T. Recio, J.Rafael Sendra, C. Villarino. The Importance of Being Zero. Proceedings of the 2018 ISSAC. pp. 327-333. ACM Press. And it is available at ACM https://doi.org/10.1145/3208976.3208981

The Importance of Being Zero*

Tomás Recio
Departamento de Matemáticas,
Universidad de Cantabria
Santander, Spain
tomas.recio@unican.es

J.Rafael Sendra
Dep. de Física y Matemáticas,
Research Group ASYNAC,
Universidad de Alcalá.
Alcalá de Henares, Madrid, Spain
rafael.sendra@uah.es

Carlos Villarino
Dep. de Física y Matemáticas,
Research Group ASYNAC,
Universidad de Alcalá.
Alcalá de Henares, Madrid, Spain
carlos.villarino@uah.es

ABSTRACT

We present a deterministic algorithm for deciding if a polynomial ideal, with coefficients in an algebraically closed field $\mathbb{K}$ of characteristic zero, of which we know just some very limited data, namely: the number n of variables, and some upper bound for the geometric degree of its zero set in $\mathbb{K}^n$, is or not the zero ideal. The algorithm performs just a finite number of decisions to check whether a point is or not in the zero set of the ideal. Moreover, we extend this technique to test, in the same fashion, if the elimination of some variables in the given ideal yields or not the zero ideal. Finally, the role of this technique in the context of automated theorem proving of elementary geometry statements, is presented, with references to recent documents describing the excellent performance of the already existing prototype version, implemented in GeoGebra.

CCS CONCEPTS

• **Computing Methodologies; Symbolic and algebraic manipulation; Algebraic algorithms**;

KEYWORDS

zero-test, polynomial ideals, Schwartz-Zippel Lemma, automated reasoning in geometry, proving by examples, GeoGebra,

ACM Reference Format:
Tomás Recio, J.Rafael Sendra, and Carlos Villarino. 2018. The Importance of Being Zero. In *ISSAC '18: 2018 ACM International Symposium on Symbolic and Algebraic Computation, July 16–19, 2018, New York, NY, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3208976.3208981

1 INTRODUCTION

Let us suppose we are given, as a query, an ideal $\mathrm{I} \subset \mathbb{K}[x_1, \ldots, x_n]$, with coefficients in an algebraically closed field $\mathbb{K}$ of characteristic zero, of which we know just some very limited data: the number n of variables, and some upper bound for the geometric degree (in the sense of [6], see Definition 2.1 below) of its zero set in $\mathbb{K}^n$, whether the ideal is not zero. Moreover, we have an oracle that allows us to check, given a point in $\mathbb{K}^n$, whether this point is or not in the zero set of I. Our first goal is to present an algorithm to conclude, by just using this protocol, whether I is the identically zero ideal or not.

As a trivial example, suppose that we deal with some unknown ideal $\mathrm{I} \subseteq \mathbb{K}[x]$, i.e. $n = 1$, and assume that we know that, if the given ideal is not zero, the cardinal of its roots (that is, in the one variable case, the geometric degree) will be bounded by d. Then, choose $d + 1$ different points in $\mathbb{K}$ and, for each of them, check if it is a root of I. If it is so in all cases, it is obvious that we are going beyond the given number of roots bound, so the ideal I must be identically zero. Else, if we have found a point in $\mathbb{K}$ which is not a zero of I, it is also obvious to conclude that I can not be zero.

The problem of detecting, by evaluation on a finite number of instances, whether a polynomial is or not zero, is a classical issue in computer algebra and complexity theory. It is impossible to summarize in a few references the state of the art. We can just mention the classical, purely algebraic, statement bounding the number of the required instances for zero-testing in [24]; the probabilistic approach in the Schwartz-Zippel Lemma [26], [22], with a curious history behind [16] that shows the wide interest of the scientific community concerning this problem; the research on *questor set* related to the BPP (Bounded error Probability Polynomial) time, as in [7], see also [18] and [19] for a historical account, etc.

It must be clarified that in most of these contributions the *rigurous* or *deterministic* approach to zero testing is not the relevant goal, since it is considered both well known (in classical references as [24]) and unpractical, for the involved exponential number of required tests. Instead, their objective is to find some feasible strategies for zero-testing with high probability.

Our contribution here goes in a different direction. First of all, a relative novelty could be the extension of the exact zero-testing protocol, from polynomials to ideals in polynomial rings of several variables (see [5], Section 2, and [17], Section 4, for related results). Let us remark that our goal is to find a kind of universal zero-testing set, i.e. we are looking for a single set to perform the test to all ideals of given bounded degree and embedded in the same polynomial ring.

In Section 2 we have accomplished this goal by introducing the notion of test-sets (playing a similar role to a fixed collection of $d+1$ points on a line, for testing the vanishing of degree d univariate polynomials), proving that this property can be reduced to testing hypersurfaces (Theorem 2.3), that it is kept under bijective affine transformations (Theorem 2.8), and providing a general example of test-sets with minimal cardinality (see Theorem 2.7). Moreover, for technical reasons, we have extended this concept to sets such that any subset of a certain cardinality is also a test-set (what we

*Authors supported by the Spanish Ministerio de Economía y Competitividad , and by the European Regional Development Fund (ERDF), under the Project MTM2017-88796-P.

ISSAC '18, July 16–19, 2018, New York, NY, USA

ACM ISBN 978-1-4503-5550-6/18/07…$15.00
https://doi.org/10.1145/3208976.3208981

have called "disjunctive test-sets", c.f. Definition 2.9). Let us remark that the terminology of "test-sets" comes from the attempts to mechanizing inductive reasonings [15].

But the final goal of our work is not exactly finding zero-test protocols for given ideals of a certain degree. It is something closely related, but more general. Assume we are given a certain ideal $\mathrm{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ of which we just know a bound of the degree d of its zero set, and the number of variables n. Then we want to decide if the result of eliminating some variables in the ideal I, say, if $\mathrm{I}_r = \mathrm{I} \cap \mathbb{K}[x_1, \ldots, x_r]$, yields or not to the zero ideal. And this zero-checking for I_r is to be performed only through a number of tests that, like in the previous situation, will consist in choosing some points $(a_1, \ldots, a_r) \in \mathbb{K}^r$, and then verifying, with an oracle, if they can be (or not) lifted to a point $(a_1, \ldots, a_n)$ in the zero-set defined by I. See Section 3.1 for details, but let us illustrate here both the goal and the method we have developed, through the following example.

Example 1.1. Imagine we are given an ideal I (of whatever dimension) in $\mathbb{K}[x_1, x_2, x_3]$, and we just know that the degree of its zero set is bounded by 2. Then we would like to check if the elimination $\mathrm{I}_2 = \mathrm{I} \cap \mathbb{K}[x_1, x_2]$ is zero. Roughly speaking, we could argue like this: this elimination variety $\mathbb{V}(\mathrm{I}_2)$ is, surely, also of degree bounded by 2, as the degree bound is preserved under affine mappings [6]. And the same happens for the Zariski closure of $\mathbb{V}(\mathrm{I}_2)$ minus the projection π of $\mathbb{V}(\mathrm{I})$ over the (x_1, x_2)-plane (c.f. proof of Theorem 3.1 at Section 3).

Then, take 11 points on the plane (what we will call a "disjunctive test-set" for degree two varieties over the plane), arranged in such a way that no subset of six points lies on a conic. Next, consider each one of these 11 points and verify if they can be lifted to a zero of I in $\mathbb{K}^3$, that is, for each of these points (a_1, a_2), check if there is a $a_3 \in \mathbb{K}$ so that $(a_1, a_2, a_3) \in \mathbb{V}(\mathrm{I}) \subset \mathbb{K}^3$. Let A be the subset of the 11 points that can be lifted and let B its complementary. Obviously, either the cardinal of A or the cardinal of B must be strictly greater than 5.

Thus, if cardinal of A is 6 or more, we are sure that $\mathbb{V}(\mathrm{I}_2)$, since it is either of degree 2 or the whole plane, and it contains A, it must be the whole plane, so I_2 is zero. Assume, on the contrary, that B has cardinal greater than 6. Now we consider the partition of the plane in three different sets of points: those in the projection of $\mathbb{V}(\mathrm{I})$, those in $\mathbb{V}(\mathrm{I}_2)$ but not in this projection, those not in $\mathbb{V}(\mathrm{I}_2)$.

By definition, B is outside the projection, so it must be included in the union of $\mathbb{V}(\mathrm{I}_2) \setminus \pi(\mathbb{V}(\mathrm{I}))$ with $\mathbb{K}^2 \setminus \mathbb{V}(\mathrm{I}_2)$. Now it happens that not all the points in B can be within $\mathbb{V}(\mathrm{I}_2) \setminus \pi(\mathbb{V}(\mathrm{I}))$, since it will imply that its Zariski closure, also of degree bounded by 2, is the whole plane. But this Zariski closure must be strictly contained in $\mathbb{V}(\mathrm{I}_2)$ (c.f. [2]), which will be impossible in this case.

It follows that B cannot be fully contained in $\mathbb{V}(\mathrm{I}_2) \setminus \pi(\mathbb{V}(\mathrm{I}))$. Thus there must be points in B that are neither in the 'bad set" (i.e. $\mathbb{V}(\mathrm{I}_2) \setminus \pi(\mathbb{V}(\mathrm{I}))$), nor in the projection, so outside of $\mathbb{V}(\mathrm{I}_2)$, and we conclude that this variety can not be the whole plane, achieving in this way a complete decision protocol.

Thus, in the last Section of this paper we will describe an algorithm for achieving such a test of the nullity of elimination ideals. Although we estimate that the theoretical foundations we have developped are already interesting, we will summarily present, as well, a concrete application of this technique, in the context of automated reasoning for geometry statements. It has been already implemented in the popular dynamic geometry and computer algebra program GeoGebra[1] (see [1] for a condensed presentation of this feature in a prototype version, although without technical details; see also [14], column "Recio").

We expect to be able to present in a near future, to the scientific community, complete results concerning the already promising performance of theorem proving algorithms using this particular approach.

2 TEST-SETS

In this section, we introduce the notion of test-set and we state its main properties. The concept of test-set will depend on two positive integer numbers (d, r). d will denote the degree of the variety to be tested and r the dimension of the affine space where the test set, or the tested variety, is included; or equivalently, r is the number of variables of the polynomial ring.

Definition 2.1. We recall that the geometric degree of an irreducible affine variety $\mathcal{U} \subset \mathbb{K}^k$ is the number of intersections of $\mathcal{U}$ with a generic affine linear variety of codimension $\dim(\mathcal{U})$. When the variety is reducible, the degree is defined as the sum of the degrees of the reducible components; for further details we refer to Def. 1. and Remark 2 in [6].

Definition 2.2. A finite subset $A \subseteq \mathbb{K}^r$ is a (d, r)-test set, with $d > 0$, if no proper variety $\mathcal{W}$ of $\mathbb{K}^r$ of geometric degree less or equal than d contains A.

Let us show a couple of trivial and typical examples of (d, r)-test sets. First example: $d + 1$ different points on a line $\mathbb{K}$ are a $(d, 1)$-test set, since there is no non-zero polynomial in one variable, of degree less or equal than d, with $d + 1$ roots. Another easy one: $r + 1$ points in $\mathbb{K}^r$, affinely independent, are a $(1, r)$-test set, since no hyperplane in $\mathbb{K}^r$ contains them.

Remark. Given a constructible set $C \subseteq \mathbb{K}^r$, let us say it is a *proper* constructible set if its closure $\overline{C}$ is a proper algebraic variety, i.e., if $\overline{C} \neq \mathbb{K}^r$. Then, an equivalent definition for (d, r)-test sets can be stated replacing in the above definition the word "variety" by "constructible set". In fact, it is enough to recall that the degree of a constructible set is, by definition, that of its Zariski closure (see [6]).

The next theorem shows that (d, r)-test set candidates need to be verified just for hypersurfaces, i.e., for single polynomials of degree up to d and r variables.

Theorem 2.3. *Let $A \subseteq \mathbb{K}^r$ and $d \in \mathbb{Z}_{>0}$. Then A is a (d, r)-test set if and only if no hypersurface of $\mathbb{K}^r$, of geometric degree less or equal than d, contains A.*

Proof. Let $A \subseteq \mathbb{K}^r$ be a (d, r)-test set. Then, obviously, no proper hypersurface $\mathcal{W}$ of $\mathbb{K}^r$ defined by a polynomial of degree less or equal than d contains A. Conversely, assume that $A \subseteq \mathbb{K}^r$ is such that no proper hypersurface $\{F = 0\} \subseteq \mathbb{K}^r$ defined by a polynomial $F(x_1, \ldots, x_r)$, of degree less or equal than d, contains A. Then,

[1] http://geogebra.org

given any proper variety $\mathcal{W}$ of $\mathbb{K}^r$, of degree at most d, let us show that it can not contain A. In fact, $\mathcal{W}$ is always contained in a hypersurface of degree bounded by d: consider $\mathcal{W} = \mathcal{W}_1 \cup \cdots \cup \mathcal{W}_m$ be the irreducible decomposition of $\mathcal{W}$. Let $\deg(\mathcal{W}_i) \leq d_i$. Then, $d_1 + \cdots + d_m \leq d$. By [6], Prop. 3, pp. 256, each $\mathcal{W}_i$ can be defined as the zero-set of a finite family of polynomials with degree bounded by d_i. Let $F = f_1 \cdots f_m$, taking each $f_i \neq 0$ in the generator set of $\mathcal{W}_i$. Then it is clear that $\mathcal{W} \subseteq \{F = 0\}$. □

In the next part of the section, we will describe a test-set of minimal cardinality. In the following, for $m_1, m_2 \in \mathbb{Z}_{>0}$, we denote by

$$\mathrm{Supp}(m_1, m_2) \subseteq \mathbb{Z}_{>0}^{m_2}$$

the set of exponents on the support of a generic polynomial of degree m_1 in m_2 variables. We recall that its cardinal is

$$\#(\mathrm{Supp}(m_1, m_2)) = \binom{m_1 + m_2}{m_2}.$$

We start with some technical lemmas

Lemma 2.4. *Let $\Pi : \mathbb{K}^r \to \mathbb{K}^{r-1}, \Pi(x_1, \ldots, x_r) = (x_2, \ldots, x_r)$. If A is a (d, r)-test set then $\Pi(A)$ is a $(d, r-1)$-test set.*

Proof. Let $\mathcal{W}^*$ be a variety of $\mathbb{K}^{r-1}$ with $\deg(\mathcal{W}^*) \leq d$ and such that $\Pi(A) \subseteq \mathcal{W}^*$. We consider the variety $\mathcal{W} = \mathbb{K} \times \mathcal{W}^* \subseteq \mathbb{K}^r$. We observe that

$$A \subseteq \mathbb{K} \times \Pi(A) \subseteq \mathcal{W} \subseteq \mathbb{K}^r$$

and $\deg(\mathcal{W}) \leq d$. Since A is a (d, r)-test set, $\mathcal{W} = \mathbb{K}^r$. Therefore, $\mathcal{W}^* = \mathbb{K}^{r-1}$. So, one concludes that $\Pi(A)$ is a $(d, r-1)$-test set. □

Lemma 2.5. *Let $\Pi : \mathbb{N}^r \to \mathbb{N}^{r-1}, \Pi(x_1, \ldots, x_r) = (x_2, \ldots, x_r)$. Then, $\Pi(\mathrm{Supp}(d, r)) = \mathrm{Supp}(d, r-1)$*

Proof. Let $\overline{u} \in \mathrm{Supp}(d, r-1)$, then $(0, \overline{u}) \in \mathrm{Supp}(d, r)$. Conversely, it is obvious that if $\overline{v} \in \mathrm{Supp}(d, r)$ then $\Pi(\overline{v}) \in \mathrm{Supp}(d, r-1)$. □

Lemma 2.6. *If $P \in \mathbb{K}[x_1, \ldots, x_r]$ has degree less or equal than d and vanishes on $\mathrm{Supp}(d, r)$, then P is the zero polynomial.*

Proof. We prove the statement by induction on r. For $r = 1$, it follows from the hypothesis that $P(x_1)$ vanishes over $\mathrm{Supp}(d, 1)$, of cardinal $d + 1$, and thus it has $d + 1$ different roots; hence it is identically zero. Let us assume that the lemma is true for $r = s - 1$, and that $P \in \mathbb{K}[x_1, \ldots, x_s]$ is such that $\deg(P) \leq d$ and $P(\overline{u}) = 0$ for all $\overline{u} \in \mathrm{Supp}(d, r)$. We consider the linear polynomials $L_k(x_1) = x_1 - k$, with $k \in \{0, \ldots, d\}$. Then, dividing w.r.t. x_1 we get that

$$P(x_1, \ldots, x_s) = Q(x_1, \ldots, x_s) L_k(x_1) + M(x_2, \ldots, x_s).$$

Since , $P(\overline{u}) = 0$ for all $\overline{u} \in \mathrm{Supp}(d, s)$, then $M(\Pi(\overline{u})) = 0$. By Lemma 2.5, we get that $M(\overline{v}) = 0$ for all $\overline{v} \in \mathrm{Supp}(d, s-1)$. So, by the induction hypothesis, M is identically 0. Thus, $\prod_{k=0}^{d} L_k$ divides P, which has degree at most d. Hence, P is also identically zero. □

In this situation, we are ready to prove the theorem.

Theorem 2.7. *$\mathrm{Supp}(d, r)$ is a (d, r)-test set of minimum cardinality.*

Proof. The fact that $\mathrm{Supp}(d, r)$ is a (d, r)-test set follows from Lemma 2.6 and Theorem 2.3. Let us prove the minimality. Let $N = \#(\mathrm{Supp}(d, r))$, and let us assume that there exists a (d, r)-test set A with $\#(A) = N^* < N$. A generic polynomial P in $\mathbb{K}[x_1, \ldots, x_r]$ of degree d has as many undetermined coefficients as elements in $\mathrm{Supp}(d, r)$; let us call them $\{a_i\}$. Now, since A is a (d, r)-test set, evaluating P at each element of A, we get an homogenous linear system $\{P(\overline{u}) = 0\}_{\overline{u} \in A}$ in the undetermined coefficients $\{a_i\}$. Since the rank of this system is at most N^*, that is smaller than N, there exists a nontrivial solution; in contradiction with the property of being a test set. □

Remark. As a consequence of this theorem it follows that, asymptotically, (d, r)-test sets have cardinality with lower bound $O(d^r)$ (if we consider d growing and r fixed) or $O(r^d)$ (if we rather consider r growing and d fixed). Thus, the result in Theorem 2.7 is, in some sense, not too different from the naive approach yielding $(d + 1)^r$ points (the cartesian product of sets of $d + 1$ points over each axis in $\mathbb{K}^r$), except if one is interested in the case of growing dimension and bounded degree, which, by the way, could be quite useful in automatic geometric reasoning (see, for example, the results in [12]), since statements therein involve several points (and, thus, many coordinates) but, generally, construction steps of low degree (involving several simple, linear or quadratic, operations such as building a line through two given points or intersecting a line and a circle, etc); note that

$$\lim_{r \to \infty} \frac{\binom{d+r}{r}}{(d+1)^r} = 0.$$

The following theorem states that the property of being test-set is invariant under bijective affine transformations.

Theorem 2.8. *Let A be a (d, r)-test set, and φ a bijective affine transformation of $\mathbb{K}^r$. Then $\varphi(A)$ is a (d, r)-test set.*

Proof. Let us assume that $\varphi(A)$ is not a (d, r)-test set. Then, by Theorem 2.3, there exists a hypersurface $\mathcal{V} = \mathbb{V}(H)$, where $H(\mathbf{x}) = H(x_1, \ldots, x_r) \in \mathbb{K}[\mathbf{x}]$, of degree $\leq d$ such that $\varphi(A) \subset \mathcal{V}$. Let $F = H(\varphi^{-1}(\mathbf{x}))$, and let $\mathcal{W} = \mathbb{V}(F)$. Since φ is an affine transformation, $\deg(F) = \deg(H)$, and $A \subset \mathcal{W}$, which is a contradiction. □

In some cases it would be interesting to construct sets having stronger properties than that of being a test set, namely, such that any subset of cardinal greater than a fixed size is also a test set. More precisely, we introduce the following definition:

Definition 2.9. Let $d, r \in \mathbb{Z}_{>0}$, and $N = \#(\mathrm{Supp}(d, r))$. We say that a finite set A, with $\#(A) \geq N$, is a (d, r)-disjunctive test set if any subset of A of cardinal N is a (d, r)-test set.

The motivation of this notion is the following. Assume that A is disjunctive and $\#(A) \geq 2N - 1$ and $B \subseteq A$, then either B or $A \setminus B$ is a (d, r)-test set. Indeed, if $\#(B) \geq N$, the statement holds by the definition of disjunctive test set. Else, $\#(A \setminus B) \geq N$, and thus $A \setminus B$ is a (d, r)-test set.

In this context, the following holds.

Lemma 2.10. *For any given $d, r \in \mathbb{Z}_{>0}$, and $N = \#(\mathrm{Supp}(d, r))$, the following algorithm derives a (d, r)-disjunctive test set of any given cardinal M greater or equal to N.*

Proof. If $M = N$ then we can take $A = \mathrm{Supp}(d, r)$ (see Theorem 2.7). We assume by induction that we know how to build a disjunctive test set, B of cardinal $M \geq N$, and let us build another one of cardinal $M + 1$. In fact, let us first remark that, for every subset C of B, of $N - 1$ elements, there exists a unique hypersurface in $H_C \subset \mathbb{K}^r$ of degree d, through these elements. This hypersurface can be constructed by solving a linear homogeneous system of $N-1$ equations in N unknowns, each equation being the generic polynomial of degree d in r variables, with undetermined coefficients, evaluated at one of the elements of C.

Notice that the rank of this linear system is $N - 1$, and thus it defines uniquely –except for multiplication by a common constant– the coefficients of a hypersurface. In fact, would the rank be strictly smaller than $N - 1$, we could add to C an extra point such that the rank of the extended system with the new equation for the extra point would be $N - 1$ or less and, therefore, it would have at least one solution. But this is a contradiction to the fact that B is disjunctive and all subsets of B with N elements (such as C plus the added point) must be (d, r)-test sets, implying that there is no hypersurface of degree d defined by these points.

Now consider all such hypersurfaces H_C for all different choices of $C \subset B$. Let $P \in \mathbb{K}^r$ be a point not in any of these hypersurfaces. Then we claim that $B^\star = B \cup \{P\}$ is also a (d, r)-disjunctive test set. In fact, if $A \subseteq B^\star$ has cardinal N and is a subset of B, it is obviously a (d, r)-test set, because B is disjunctive. On the other hand, if $P \in A$, then $A \cap B \subseteq B$ is of cardinal $N - 1$. By construction point P does not belong to the only hypersurface $H_{A\cap B}$ of degree d defined by $A \cap B$, and therefore A is a (d, r)-test set. □

The algorithm described in the proof of Lemma 2.10 can be outlined as follows.

Algorithm 1. Given $d, r \in \mathbb{Z}_{>0}$, and $N = \#(\mathrm{Supp}(d, r))$, the following algorithm derives a (d, r)-disjunctive test set of any given cardinal M greater or equal to N.

(1) If $M = N$ Return $\mathrm{Supp}(d, r)$.
(2) Set $B = \mathrm{Supp}(d, r)$.
(3) For i from 1 to $M - N$ do
   (a) For any subset C of B with $\#(C) = N - 1$ determine the unique hypersurface H_C of $\mathbb{K}^r$ of degree d.
   (b) Compute a point $P \in \mathbb{K}^r$ not in any of the hypersurfaces obtained in the previous step.
   (c) Set $B = B \cup \{P\}$.
(4) Return B.

Example 2.11. We use the notation as in Algorithm 1. Let us consider $d = 2, r = 2 \in \mathbb{N}$, $\#(\mathrm{Supp}(2, 2)) = 6$ and let $M = 7$. Then a $(2, 2)$-disjunctive test set of cardinal 7 can be build as follows.

$$\begin{aligned} \mathrm{Supp}(2,2) &= \{P_1, P_2, P_3, P_4, P_5, P_6\} \\ &= \{(0,0), (0,1), (0,2), (1,0), (1,1), (2,0)\}. \end{aligned}$$

Let H_i be the unique conic passing through $\mathrm{Supp}(2, 2) \setminus \{P_i\}$. More precisely, $H_1 = (x + y - 2)(x + y - 1), H_2 = x(x + y - 2), H_3 = x(x - 1), H_4 = y(x + y - 2), H_5 = xy$ and $H_6 = y(y - 1)$. Then taking $P \notin \cup H_i$, for instance, $P = (2/3, 2/3)$, we have that $\mathrm{Supp}(2, 2) \cup \{P\}$ is a $(2, 2)$-disjunctive test set of cardinal 7.

Remark. Given a (d, r)-disjunctive test set A of cardinal $M \geq N = \#(\mathrm{Supp}(d, r))$, we have remarked –after Definition 2.9– that, if $M \geq 2N - 1$, it is true that, for every subset of $B \subseteq A$, at least one from B or its complement $A \setminus B$, must be a (d, r)- test set. Obviously $2N - 1$ is the minimum cardinal of sets A holding this property, since for $M < (2N - 1)$ we can always find subsets of A such that both the subset and its complement have cardinal strictly smaller than N. Now, since N is the minimum size of a (d, r)-test set (cf. Theorem 2.7), it is obvious that in this case neither A nor $A \setminus B$ can be (d, r)-test sets.

3 AN APPLICATION: TESTING THE NULLITY OF ELIMINATION IDEALS

In the sequel, we will denote by $\mathbf{x}_i = (x_1, \ldots, x_i)$ with $i \in \{1, \ldots, n\}$. Let us consider the ideal $\mathrm{I} \subset \mathbb{K}[\mathbf{x}_\mathrm{n}]$ as well as its associated variety $\mathcal{V} = \mathbb{V}(\mathrm{I}) \subset \mathbb{K}^\mathrm{n}$. In addition, we also consider the projection

$$\begin{array}{rccc} \pi_r : & \mathcal{V} \subseteq \mathbb{K}^n & \to & \mathbb{K}^r \\ & \mathbf{x}_n & \mapsto & \mathbf{x}_r \end{array}$$

and let $\mathrm{I_r}$ be the $\mathbf{x}_r$-elimination ideal, that is $\mathrm{I_r} = \mathrm{I} \cap \mathbb{K}[\mathbf{x}_\mathrm{r}]$, and $\mathcal{V}_r = \mathbb{V}(\mathrm{I_r}) \subseteq \mathbb{K}^\mathrm{r}$. By the Theorem of the Closure (see Theorem 3 pp. 125 in [2]) it holds that

$$\mathcal{V}_r = \overline{\pi_r(\mathcal{V})}.$$

We provide an algorithm that decides whether $\mathcal{V}_r$ is $\mathbb{K}^r$ or, equivalently, whether $\mathrm{I_r} =< 0 >$.

It holds that $\mathcal{V}_r \setminus \pi_r(\mathcal{V})$ is a constructible set. Let $\mathcal{W}_r$ be a subvariety of $\mathcal{V}_r$, of lower dimension, such that $\mathcal{V}_r \setminus \pi_r(\mathcal{V}) \subset \mathcal{W}_r$. The existence of $\mathcal{W}_r$ is also guaranteed by the Closure Theorem.

The algorithm is as follows

Algorithm 2. Given a bound d for the geometric degree of $\mathcal{V}$, the algorithm decides whether the ideal I_r is zero or not.

(1) Set $N = \binom{d+r}{r}$.
(2) Apply Algorithm 1 to N and (d, r) to get a (d, r)–disjunctive test set of cardinality $2N - 1$, say C.
(3) Using an oracle, decompose C as $C = A \cup B$, where for every $P \in A$ it holds that $P \in \pi_r(\mathcal{V})$ and for every $P \in B$ it holds that $P \notin \pi_r(\mathcal{V})$
(4) If $\#(A) \geq N$ then Return $\mathrm{I_r} =< 0 >$ else $\mathrm{I_r} \neq< 0 >$.

Theorem 3.1. *The previous algorithm is correct.*

Proof. By Lemma 2 in [6], we know that d also bounds the degree of $\mathcal{V}_r$. Moreover[2], the same bound applies to $\mathcal{W}_r$, that is to the closure of the "bad set" (i.e. the set of points that are in $\mathcal{V}_r$ but can not be lifted to $\mathcal{V}$). Assume $\#(A) \geq N$. By definition of disjunctive test set, A contains a (d, r)-test set. Now, since $A \subset \mathcal{V}_r$ and the degree of $\mathcal{V}_r$ is bounded by d, $\mathcal{V}_r$ must be $\mathbb{K}^r$. Thus, $\mathrm{I_r} =< 0 >$.

On the other hand if $\#(A) < N$, we prove that $\mathrm{I_r} \neq< 0 >$. Let us assume that $\mathrm{I_r} =< 0 >$. Since $\#(A) < N$, then $\#(B) \geq N$ and B contains a (d, r)-test set. Since B is included in $\mathcal{W}_r$ and its degree is also bounded by d, one concludes that $\mathcal{W}_r$ must be $\mathbb{K}^r$. But this

[2]Personal communication by prof. Martín Sombra, ICREA Research Professor at Universitat de Barcelona, Spain, to whom we would like to express our gratitude. Roughly, the idea is to reduce the general case to the case of irreducible varieties, then to the case in which both the given variety and the closure of its projection have the same dimension and, finally, work in a projective setting, studying the intersection of the variety with the hyperplane at infinity and project (yielding those points that can not be affinely lifted). See related ideas at [3].

is impossible, because, by construction, its dimension is strictly smaller than r. □

Remark.

(1) In Step 3 of Algorithm 2 we need to check through an oracle whether a point P is in the projection of the variety. This can be done, for example, by substituting the variables $x_1, \ldots, x_r$ by the corresponding coordinates of P in the generators of the ideal I to check afterwards whether the new variety in $\mathbb{K}^{n-r}$ is non-empty; this can be done by elimination theory techniques. In the context of the applications of these ideas to automatic theorem proving, the fiber of almost all points P is finite. Hence, the variety to be tested is zero-dimensional. Thus, the decision is faster.

(2) Note that the disjoint test-set C, appearing in Step 2 of Algorithm 2, only depends on d and r and not on the ideal I. Therefore, one may have a pre-computed data basis, for different values of d and r, to be used directly on Algorithm 2. Even, if one does not have at hand such a basis, one may combine Algorithms 1 and 2 as follows: whenever a point $P \in C$ is computed, one decides whether P belongs or not to $\pi_r(\mathcal{V})$. As soon as the cardinality of either A or B is greater or equal N, the process can be stopped, and one does not need to determine all elements in C.
A third option, probably the most efficient, is as follows. We compute a test-set T, via the support, with N elements and we apply a random linear transformation to T (see Theorem 2.8) to get T^*. In this situation, we check how many points in T^* can be lifted to $\mathcal{V}$. If this number is N, then we can conclude that $\mathrm{I}_r =< 0 >$. If not, we add to T^* a new point, as explained in Algorithm 1, to get T^{**} and we repeat the process.

Example 3.2. We illustrate Algorithm 2 by a toy example. We consider the ideal $\mathrm{I} \subset \mathbb{C}[x, y, z, w]$ defined by the generators

$$\begin{aligned}\mathrm{I} \quad =< & -w^2x^2 + 2wx^3 - 2x^3z + 2x^2y^2 + 2x^2yz + x^2z^2 - 2\,xy^2z \\ & -2\,xyz^2 + y^4 + 2y^3z + y^2z^2 + 2w^2x - 2wx^2 - w^2, \\ & w^2x^2 - 2wx^3 + 2x^4 - 2x^3z + 2x^2y^2 + 2x^2yz + x^2z^2 - \\ & 2xy^2z - 2xyz^2 + y^4 + 2y^3z + y^2z^2 - 2w^2x + 2wx^2 + w^2 > .\end{aligned}$$

One may check that $\mathcal{V} = \mathbb{V}(\mathrm{I}) \subset \mathbb{C}^4$ has degree 4. Now, we consider the projection $\pi_2 : \mathcal{V} \subset \mathbb{C}^4 \to \mathbb{C}^2; (x, y, z, w) \mapsto (x, y)$. We want to check whether $\overline{\pi_2(\mathcal{V})} = \mathbb{C}^2$ or, equivalently, whether $\mathrm{I} \cap \mathbb{C}[x, y] =< 0 >$. For this purpose, we apply Algorithm 2 with $N = 15$. So, we need a $(4, 2)$-disjoint test set of cardinality 29. Applying Algorithm 1 one get the following disjoint test set

$$\begin{aligned}C = \quad & \{(-18, 28), (-15, -30), (-6, -5), (-5, 28), (-2, -17), \\ & (-2, 29), (0, 0), (0, 1), (0, 2), (0, 3), (0, 4), (1, 0), (1, 1), (1, 2), \\ & (1, 3), (2, 0), (2, 1), (2, 2), (3, -13), (3, 0), (3, 1), (4, 0), (9, 6), \\ & (11, 15), (12, -12), (13, -22), (16, -23), (19, 28), (21, 25)\}.\end{aligned}$$

Decomposing $C = A \cup B$, as in Step 3, by using some of the oracles described in the previous remark, we get that $\#(A) = 24$ and $\#(B) = 5$; Indeed, $B = \{(1, 0), (1, 1), (1, 2), (1, 3), (2, 2)\} \subset \mathbb{C}^2 \setminus \pi_2(\mathcal{V})$. Therefore, $\mathrm{I} \cap \mathbb{K}[x, y] =< 0 >$.

Now, we repeat the example but using the projection $\pi_2 : \mathcal{V} \subset \mathbb{C}^4 \to \mathbb{C}^2; (x, y, z, w) \mapsto (x, w)$. So, C is as above but in this case it decomposes as $C = A \cup B$ with $\#(A) = 1$ and $\#(B) = 28$, being $A = \{(0, 0)\}$. Thus, in this case $\mathrm{I} \cap \mathbb{C}[y, z] \neq< 0 >$.

What could be the interest of having some test-by-examples of the nullity of an elimination ideal? Obviously, such tests could help computing the dimension of a polynomial ideal and selecting a collection of independent variables modulo the ideal. But, although our current work does not address this issue, the specific application of the zero-testing method we have in mind –and also the initial motivation for this work— is automated geometric theorem proving, within the realm of the "proof by exhaustion" method[3].

Without going into details, it happens that, for some approaches, the truth of a certain type of geometric statements involves checking that some multivariate polynomial is identically zero; and this is accomplished by verifying that the polynomial is zero on some sort of test set, where each element of the set corresponds to a geometric instance of the given statement (say, a particular position of a vertex on a triangle). Some attempts in this direction have been labeled as the method of *proving by examples*. We can find early occurrences of this approach in the works of [8],[9] and [25], while in [4] a survey of these early procedures for automatic theorem proving in geometry, till 1988, is presented. The dissertation of Kortenkamp [10] or the paper [11] provide a fine analysis on the advantages and limitations of this approach, in the context of Dynamic Geometry.

More recently, both the master dissertation of Weitzhofer [23] and the doctoral dissertation of Kovács [12], reconsider, extend, implement and test this technique in the popular program GeoGebra, following the completely general theorem proving and discovery approach of [21], that we can summarize as follows.

Let $\{H \Rightarrow T\}$ be a geometric statement, where $H = \{h_1, \ldots, h_\ell\}$ stands for the ideal of equations describing the geometric construction of the hypotheses and $T = (f)$ describes the thesis (or, more generally, the theses). Both ideals lie on a polynomial ring $\mathbb{K}[X]$, where the variables $X = \{x_1, \ldots, x_n\}$ refer to the coordinates involved in the algebraic description of the hypotheses, over a base field $\mathbb{K}$. Fix a maximum-size set $Y = \{x_1, \ldots, x_m\}$ of independent variables for the hypotheses ideal H (i.e. $m = \dim(H)$), and label as "non-degenerate" the irreducible components of H where Y remains independent. Consider $\mathbb{L}$, an algebraically closed extension on $\mathbb{K}$ (for instance $\mathbb{L} = \mathbb{C}$ and $\mathbb{K} = \mathbb{Q}$), and let the geometric instances verifying the hypotheses (respectively, the thesis) of the statement be the algebraic variety $\mathbb{V}(H)$ (respectively, $\mathbb{V}(T)$) in the affine space $\mathbb{L}^n$.

We say that a statement is "generally true" iff T holds over all non-degenerate components; and that it is "generally false" if it does not hold over any of them. Then it is shown that

a) The statement $\{H \Rightarrow T\}$ is generally true if and only if
$$\mathrm{I} \cap \mathbb{K}[Y] \neq \langle 0 \rangle .$$
where I is the ideal $\mathrm{I} = \langle h_1, \ldots, h_\ell, f \cdot t - 1 \rangle \subset \mathbb{K}[X, t]$.

b) The statement $\{H \Rightarrow T\}$ is generally false if and only if
$$\mathrm{I}^* \cap \mathbb{K}[Y] \neq \langle 0 \rangle .$$
where I^* is the ideal $\mathrm{I}^* = \langle h_1, \ldots, h_\ell, f \rangle \subset \mathbb{K}[X]$.

[3] "Proof by exhaustion, also known as proof by cases…is a method…in which the statement to be proved is split into a finite number of cases and each case is checked to see if the proposition in question holds". C.f. https://en.wikipedia.org/wiki/Proof_by_exhaustion

see [21].

Obviously, here the key tool is to decide –by dragging, on the GeoGebra window, the construction to a suitable number of positions, i.e. by considering some special values of $(x_1, \ldots, x_n)$ and verifying if the statement is false or true in these cases– if the elimination ideal of hypotheses and the negation of the theses or the ideal of hypotheses and theses is or not zero. See the above mentioned academic works for details of the excellent performance of this technique in the prototype version already implemented. Moreover, in [14], a detailed benchmark is presented on the comparative performance of different proving methods implemented in GeoGebra. The first column contains a list of ggb files describing geometric statements, alphabetically ordered. Then, there is a series of blocks (labeled as Recio, Botana, Botana D, BotanaGiac, etc.) referring to the considered theorem proving method, each one containing two columns: Result (true, false, empty, i.e. undefined for some reason) and Speed (in milliseconds, t/o means time-out!). Details about the different methods are provided in [13], although, concerning the method we are dealing with here, the reference in [13] is very limited: only the two-variables case is sketched, with some hints about its generalization for three variables. Notice that we are considering just a prototype implementation, thus it happens that, in many instances, some of the methods are not programmed to include some types of input (for example, in [13] the so called Recio's method –i.e. the one described in the current paper– is not yet programmed to deal with circles, thus it yields no answer in many cases!). Despite all these limitations it is clear that, when applicable, our method is much faster than any other one.

We finish with an example of the application of our algorithms to a geometric problem.

Example 3.3. In this example we illustrate how the ideas described above are applicable to prove that Simson's Theorem is generically true. The Theorem of Simson claims that

> *Given a triangle abc and a point d on its circumcircle, the feet e, f, g of the perpendiculars from d to the lines bc, ab, and ac, respectively, are collinear.*

We will follow the notation in [20] (subsections 1.4 and 1.5) but adding, as a non-degeneracy hypothesis, the condition h_6 below. Thus, the variables in the construction are $\{r, s, m, n, q, t, u, v, w\}$, being $\{r, s, m\}$ a maximum size set of independent variables (see Fig. 1). The hypotheses are

$h_1 = s(t-1) - u(r-1)$ (f is on the line ab).
$h_2 = (t-m)(r-1) + s(u-n)$ (df is perpendicular to ab).
$h_3 = -rw + sv$ (e is on the line cb).
$h_4 = r(m-v) + s(n-w)$ (de is perpendicular to cb).
$h_5 = m^2 s - n^2 s + nr^2 + ns^2 + ms - nr$ (d is on the circumcircle).
$h_6 = qs - 1$ (abc does not degenerate as a triangle).

And the thesis

$$F = (w-u)(m-t) + u(v-t).$$

Therefore, we consider the ideal

$$\mathrm{I} =< h_1, \ldots h_6, zF - 1 > \subset \mathbb{C}[r, s, m, n, q, z, t, u, v, w].$$

The variety $\mathcal{V} = \mathbb{V}(\mathrm{I}) \subset \mathbb{C}^{10}$ has degree $d = 32$. In order to decide whether $\mathrm{I} \cap \mathbb{C}[r, s, m] =< 0 >$ we apply Algorithm 2 with the third optimization approach described in the remark after the algorithm, namely taking the support with $N = \binom{32+3}{3} = 6545$, applying a random bijective affine transformation and checking whether all elements are liftable. For the random affine transformation we have taken integers in $\{-10..10\}$, and we have consider an upper triangular matrix. The precise transformation $\mathcal{T}$ is

$$\mathrm{Y} = \begin{pmatrix} 7 & 0 & 9 \\ 0 & 2 & -3 \\ 0 & 0 & 6 \end{pmatrix} \mathrm{X} + \begin{pmatrix} -5 \\ 9 \\ 6 \end{pmatrix}.$$

The result is that none element in $\mathcal{T}(\mathrm{Supp}(N))$ can be lifted. Therefore, the conclusion is that elimination ideal is non-zero, and hence the theorem is generically true. The computation were performed with Maple 2017 on a PC with i7-5500U CPU 240GHz, and the 6545 lifting checks took 1.3 seconds.

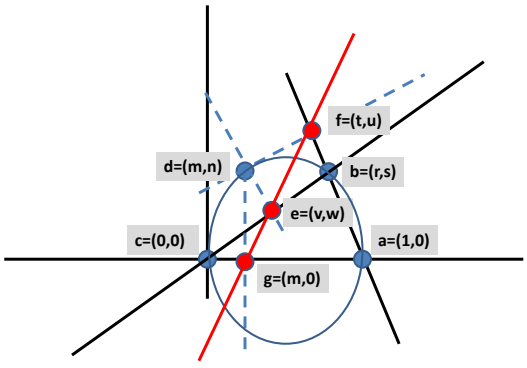

Figure 1: Illustration of Simson's Theorem

REFERENCES

[1] Abánades, M., Botana, F., Kovács, Z., Recio, T., Sólyom-Gecse, C. Development of automatic reasoning tools in GeoGebra. *ACM Communications in Computer Algebra.* Volume 50 Issue 3, September 2016. Pages: 85-88.

[2] Cox, D., Little, J., O'Shea, D. (2012). Ideals, Varieties, and Algorithms. Springer, New York, third edition.

[3] D'Andrea C., Krick T. and Sombra M. (2013). Heights of varieties in multiprojective spaces and arithmetics Nullstellensätze. *Annales scientifiques de l'École Normale Supérieure.* Vol 46, issue 4, pp. 549–627.

[4] Ferro A. and Gallo G. (1988). Automated theorem proving in elementary geometry. *Le Matemathiche*, vol. XLIII, pp. 195–224.

[5] Gasca M. and Sauer T. (2000). Advances in Computational Mathematics (Special issue on Multivariate polynomial interpolation), vol. 12 (2000), pp. 377–410.

[6] Heintz J. (1983). Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24, pp. 239-277.

[7] Heintz, J., Schnorr, C.P. (1982). Testing polynomials wich are easy to compute, *L'Enseignement Mathématique*, 30, 237–254.

[8] Hong J. (1986). Can we prove geometry theorems by computing an example?. *Science China Mathematics.* 29(8): 824-834.

[9] Hong J. (1986). Proving by example and gap theorems. *Proc. 27th Ann. Symp. Foundations Comp. Science.* 107–116. IEEE.

[10] Kortenkamp, U. (1999). Foundations of Dynamic Geometry. Ph. D. thesis. ETH Zürich. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.2207&rep=rep1&type=pdf

[11] Kortenkamp, U., Richter-Gebert, J. (2004): Using automatic theorem proving to improve the usability of geometry software. Proceedings of MathUI, 2004. (Online publication available at https://www.researchgate.net/publication/215908130_Using_Automatic_Theorem_Proving_to_Improve_the_Usability_of_Geometry_Software).

[12] Kovács, Z. (2015). Computer based conjectures and proofs in teaching euclidean geometry. Ph. D. thesis. Johannes Kepler University, Linz. Available at http://www.jku.at/content/e263/e16099/e16086/e173791?view=PUBD&pub_id=51957

[13] Kovács, Z. (2015) Prover benchmark for GeoGebra 5.0.65.0 (r38763). http://test.geogebra.org/~kovzol/data/Prove-20150219b/

[14] Kovács, Z. (2018). Prover benchmark for GeoGebra 611. https://prover-test.geogebra.org/job/GeoGebra-provertest/ws/test/scripts/benchmark/prover/html/all.html

[15] Kounailis, E., Rusinowitch, M. (1990). Mechanizing inductive reasoning. In the*Eight National Conference on Artificial Intelligence*. AAAI-90 Proceedings. 240–245.

[16] Lipton, R. J.(2009). The curious history of the Schwartz-Zippel lema. In *Gödel's lost letter and P=NP*, Nov. 30, 2009. Available at https://rjlipton.wordpress.com/2009/11/30/the-curious-history-of-the-schwartz-zippel-lemma/

[17] Mora, T. (2003). De Nugis Groebnerialium 2: Applying Macaualay's Trick in order to easily write a Groebner basis, J. AAECC. 13 (2003) 437–446

[18] Pardo, L.M., (1995). How lower and upper complexity bounds meet in elimination theory, *Proc. AAECC–11*, (G. Cohen, M.Giusti, T. Mora, eds.), Springer LNCS. 948, 33–69.

[19] Pardo, L.M. (2012). La Conjetura de Cook (P = NP?). Parte II: Probabilidad, Interactividad y Comprobación Probabilística de Demostraciones. *La Gaceta de la Real Sociedad Matemática Española*, 15-2. 303–333.

[20] Recio, T. (1998). Cálculo simbólico y geométrico. *Editorial SÃŋntesis*. Madrid.

[21] Recio, T., Vélez, M.P. (1999(: Automatic discovery of theorems in elementary geometry, Journal of Automated Reasoning, 23, 63–82.

[22] Schwartz J.T. (1980). Fast probabilistic algorithms for verification of polynomial identities. *Journal of ACM*. 27: 701–717.

[23] Weitzhofer, S. (2013). Mechanic proof of theorems in plane geometry. Masterarbeit, Johannes Kepler University, Linz. Available at http://test.geogebra.org/%7Ekovzol/guests/SimonWeitzhofer/DiplArbeit.pdf

[24] Zariski, O. and Samuel, P. (1958). Commutative Algebra, Vol. 1, Van Nostrand.

[25] Zhang J., Yang L. and Deng M. (1990). The parallel numerical method of mechanical theorem proving. *Theoretical Computer Sience* 74:253–271.

[26] Zippel R. (1979). Probabilistic algorithms for sparse polynomials. In: Ng E.W. (eds) Symbolic and Algebraic Computation. EUROSAM 1979. Lecture Notes in Computer Science, vol 72. Springer, Berlin, Heidelberg.