduces to a line, that can be considered a degenerate isosceles triangle. But solution 3) is a nice novelty: it exists a one parameter family of non-isosceles triangles having isosceles orthic triangles.

The remaining two cases in the *MCCGS* output with lpp $= [y_2, x_3^2, x_2]$ and lpp$=$ $[y_2, x_3, x_2^2]$ represent degenerate triangles without geometric interest (namely $C = A$ and $C = B$).

Thus, after performing an automatic proving procedure for the new hypotheses, we can formulate the following theorem:

Theorem 1. *Given a triangle with vertices* $A(-1,0)$, $B(1,0)$ *and* $C(a,b)$, *its orthic triangle will be isosceles if and only if vertex* C *lies either on the line*

$a = 0$ *(and then the given triangle is itself isosceles) or in the circle* $a^2 + b^2 = 1$ *(and then it is rectangular) or in the hyperbola* $a^2 - b^2 = 1$.

Example 5. [Skaters]
Our final example is taken from the pastimes section of the French journal *Le Monde*, published on the printed edition of Jan. 8, 2007. This example is there attributed to E. Busser and G. Cohen. We think it is nice from *Le Monde* to include the proof of a theorem as a pastime. Actually, the statement to be proved was presented as arising from a more down-to-earth situation: two ice-skaters are moving forming two intersecting circles, at same speed and with the same sense of rotation. They both depart from one of the points of intersection of the two circles. Then the journal asked to show that the two skaters were always aligned with the other point of intersection (where some young lady, both skaters were interested at, was placed...).

Let us translate this problem into a theorem discovering question, as follows.

We will consider two circles with centers at $P(a, 1)$ and $Q(-b, 1)$ and radius $r_1^2 = a^2 + 1$ and $r_2^2 = b^2 + 1$, as shown in Figure 8, intersecting at points $O(0, 0)$ and $M(0, 2)$. Consider generic points –the skaters– $A(x_1, y_1)$ and $B(x_2, y_2)$ on the respective circles. Point A will be parametrized by the oriented angle $v = \widehat{OPA}$ and, correspondingly, point B will describe the oriented angle $w = \widehat{OQB}$. Therefore we can say that angle zero corresponds to the departing location of both skaters, namely, point O.

We claim that, for whatever position of points A, B, *the points* A, M, B *are aligned*, which is obviously false in general. But we want to determine if there is a relation between the two oriented angles making this statement to hold true. Denote c_v, s_v, c_w, s_w the cosine and sine of the angles v and w. It is easy to establish the basic hypotheses, using scalar products:

$$H_1 = [(x_1 - a)^2 + (y_1 - 1)^2 - a^2 - 1, (x_2 + b)^2 + (y_2 - 1)^2 - b^2 - 1, \\ a(x_1 - a) + (y_1 - 1) + (a^2 + 1)c_v, -b(x_2 + b) + (y_2 - 1) + (1 + b^2)c_w$$

Now, as the angles are to be taken oriented (because we assume the skaters tare moving on the corresponding circle in the same sense), we need to add the vectorial products involving also the sine to determine exactly the angles and not only their cosines. So we add the hypotheses:

$$H_2 = [a(y_1 - 1) - (x_1 - a) + (a^2 + 1)s_v, -b(y_2 - 1) - (x_2 + b) + (b^2 + 1)s_w]$$

The thesis is, clearly:

$$T = x_1 y_2 - 2x_1 - x_2 y_1 + 2x_2.$$

The radii of the circles are

$$r_1^2 = a^2 + 1 \text{ and } r_2^2 = b^2 + 1$$

and for $r_1 \neq 0$ and $r_2 \neq 0$ we have

$$c_{v_0} = \cos v_0 = \cos \widehat{OPM} = \frac{a^2 - 1}{a^2 + 1}, \; s_{v_0} = \sin v_0 = \sin \widehat{OPM} = \frac{-2a}{a^2 + 1}, \\ c_{w_0} = \cos w_0 = \cos \widehat{OQM} = \frac{b^2 - 1}{b^2 + 1}, \; s_{w_0} = \sin w_0 = \sin \widehat{OQM} = \frac{2b}{b^2 + 1}.$$

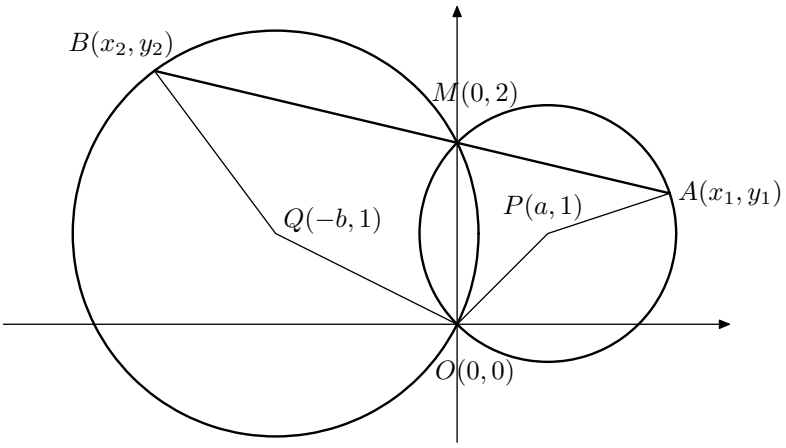

Fig. 8. Skaters problem

We want to take a, b and the angles v and w –in terms of the sines and cosines– as parameters. So we must introduce the constraints on the sine and cosine parameters. Moreover, we notice there are also some obvious degenerate situations, namely $r_1 = 0$, $r_2 = 0$ and $a + b = 0$, corresponding to null radii or coincident circles, and we want to avoid them.

Currently, *MCCGS* allows us to introduce all these constraints in order to discuss the parametric system. The call is now

$$\begin{aligned}&\text{mccgs}(H_1 \cup H_2 \cup T,\ \text{lex}(x_1, y_1, x_2, y_2),\ \text{lex}(a, b, s_v, c_v, s_w, c_w),\\ &\qquad \text{null} = [c_v^2 + s_v^2 - 1, c_w^2 + s_w^2 - 1],\ \text{notnull} = \{a^2 + 1, b^2 + 1, a + b\}).\end{aligned}$$

including the constraints on the parameters and eluding degenerate situations as options for *MCCGS*.

The result is that *MCCGS* outputs only 2 cases. The first one has basis [1], showing that, in general, there is no solution to our query. The second one has $\text{lpp} = [y_2, x_2, y_1, x_1]$ determining in a unique form the points A and B for the given values of the parameters. The associated basis is

$$[y_2 + c_w - bs_w - 1, x_2 - bc_w - s_w + b, y_1 + c_v + as_v - 1, x_1 + ac_v - s_v - a]$$

with parameter conditions that can be expressed as the union of three irreducible varieties:

$$\begin{aligned}V_1 &= \mathbb{V}(c_w^2 + s_w^2 - 1, c_v - c_w, s_v - s_w)\\ V_2 &= \mathbb{V}(c_w^2 + s_w^2 - 1, c_v^2 + s_v^2 - 1, s_w + bc_w - b, bs_w - c_w - 1)\\ V_3 &= \mathbb{V}(c_w^2 + s_w^2 - 1, c_v^2 + s_v^2 - 1, -s_v + ac_v - a, as_v + c_v + 1)\end{aligned}$$

The interpretation is easy: V_1 corresponds to arbitrary a, b, w, plus the essential condition $v = w$, which is the interesting case, stating that our conjecture

requires (and it is easy to show that this condition is sufficient) that both skaters keep moving with the same angular speed.

V_2 corresponds to $s_w = s_{w_0},\ c_w = c_{w_0}$ and a, b, v free, thus $B = M$ and A can take any position.

V_3 is analogous to V_2, and corresponds to placing $A = M$ and B anywhere.

So we can summarize the above discussion in the following

Theorem 2. *Given two non coincident circles of non-null radii and centers P and Q, intersecting at two points O and M, let us consider points A, B on each of the circles. Then the three points A, M, B are aligned if and only if the oriented angles $\widehat{OPA}$ and $\widehat{OQB}$ are equal or A or B or both coincide with M.*

6 Performances

Although the principal advantage of *MCCGS* in relation to other CGS algorithms is the simplicity and properties of the output: the minimal number of segments and the characterization of the type of the solution depending on the values of the parameters, the computer implementation[8] of the corresponding package, named *dpgb* release 7.0, in *Maple 8* is relatively short time consuming. Moreover,we think that no other actual PCAD software will be able to obtain the accurate result obtained, for example, in example 13. We give here a table with the CPU time and number of segments for the examples of the paper.

Example	CPU time (sec.)	Number of segments
1	1.9	3
2	12.8	6
3	0.98	3
4	4.4	4
5	129.4	2

The computations were done with a Pentium(R) 4 CPU at 3.40 Ghz and 1.00 GB RAM.

7 Conclusion

We have briefly introduced the principles of automatic discovery and also the ideas –in the context of comprehensive Gröbner basis– for discussing polynomial systems with parameters, via the new *MCCGS* algorithm. Then we have shown how natural is to merge both concepts, since the parameter discussion can be interpreted as yielding, in particular, the projection of the system solution set over the parameter space; and since the conditions for discovery can be obtained by the elimination of the dependent variables over the ideal of hypotheses and

[8] That can be freely obtained at http://www-ma2.upc.edu/∼montes

thesis. Moreover, we have also remarked how the approach through *MCCGS* provides new candidate complementary conditions of more general type and, in some particular instances (segments of the parameter space yielding to unique solution), quite common in our examples, an easy test for the sufficiency of these conditions. Finally, the use of *MCCGS* for automatic proving has been presented, as part of a formal discussion on the limitations of the discovery method.

We have exemplified this approach through a collection of non-trivial examples (performed by running the current Maple implementation of *MCCGS*, see [MaMo06], over a laptop, without special time – a few seconds– or memory requirements), showing that in all cases, the *MCCGS* output is very suitable to providing geometric insight, allowing the actual discovery of interesting and new? theorems (and pastimes!).

References

[BDR] Beltrán, C., Dalzotto, G., Recio, T.: The moment of truth in automatic theorem proving in elementary geometry. In: Botana, F., Roanes-Lozano, E. (eds.) Proceedings ADG 2006 (extended abstracts), Universidad de Vigo (2006)

[BR05] Botana, F., Recio, T.: Towards solving the dynamic geometry bottleneck via a symbolic approach. In: Hong, H., Wang, D. (eds.) ADG 2004. LNCS (LNAI), vol. 3763, pp. 92–111. Springer, Heidelberg (2006)

[CLLW] Chen, X.F., Li, P., Lin, L., Wang, D.K.: Proving geometric theorems by partitioned-parametric Gröbner bases. In: Hong, H., Wang, D. (eds.) ADG 2004. LNCS (LNAI), vol. 3763, pp. 34–44. Springer, Heidelberg (2005)

[CW] Chen, X.F., Wang, D.K.: The projection of a quasivariety and its application on geometry theorem proving and formula deduction. In: Winkler, F. (ed.) ADG 2002. LNCS (LNAI), vol. 2930, pp. 21–30. Springer, Heidelberg (2004)

[Ch84] Chou, S.-C.: Proving Elementary Geometry Theorems Using Wu's Algorithm Contemporary Mathematics. Automated Theorem Proving: After 25 Years, American Mathematical Society, Providence, Rhode Island 29, 243–286 (1984)

[Ch85] Chou, S.-C.: Proving and discovering theorems in elementary geometries using Wu's method Ph.D. Thesis, Department of Mathematics, University of Texas, Austin (1985)

[Ch87] Chou, S.C.: A Method for Mechanical Derivation of Formulas in Elementary Geometry. Journal of Automated Reasoning 3, 291–299 (1987)

[Ch88] Chou, S.-C.: Mechanical Geometry Theorem Proving. Mathematics and its Applications, D. Reidel Publ. Comp. (1988)

[ChG90] Chou, S.-C., Gao, X.-S.: Methods for Mechanical Geometry Formula Deriving. In: Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 265–270. ACM Press, New York (1990)

[CNR99] Capani, A., Niesi, G., Robbiano, L.: CoCoA, a System for Doing Computations in Commutative Algebra. The version 4.6 is available at the web site, `http://cocoa.dima.unige.it`

[DR] Dalzotto, G., Recio, T.: On protocols for the automated discovery of theorems in elementary geometry. J. Automated Reasoning (submitted)

[DG] Dolzmann, A., Gilch, L.: Generic Hermitian Quantifier Elimination. In: Buchberger, B., Campbell, J.A. (eds.) AISC 2004. LNCS (LNAI), vol. 3249, pp. 80–93. Springer, Heidelberg (2004)

[DSW] Dolzmann, A., Sturm, T., Weispfenning, V.: A new approach for automatic theorem proving in real geometry. Journal of Automated Reasoning 21(3), 357–380 (1998)

[K86] Kapur, D.: Using Gröbner basis to reason about geometry problems. J. Symbolic Computation 2(4), 399–408 (1986)

[K89] Kapur, D.: Wu's method and its application to perspective viewing. In: Kapur, D., Mundy, J.L. (eds.) Geometric Reasoning, The MIT press, Cambridge (1989)

[K95] Kapur, D.: An approach to solving systems of parametric polynomial equations. In: Saraswat, Van Hentenryck (eds.) Principles and Practice of Constraint Programming, MIT Press, Cambridge (1995)

[KR00] Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 1. Springer, Heidelberg (2000)

[Ko] Koepf, W.: Gröbner bases and triangles. The International Journal of Computer Algebra in Mathematics Education 4(4), 371–386 (1998)

[MaMo05] Manubens, M., Montes, A.: Improving DISPGB Algorithm Using the Discriminant Ideal. Jour. Symb. Comp. 41, 1245–1263 (2006)

[MaMo06] Manubens, M., Montes, A.: Minimal Canonical Comprehensive Groebner System. arXiv: math.AC/0611948. (2006)

[Mo02] Montes, A.: New Algorithm for Discussing Gröbner Bases with Parameters. Jour. Symb. Comp. 33(1-2), 183–208 (2002)

[Mo06] Montes, A.: About the canonical discussion of polynomial systems with parameters. arXiv: math.AC/0601674 (2006)

[R98] Recio, T.: Cálculo simbólico y geométrico. Editorial Síntesis, Madrid (1998)

[RV99] Recio, T., Pilar, M., Pilar Vélez, M.: Automatic Discovery of Theorems in Elementary Geometry. J. Automat. Reason. 23, 63–82 (1999)

[RB] Recio, T., Botana, F.: Where the truth lies (in automatic theorem proving in elementary geometry). In: Laganà, A., Gavrilova, M., Kumar, V., Mun, Y., Tan, C.J.K., Gervasi, O. (eds.) ICCSA 2004. LNCS, vol. 3044, pp. 761–771. Springer, Heidelberg (2004)

[Ri] Richard, P.: Raisonnement et stratégies de preuve dans l'enseignement des mathématiques. Peter Lang Editorial, Berne (2004)

[SS] Seidl, A., Sturm, T.: A generic projection operator for partial cylindrical algebraic decomposition. In: Sendra, R. (ed.) ISSAC 2003. Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, Philadelphia, Pennsylvania, pp. 240–247. ACM Press, New York (2003)

[St] Sturm, T.: Real Quantifier Elimination in Geometry. Doctoral dissertation, Department of Mathematics and Computer Science. University of Passau, Germany, D-94030 Passau, Germany (December 1999)

[Wa98] Wang, D.: Gröbner Bases Applied to Geometric Theorem Proving and Discovering. In: Buchberger, B., Winkler, F. (eds.) Gröbner Bases and Applications, 251th edn. London Mathematical Society Lecture Notes Series, vol. 251, pp. 281–301. Cambridge University Press, Cambridge (1998)

[Weis92] Weispfenning, V.: Comprehensive Grobner bases. Journal of Symbolic Computation 14(1), 1–29 (1992)

[Wib06] Wibmer, M.: Gröbner bases for families of affine or projective schemes. arXiv: math.AC/0608019. (2006)