A PROMENADE THROUGH CORRECT TEST SEQUENCES I: DEGREE OF CONSTRUCTIBLE SETS, BÉZOUT'S INEQUALITY AND DENSITY

LUIS M. PARDO AND DANIEL SEBASTIÁN

ABSTRACT. In [HeSc, 82], Heintz and Schnorr introduced the notion of *correct test sequence* and since then it has been widely used to design probabilistic algorithms for *Polynomial Equality Test*. The aim of this manuscript is to study the *foundations* and *generalizations* of this notion. We show that correct test sequences are almost omnipresent and appear in many different forms in the mathematical literature: As *identity sequences* for *Function Identity Test*, as *norming sets* in the field of Banach algebras or as *samples* in the context of Reproducing Kernel Hilbert Spaces. As main outcome, we generalize the main statement of [HeSc, 82] proving that short correct test sequences for constructible sets of lists of polynomials do exist and are densely distributed in any constructible set of accurate dimension and degree. The main tool used to prove this result is the theory of degree of constructible sets, which we introduce and develop in this manuscript, generalizing the results of [He, 83] and proving two Bezout's Inequalities for two different notions of degree. We present a $\mathbf{BPP}_K$ algorithm to exhibit the *power* of correct test sequences, this algorithm decides whether a list of polynomials is a secant sequence by just evaluating the input list at some well-suited points. We show the differences between correct test sequences and Demillo-Lipton-Schwartz-Zippel probabilistic tests and we reformulate, prove and generalize two well-known results of the *Polynomial Method*: We prove *Dvir's exponential lower bounds for Kakeya sets* from lower bounds for the length of correct test sequences and generalize *Alon's Combinatorial Nullstellensatz*.

1. INTRODUCTION

This manuscript is a first step of a long term project to understand the meaning of *correct test sequences (CTS's)*. This notion was introduced in [HeSc, 82] and it has been extensively used to design probabilistic algorithms for *Polynomial Equality Tests*, when polynomials are given by arithmetic programs or black-boxes that evaluate them (see, for instance, [Pa, 95], [KP, 96], [CKKLW,95], [Ko, 99], [CGHMP, 03] and references in all of them).

In this manuscript we do not focus on the applications of the notion in complexity terms. *We focus on the foundations and generalizations of the notion as is:* Seeking for foundational results (as Bézout's Inequality for constructible sets), trying to see how they underlie other notions in the existing mathematical literature and introducing mathematical generalizations and (as in the original [HeSc, 82] manuscript) proving not only the existence but also probabilistic results. We finally exhibit a strange algorithm in $\mathbf{BPP}_K$ to decide whether a list of polynomial equations is a secant sequence. The main feature of this algorithm is not its complexity but the fact that it decides the generic co-dimension simply by evaluating the input list of polynomials at some well-suited points.

Correct test sequences appear in the mathematical literature in many different forms. You may see equivalent notions in different fields: From the notion of finite length *norming set* in a Banach algebra to the notion of *sample* in Reproducing Kernel Hilbert Spaces. Also, many correct test sequences satisfy the main ingredient of the "Polynomial Method" and, in particular, they are implicitly used in the lower bound for *Kakeya* sets in [Dv, 09]. We discuss some of these characterizations in our manuscript.

arXiv:2012.15296v2 [math.AG] 5 Jan 2021

Correct test sequences have been seen a as concurrent technique to *DeMillo-Lipton-Schwartz-Zippel probabilistic tests* (cf. [DML, 78], [Zp, 79] and [Sch, 80]). But both approaches have subtle differences. Some of these features are the following ones:

- Correct test sequences are by definition "correct" for the whole class of inputs under consideration: The error probability of their answers is always zero, independent of the input instance.
- DeMillo-Lipton-Schwartz-Zippel probabilistic tests are based on an easy-to-construct sampling set, which is itself a correct test sequence. In such large class, each input instance has some accurate sample where it does not vanish, but different inputs require different accurate sample point. Bounding the error probability of a random guess in the sampling set, we get the probabilistic algorithm.
- Correct test sequences have a length of the same asymptotic order than the Krull dimension of the input set under consideration, whereas DeMillo-Lipton-Schwartz-Zippel probabilistic tests require a sample set of size exponential in the number of variables to get a zero error probability.
- There is no known efficient deterministic procedure to generate correct test sequences and, hence, their existence (and generation) is based on a statement that proves that they are highly dense in probability terms.
- Under some simple hypothesis, we even see that correct test sequences are highly dense inside the (exponentially big) DeMillo-Lipton-Schwartz-Zippel sampling set (see Corollary 5.10).

These subtle differences require of further explanations and this is the motivation of the research trend we initiate with this manuscript, whose main outcomes will serve as foundations for future research. The manuscript is twofold and based on two main frameworks:

- To our knowledge, there is no *Bézout's Inequality for constructible sets* in the mathematical literature. Constructible sets are natural geometric objects that arise naturally as projections of algebraic varieties (see [Ch, 64-65], for instance) and, hence, they are natural objects of Elimination Theory or Computational Algebraic Geometry. Nevertheless, the notion of the degree of these geometric objects has not been correctly stated in the mathematical literature. The study was initiated in [He, 83], who introduced a first notion of degree of a constructible set: This author defined the degree of a constructible set in some affine space $C \subseteq \mathbb{A}^n(K)$ as the degree of its Zariski closure (which we denote by $\deg_z(C)$ below). Unfortunately, Heintz's notion of degree does not satisfy Bézout's Inequality (see Example 2.15, for instance). In [He, 85] the author already observed that his results in [He, 83] only hold for locally closed subsets of some affine space. We devote Part 1 (Sections 2, 3 and Appendix A) of the present manuscript to this topic. We introduce two different notions of degree of a constructible set that satisfy the paradigms of affine degree stated in [He, 83]: $\deg_\pi(C)$ and $\deg_{\mathrm{lci}}(C)$. We prove that both of them satisfy a Bézout's Inequality and we study several other relevant properties of both notions.
- We devote the rest of the manuscript to *correct test sequences*. We first observe different equivalent forms of the notion of correct test sequence in different contexts (in Section 4). We emphasize the fact that correct test sequences are not naturally defined to distinguish between zero and non-zero functions, but to detect by sample evaluation whether an input $f \in \Omega$ belongs or not to some "discriminant" subset $\Sigma \subseteq \Omega$ of codimension at least one. We observe that correct test sequences also satisfy a *curse of dimensionality*: The Krull dimension of the restricted input set Ω is a lower bound for the length of any correct test sequence for Ω with respect to $\{0\}$. Once some good degree notion for constructible sets has been established, we have the tools to provide statements that claim that correct test sequences do exist in any constructible set of accurate dimension and degree (and not only in sets of "grid" shape as established in the existing literature). This is done in Section 5. In this Section we not only establish an existential outcome, but also a probabilistic statement that shows that correct test sequences of asymptotical optimal length are densely distributed in any locally closed set of accurate dimension and degree: We exhibit probability estimates for success. Next, we emphasize that detecting dimension gaps is one of the underlying ingredients

in applications of correct test sequences. In Section 6, we present a $\mathbf{BPP}_K$ algorithm to detect secant sequences which do not manipulate the input list of polynomials in any form. It simply evaluates lists of polynomials at some well-suited sample points. In a final Appendix B we compare correct test sequences to two celebrated combinatorial results, basic for *The Polynomial Method* in Combinatorics: *Dvir's exponential lower bounds for Kakeya sets* and *Alon's Combinatorial Nullstellensatz.*

In forthcoming subsections we exhibit in more detail our main outcomes.

1.1. **Main outcomes of Part 1: Degree, Bézout's Inequality and variations for constructible sets (Sections 2, 3 and Appendix A).** We first need to fix some notations that are going to be used in the sequel. Let κ be a field and let K be its algebraic closure. For every positive integer $m \in \mathbb{N}$, we denote by $\mathbb{A}^m(\kappa)$ the $m-$dimensional affine space over κ. A *constructible set* is a subset $C \subseteq \mathbb{A}^m(K)$ which can be obtained as the projection of an algebraic variety of some affine space $\mathbb{A}^M(K)$ of higher dimension $M \geq m$ (cf. [Ch, 64-65], for instance). A technical difficulty is the lack of a consistent theory of degree of constructible sets that satisfy (at least) a Bézout's Inequality. As soon noticed in [He, 85], Bézout's Inequality in [He, 83] is only valid for locally closed sets. In Example 2.15 we exhibit a constructible set C and an algebraic variety V such that $\deg_z(C \cap V)$ is not bounded by the product $\deg_z(C)\deg_z(V)$. Hence, $\deg_z$ does not satisfy either Bézout's Inequality or some other statements in [He, 83], which we revise here.

According to the *paradigm* stated in [He, 83], a notion of degree of constructible sets must be a quantity (acting as a volume) which satisfies the following properties:

- It is always finite and agrees with the usual notion in the case of algebraic varieties and locally closed sets.
- It is sub-additive.
- It has a good behaviour with respect to intersections with linear varieties and with respect to Cartesian products.
- It satisfies a Bézout's Inequality.
- It is controlled under projections and images by linear mappings.
- It satisfies some variation of Proposition 2.3 in [HeSc, 82].

From these properties, only Proposition 2.3 of [HeSc, 82] requires of some additional explanations.

Observe that a literal application of Bézout's Inequality puts the co-dimension at the exponent of bounds for the degree of several geometric objects. Namely, given $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ such that $V := V_{\mathbb{A}}(f_1, \ldots, f_m)$ has dimension $n - m$, and let $W \subseteq \mathbb{A}^n$ be an algebraic variety. Bézout's Inequality yields the following upper bound:

$$\deg(W \cap V_{\mathbb{A}}(f_1, \ldots, f_m)) \leq \deg(W) \prod_{i=1}^{m} \deg(f_i) \leq \deg(W) \left(\max\{\deg(f_1), \ldots, \deg(f_m)\}\right)^{\mathrm{codim}(V)}.$$

Nevertheless, Proposition 2.3 in [HeSc, 82] replaces co-dimension of V by dimension of W, emphasizing the role of dimension of W in this kind of upper bounds. Namely, Proposition 2.3 in [HeSc, 82] yields:

$$\deg(W \cap V_{\mathbb{A}}(f_1, \ldots, f_m)) \leq \deg(W) \left(\max\{\deg(f_1), \ldots, \deg(f_m)\}\right)^{\mathrm{dim}(W)}.$$

The trade-off between these two upper bounds is the key ingredient to prove the existence and high probability of optimal length correct test sequences.

Having in mind these requirements, we introduce two notions of degree for constructible sets. One is the notion of degree of a constructible set $C \subseteq \mathbb{A}^n$ based on the fact that they may be presented as projections $C = \pi(W)$ of locally closed sets $W \subseteq \mathbb{A}^m$, where $m \geq n$. We denote this notion of degree by $\deg_\pi(C)$ (see Definition 5 for details). Another one is based on the fact that constructible sets $C \subseteq \mathbb{A}^n$ may be presented as finite unions of locally closed irreducible sets (i.e. open sets in irreducible varieties for the Zariski topology). We denote by $\deg_{\mathrm{lci}}(C)$ this notion of degree (see Definition 4 for details). We see how different properties apply accurately to either $\deg_\pi$ or $\deg_{\mathrm{lci}}$ and we have not taken any decision on which is best choice. Let us resume some of the properties we prove in this manuscript.

In Example 2.17, we observe that they are different notions by exhibiting a constructible set $C \subseteq \mathbb{A}^2(\mathbb{C})$ such that:

$$\deg_z(C) < \deg_\pi(C) < \deg_{\mathrm{lci}}(C).$$

We discarded $\deg_z$ as notion of degree since it does not satisfy Bézout's Inequality. We concentrate our study in $\deg_\pi$ and $\deg_{\mathrm{lci}}$. We then prove that both notions of degree satisfy the expected properties: They are sub-additive (cf. Proposition 2.16), they generalize the notion of degree for locally closed sets of [He, 83] (cf. Proposition 2.23) and they behave well with intersections of linear affine varieties and Cartesian products (see Proposition 2.27). Finally, we prove that both notions satisfy a *Bézout's Inequality for constructible sets* (see Theorem 2.28). This statement simply says that given two constructible subsets $C, D \subseteq \mathbb{A}^n(K)$, the following inequalities hold:

$$\deg_\pi(C \cap D) \le \deg_\pi(C) \deg_\pi(D), \quad \deg_{\mathrm{lci}}(C \cap D) \le \deg_{\mathrm{lci}}(C) \deg_{\mathrm{lci}}(D).$$

Nevertheless, we have not been able to clarify the complete role of both notions with respect to the remaining two properties: *Proposition 2.3 of* [HeSc, 82] and *degree of images under linear mappings*. It is immediate to extend the first of those results for the intersection of a constructible set with several locally closed sets for both $\deg_{\mathrm{lci}}$ (see Proposition 3.1) and $\deg_\pi$ (under the globally equi-dimensional hypothesis, see Proposition 3.2).

In Section 3 we prove that $\deg_{\mathrm{lci}}$ satisfies a similar estimate to Proposition 2.3 of [HeSc, 82] for constructible sets of any kind (cf. Theorem 3.4) exchanging co-dimension by dimension in the exponent of the upper bound. We reproduce here that statement for helping readability:

Main Theorem 1.1 (Bounds for the LCI-degree of the intersection of several constructible sets). *Let $C_1, \ldots, C_s \subseteq \mathbb{A}^n$ be a sequence of constructible sets. Let $r := \dim(C_1)$ be the dimension of the constructible set C_1. The following inequalities hold:*

i) First upper bound:

$$\deg_\pi \left(\bigcap_{i=1}^s C_i \right) \le \deg_{\mathrm{lci}} \left(\bigcap_{i=1}^s C_i \right) \le \binom{s+r-1}{r} \deg_{\mathrm{lci}}(C_1) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 2 \le j \le s\} \right)^r.$$

ii) Second upper bound:

$$\deg_\pi \left(\bigcap_{i=1}^s C_i \right) \le \deg_{\mathrm{lci}} \left(\bigcap_{i=1}^s C_i \right) \le \deg_{\mathrm{lci}}(C_1) \left(1 + \sum_{i=1}^s \deg_{\mathrm{lci}}(C_i) \right)^{\dim(C_1)}.$$

iii) Upper bound in terms of the average degree: Given a family of constructible sets $C_1, \ldots, C_s \subseteq \mathbb{A}^n$, we define its average $E-$degree as:

$$\deg_{\mathrm{av}}^{(E)}(C_1, \ldots, C_s) := \frac{1}{s} \sum_{i=1}^s \deg_{\mathrm{lci}}(C_i).$$

Then, we also have:

$$\deg_\pi \left(\bigcap_{i=1}^s C_i \right) \le \deg_{\mathrm{lci}} \left(\bigcap_{i=1}^s C_i \right) \le \deg_{\mathrm{lci}}(C_1) s^{\dim(C_1)} \left(\deg_{\mathrm{av}}^{(E)}(C_1, \ldots, C_s) \right)^{\dim(C_1)}.$$

We have not been able to establish a similar result with $\deg_\pi$ on the right hand side of any of the inequalities.

On the other hand, we also consider the transformation of the degree by taking images by linear mappings (Lemma 2 of [He, 83]). We consider a constructible subset $C \subseteq \mathbb{A}^n(K)$ and a linear mapping $\ell : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$. In Example 2.17 we prove that there are algebraic varieties $W \subseteq \mathbb{A}^3(\mathbb{C})$ such that $\deg_{\mathrm{lci}}(\ell(W)) > \deg_{\mathrm{lci}}(W) = \deg(W)$. Hence, Lemma 2 of [He, 83] is false for constructible sets and $\deg_{\mathrm{lci}}$. It may increase under linear images. In Proposition 2.25 we prove that $\deg_z(\ell(C)) \le \deg_{\mathrm{lci}}(C)$, whereas in Claim *iii)* we exhibit an example of a constructible set that proves that $\deg_{\mathrm{lci}}(\ell(C))$ is not bounded by $\deg_{\mathrm{lci}}(C)$.

As expected, we prove in Proposition 2.26 that $\deg_\pi$ has a good behaviour with respect to linear transformations. Namely, we prove that the following holds:

$$\deg_z(\ell(C)) \le \deg_\pi(\ell(C)) \le \deg_\pi(C) \le \deg_{\mathrm{lci}}(C),$$

for any constructible set and any linear transformation ℓ. This yields to the notion of *defect* of the image $\ell(C)$ of some constructible set given as the following difference:

$$\deg_{\text{lci}}(\ell(C)) - \deg_z(\ell(C)).$$

This manuscript would be somehow uncomplete if we do not try to show some upper bounds for this defect. This is done in our Appendix A. There, in Subsection A.1 we state some upper bound for the defect in Lemma A.2. In Remark A.3, we also exhibit examples such that the bound of Lemma A.2 is optimal. Nevertheless, we hope to have sharper upper bounds for the defect in forthcoming works.

Additionally, we claimed that one of the paradigmatic requirements of the degree must be some kind of control of the LCI-degree of $\ell(C)$. In Subsection A.2 we also exhibit an extrinsic (not sharp, in our opinion) upper bound for $\deg_{\text{lci}}(\ell(C))$. Just for giving some idea of what we mean, we reproduce here the following statement, which is Theorem A.4 of Subsection A.2, that stated an upper bound for $\deg_{\text{lci}}(\ell(C))$. We prove that $\deg_{\text{lci}}(\ell(C))$ is bounded (and, hence, "controlled") in terms of some syntactical quantities depending only on C:

Main Theorem 1.2. *Assume $\kappa = K$ is an algebraically closed field. Let $V \subseteq \mathbb{A}^n(K)$ be an irreducible algebraic variety of dimension r. Let m be an integer such that $m \leq n$. Assume that there are polynomials $g_1, \ldots, g_s \in K[X_1, \ldots, X_n]$ of degrees $d_i := \deg(g_i)$, $1 \leq i \leq r$, such that $V = V_{\mathbb{A}}(g_1, \ldots, g_s)$ and the following inequalities hold:*

$$d_1 \geq d_2 \geq \ldots \geq d_s.$$

Let us consider the following quantity:

$$N := N(d_1, \ldots, d_s, n, r) := \begin{cases} \prod_{i=1}^s d_i & \text{if } s \leq n - m \\ 2d_s \left(\prod_{i=1}^{n-m-1} d_i \right) - 1 & \text{if } s > n - m \end{cases}$$

Let us define the following quantities:

$$\widetilde{N} := \binom{N + (n-m)}{n-m},$$

$$M := \sum_{i=1}^s \binom{N - d_i + (n-m)}{(n-m)},$$

and

$$\mathcal{N}' := \min\{N, M+1\}.$$

Let $\pi : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$ be the canonical projection that forgets the last $n - m$ variables and let $W := \overline{\pi(V)}^z$ be the Zariski closure of $\pi(V)$ in $\mathbb{A}^m(K)$. Then, we have:

$$\deg_{\text{lci}}(\pi(V)) \leq \deg(V) \, (2d_1)^{\dim(W)} \, (\mathcal{N}')^{\dim(W)+1} .$$

1.2. **Main outcomes of Part 2: Correct Test Sequences, generalizations, relations to other notions, density estimates and immediate applications (Sections 4, 5, 6 and Appendix B).** In the remaining sections of the manuscript we deal with correct test sequences (CTS's). We begin in Section 4 by establishing the notion of correct test sequence in Definition 7. We consider a set X and a class of functions $\mathscr{F}(X) \subseteq K^X$ with values in a field K. Given $\Omega \subseteq \mathscr{F}(X)^m$ a distinguished class of functions in $\mathscr{F}(X)^m$ (i.e. maps from X to K^m) and a subset $\Sigma \subsetneq \Omega$, a *correct test sequence of length L for Ω with discriminant Σ* is a finite set of L elements $\mathbf{Q} := \{x_1, \ldots, x_L\} \subseteq X$ such that the following formula holds:

(1.1) $$\forall f \in \Omega, \quad f(x_1) = \cdots = f(x_L) = 0 \in K^m \Longrightarrow f \in \Sigma.$$

In the case $\Sigma = \{0\} \subsetneq \Omega$, we say that $\mathbf{Q}$ is a correct test sequence for Ω. The section is structured as an expository section where we show several equivalent notions of correct test sequences, depending on the context: As identity sequences (when viewed in $\Omega - \Omega$ and $\Sigma = \{0\}$), as finite *norming sets* in the case K is a field with some absolute value (see Proposition 4.4), in the ring of continuous functions $\mathscr{C}(X)$ on a topological space (see Proposition 4.6) or in Reproducing Kernel Hilbert Spaces (see Proposition 4.9).

In Subsection 4.2 we focus on multivariate polynomials as the main subject of these pages. For an algebraically closed field K and a positive integer $d \in \mathbb{N}$, we consider the vector space $P_d^K := P_d^K(X_1, \ldots, X_n)$ of all polynomials in $K[X_1, \ldots, X_n]$ of degree at most d. For a list

of degrees $(d) := (d_1, \ldots, d_m) \in \mathbb{N}^m$, we consider the class $\mathscr{P}_{(d)}^K$ of all lists $f := (f_1, \ldots, f_m)$ of m polynomials such that $f_i \in P_{d_i}^K$ for every i, $1 \leq i \leq m$. Thus, we discuss correct test sequences $\mathbf{Q}$ associated to constructible subsets $\Omega \subseteq \mathscr{P}_{(d)}$ with respect to some discriminant subset $\Sigma \subsetneq \Omega$. Our main remark in this subsection is a kind of *curse of dimensionality of correct test sequences* (cf. Proposition 4.12): If $\mathbf{Q}$ is a correct test sequence of length L for a constructible set $\Omega \subseteq \mathscr{P}_{(d)}^K$ with respect to Σ, then:

$$L \geq \dim(\Omega) - \dim(\Sigma) = \operatorname{codim}_\Omega(\Sigma).$$

This lower bound establishes the limits to have correct test sequences: An *optimal length correct test sequence for* Ω will be a correct test sequence of length in $O(\dim(\Omega))$.

Then, we address the question of whether correct test sequences of optimal length exist in Section 5. Our main outcome first proves that correct test sequences of optimal length exist not only for parametrized constructible sets (as in [HeSc, 82]) but for any constructible set. Secondly, we prove that length L correct test sequences do exist not only in *grid-like sets* (of the form $(Q_1 \times \cdots \times Q_n)^L \subseteq (\mathbb{A}^n)^L$, where $Q_i \subseteq K$ is a finite set): Correct test sequences may be found in any constructible set of accurate dimension and degree. Last but not least, we prove that correct test sequences of optimal length are highly dense in probability terms in any set of the form C^L, where C is locally closed and L is in $O(\dim(\Omega))$.

All these properties are stated in Theorem 5.1. Given $C \subseteq \mathbb{A}^n$ a locally closed set, $L \in \mathbb{N}$ a positive integer and Ω and Σ as above, we denote by $R(\Omega, \Sigma, C, L)$ the constructible set of all sequences $\mathbf{Q} \in C^L$ of length L which are correct test sequences for Ω with respect to Σ. Theorem 5.1 proves that, under some technical hypothesis on the degree and the dimension of C, for $L \geq 6 \dim(\Omega)$, the set $R(\Omega, \Sigma, C, L)$ is highly dense in C^L. We discuss the particular case when C is a complete intersection variety in several Corollaries. We reproduce here Corollary 5.5 which exhibits the high density of correct test sequences in the case C is a complete intersection variety of accurate dimension and degree:

Main Theorem 1.3. *Let $m, n \in \mathbb{N}$ be two positive integers, with $m \leq n$, and let $(d) := (d_1, \ldots, d_m)$ be a list of degrees and $d := \max\{d_1, \ldots, d_m\}$. Let $\Sigma \subseteq \Omega$ be two constructible subsets of $\mathscr{P}_{(d)}(X_1, \ldots, X_n)$ such that Σ has co-dimension at least 1 in Ω. Assume that $\Omega \setminus \Sigma$ satisfies the following property:*

$$(1.2) \qquad \forall f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma, \ \dim(V_\mathbb{A}(f_1, \ldots, f_m)) = n - m,$$

Let $C := V_\mathbb{A}(h_1, \ldots, h_r) \subseteq \mathbb{A}^n$ be a complete intersection algebraic variety of co-dimension $r \geq (n - m) + m/2 + 1/2$ such that $\deg(C) \geq \delta^r$, where $\delta := \min\{\deg(h_1), \ldots, \deg(h_r)\}$. Let $L \in \mathbb{N}$ be a positive integer and assume that the following properties hold:

i) $L \geq 6 \dim(\Omega)$,
ii) $\log(\delta) \geq \max\{2(1 + \log(d + 1)), \frac{2 \log(\deg_{\mathrm{lci}}(\Omega))}{\dim(\Omega)}\}$,
iii) $\max\{\deg(h_1), \ldots, \deg(h_r)\} \leq (1 + \frac{1}{n-m})\delta$,

where $\log$ stands for the natural logarithm. Let $R := R(\Omega, \Sigma, C, L)$ be the constructible set of all sequences $\mathbf{Q} \in C^L$ of length L which are correct test sequences for Ω with respect to Σ. Then, there is a non-empty Zariski open subset $\mathbb{G}(C)$, in the space $\mathbb{G}(n, n - r)$ of all linear affine varieties of co-dimension $n - r$, such that for every $A \in \mathbb{G}(C)$ the probability that a randomly chosen list $\mathbf{Q} \in (C \cap A)^L$ is in R satisfies:

$$\operatorname{Prob}_{(C \cap A)^L}[R] \geq 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega) e^{\dim(\Omega) + (m-1)L}},$$

where $(A \cap C)^L$ is endowed with its uniform probability distribution.

Note that if we introduce in C a probability distribution based on a Poincaré-like formula for algebraically closed fields (see Section 2 of [BP, 07] for the complex case) involving $\sharp(C \cap A)$ with $A \in \mathbb{G}(n, n - r)$, the previous statement simply claims that the measure of $R(\Omega, \Sigma, C, L)$ in C^L is close to 1.

Trying to answering some of the features that differ between DeMillo-Lipton-Schwartz-Zippel test and correct test sequences, we also prove that correct test sequences of optimal length are highly dense inside the sampling set of the test designed by these authors in [DML, 78], [Zp, 79] and [Sch, 80]. This is done in Corollary 5.10.

In Section 6 we exhibit an immediate application of our approach to correct test sequences: A **BBP**$_K$ algorithm for the *"Suite Sécante" Problem*. Our goal is to design an algorithm that solves the following problem:

Problem 1 ("Suite Sécante" Problem). *Given $f \in \mathscr{P}_{(d)}$ decide whether f is a "Suite Sécante". Namely, decide whether the following property holds:*
The algebraic variety $V_{\mathbb{A}}(f_1, \ldots, f_m) \subseteq \mathbb{A}^n$ is a non-empty variety of dimension $n - m$.

But we do not want to use any of the standard techniques in Computational Algebraic Geometry. In this field, the input is usually a list of polynomials and the goal is to determine, among other things, the dimension of the affine set of their common zeros. This is done by manipulating the input list in different forms (computing a Gröbner basis of the ideal, using variations of Bertini's Theorems to approximate the zero set by a complete intersection variety, etc.). *Our method exhibits the "strange" power of correct test sequences: Our algorithm answers to this problem in polynomial time doing no manipulation of the input list of polynomials. It just evaluates the input list of polynomial equations f at some well-suited points, i.e., it computes $f(x_1), \ldots, f(x_L) \in K^m$ for some $x_1, \ldots, x_L$.*
We restrict to the case of *fields which are well-suited for CTS's guessing*. We say that a field K is well-suited for CTS's guessing in zero-dimensional varieties if it satisfies the following property:
For every $R \in \mathbb{N}$ and every positive integer $n \in \mathbb{N}$, there is a zero-dimensional variety $V_R \subseteq \mathbb{A}^n(K)$ of degree R^n given by polynomial equations of degree at most R, and such that the following task may be performed with at most $O(n \log_2(R))$ arithmetic operations:

$$\textbf{guess at random } x \in V_R.$$

Thus, we prove Theorem 6.2, which we reproduce here in order to improve accessibility for the reader:

Main Theorem 1.4. *If K is a field well-suited for CTS's guessing, the problem "Suite Sécante" with restricted inputs is in* **BPP**$_K$. *Namely, let (d) be a degree list and let $\Omega \subseteq \mathscr{P}_{(d)}$ be a constructible subset of lists of polynomials. Let $U \subseteq \mathscr{P}_{(d)}$ be the Zariski open subset described in Theorem 6.1 of lists that are "Suites Sécantes". Assume that $\Omega \setminus (\Omega \cap U)$ has dimension at most $\dim(\Omega) - 1$. Then, there is an algorithm in* **BPP**$_K$ *that solves "Suite Sécante" Problem with inputs in Ω, i.e.:*
Given as input $f \in \Omega$ and the data $\dim(\Omega)$ and $\deg_{\mathrm{lci}}(\Omega)$, the algorithm decides whether f is a "Suite Sécante" or not.
The running time of the algorithm in terms of arithmetic operations is at most:

$$O\left(\dim(\Omega)n\left((T + \log(\dim(\Omega)) + \log(d)) + Tn\log(\deg_{\mathrm{lci}}(\Omega))\right)\right).$$

where T is the maximum number of arithmetic operations required to evaluate at one point any list $f := (f_1, \ldots, f_m) \in \Omega$ and $d := \max\{d_1, \ldots, d_m\}$. The error probability is bounded by:

$$\frac{1}{\deg_{\mathrm{lci}}(\Omega)e^{6m\dim(\Omega)}}.$$

In the dense input case (i.e. $\Omega = \mathscr{P}_{(d)}^K$) the total number of arithmetic operations is of order:

$$O(nN_{(d)}^2),$$

where $N_{(d)} = \dim_K(\mathscr{P}_{(d)})$ and the error probability is bounded by:

$$\frac{1}{e^{6mN_{(d)}}}.$$

We finally devote Appendix B to reformulate two well-known statements of the *Polynomial Method* in terms of correct test sequences:

- In Subsection B.2 we discuss Dvir exponential lower bounds for Kakeya sets (cf. [Dv, 09]) in terms of correct test sequences. We show that Kakeya sets are correct test sequences for certain constructible sets and, hence, Dvir's lower bound is a consequence of the *curse of dimensionality* discussed above (in Corollary B.2). We also prove that most correct test sequences are not Kakeya sets when the degree of the involved polynomials is bounded by $q^{1-\varepsilon} - 1$ for small $\varepsilon > 0$ (see Corollary B.3).

- In Subsection B.3 we also see that Alon's Combinatorial Nullstellensatz (cf. [Al, 99]) is also related to our treatment of correct test sequences. In particular, we show how duality in zero-dimensional reduced algebras is related to Alon's main outcome in [Al, 99].

2. Bézout's Inequality for constructible sets

In the early 80's of the last century, three authors have independently arrived to three different proofs of some Bézout's Inequalities. They took different approaches of the notion of degree of an algebraic variety, and they used different techniques to achieve their outcomes, although the underlyign notion has some coincidences. These three authors were W. Vogel (cf. [Vo, 84]), J. Heintz (cf. [He, 83]) and W. Fulton (cf. [Fu, 83]). Neither Fulton nor Vogel dealt with constructible sets, whereas Heintz developed [He, 83] an affine version of the notion which was systematically called *degree of constructible sets*. Nevertheless, as already observed in [He, 85], Heintz's statements do not hold for constructible sets and they only hold for locally closed subsets of some affine space. The question that remained open was to introduce a right notion of degree of constructible sets and prove that this notion satisfies a Bézout's Inequality. In this section we close that gap.

2.1. **Closed, locally closed and constructible sets in Zariski's topopology.** As in the introduction, K is an algebraically closed field and $K[X_1, \ldots, X_n]$ is the ring of polynomials in the set of variables $\{X_1, \ldots, X_n\}$ with coefficients in K. We shall denote by $\mathbb{A}^n(K)$ (or $\mathbb{A}^n$ when no confusion may arise) the affine space of dimension n over K. Given a finite set of polynomials $\{f_1, \ldots, f_s\} \subseteq K[X_1, \ldots, X_n]$, we denote by $V_{\mathbb{A}}(f_1, \ldots, f_s) \subseteq \mathbb{A}^n(K)$ the algebraic variety of the common zeros in $\mathbb{A}^n(K)$ of these polynomials. Namely,

$$V_{\mathbb{A}}(f_1, \ldots, f_s) := \{x \in \mathbb{A}^n(K) \ : \ f_1(x) = f_2(x) = \cdots = f_s(x) = 0\}.$$

If $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ is an ideal, we also denote by $V_{\mathbb{A}}(\mathfrak{a}) \subseteq \mathbb{A}^n(K)$ the set of common zeros of all polynomials in $\mathfrak{a}$. Obviously, if $\mathfrak{a}$ is the ideal generated by the finite set $\{f_1, \ldots, f_s\}$ (i.e. $\mathfrak{a} = (f_1, \ldots, f_s)$), we then have $V_{\mathbb{A}}(\mathfrak{a}) = V_{\mathbb{A}}(f_1, \ldots, f_s)$.

There is a unique topology in $\mathbb{A}^n(K)$ whose closed sets are affine algebraic varieties, which is usually known as the *Zariski topology* on $\mathbb{A}^n(K)$. For each subset $S \subseteq \mathbb{A}^n$ we denote by $\overline{S}^z$ the closure of S with respect to the Zariski topology in $\mathbb{A}^n$. For every subset $X \subseteq \mathbb{A}^n$, the topology induced on X by the Zariski topology of $\mathbb{A}^n$ will be called the Zariski topology of X. We then use the terms *Zariski open in X* or *Zariski closed in X* to describe open and closed sets in X with respect to its Zariski topology.

Definition 1 (Locally closed and constructible sets in Zariski's topology of $\mathbb{A}^n$). *The intersection of an open and a closed subsets of the Zariski topology of $\mathbb{A}^n$ will be called* locally closed *subset. A locally closed subset $V \subseteq \mathbb{A}^n$ is called* irreducible *if V is an open subset in a closed irreducible variety of $\mathbb{A}^n$. Finite unions of locally closed sets are called* constructible sets *(in the most classical tradition of Elimination Theory, see [Ch, 64-65]).*

Some authors prefer to use the term *quasi-projective variety* instead of locally closed (cf. [Sha, 77], for instance). As the context of this manuscript is essentially affine, we avoid to discuss the projective terminology, except if required.

The classical Chevalley Theorem explains the need of using constructible sets in Elimination Theory: They are the projections of closed sets.

Theorem 2.1 ([Ch, 64-65]). *A subset $C \subseteq \mathbb{A}^n(K)$ is constructible if and only if there is some $m \in \mathbb{N}$ and some algebraic variety $V \subseteq \mathbb{A}^{n+m}(K)$ such that $C := \pi(V)$, where $\pi : \mathbb{A}^{n+m}(K) \longrightarrow \mathbb{A}^n(K)$ is the canonical projection.*

As affine Zariski topology is Noetherian, locally closed sets admit a minimal decomposition as finite union of locally closed irreducible sets. Uniqueness up to permutation of these minimal decompositions of locally closed sets allow us to use the term *locally closed irreducible components*. For a locally closed subset $V \subseteq \mathbb{A}^n$, its locally closed irreducible components are uniquely determined because they are in bijection with the irreducible components of its Zariski closure $\overline{V}^z$. This fact is easy to prove since every locally closed irreducible set is dense in its Zariski closure. We see later that this uniqueness cannot be immediately extended to constructible sets.

For every locally closed subset $V \subseteq \mathbb{A}^n$ we denote by $K[V]$ the ring of polynomial functions defined on V. A polynomial map between two locally closed sets $\varphi : V \longrightarrow W$ is called *dominant* if the image $\varphi(V)$ is Zariski dense in W (which is equivalent to the fact that $K[W]$ is embedded as subring of $K[V]$). If V is irreducible, $K[V]$ is an integral domain and we denote by $K(V)$ the field of rational functions defined on V (i.e. the field of fractions of $K[V]$).

The *dimension* of a constructible subset $C \subseteq \mathbb{A}^n$ will be its Krull dimension as topological space. Namely, the length of the longest chain of locally closed irreducible subsets of $\mathbb{A}^n$ included in C. Constructible sets also admit a decomposition into irreducible components (cf. [Ch, 64-65], for instance). As we shall see in Example 2.3, irreducible components of constructible sets are not always closed irreducible subsets. We have the following decomposition:

Lemma 2.2. *Let $C \subseteq \mathbb{A}^n(K)$ be a constructible subset. Then, there is a finite set $\mathscr{C} := \{U_1 \cap V_1, \ldots, U_s \cap V_s\}$ of locally closed irreducible sets such that the following properties hold:*

$$(2.1) \qquad\qquad C := (U_1 \cap V_1) \cup \cdots \cup (U_s \cap V_s),$$

and

> *i) V_i is an irreducible algebraic variety in $\mathbb{A}^n$,*
> *ii) U_i is the maximum of the Zariski open subsets $O_i \subseteq \mathbb{A}^n$ such that $O_i \cap V_i \subseteq C$,*
> *iii) $V_i \neq V_j$.*

Proof. As C is a finite union of locally closed subsets $C = W_1 \cup \cdots \cup W_s$, just taking the irreducible components of each W_i we conclude that C is a finite union of locally closed irreducible sets. As non-empty open subsets of irreducible varieties are dense in the Zariski topology, just rearranging these locally closed irreducible sets, we may assume a decomposition as the following one:

$$(2.2) \qquad\qquad C := (O_1 \cap V_1) \cup \cdots \cup (O_r \cap V_r),$$

where for each i, $1 \leq i \leq r$, $O_i \subseteq \mathbb{A}^n$ is a Zariski open subset and $V_i \subseteq \mathbb{A}^n$ is a locally closed irreducible subset such that $V_i \neq V_j$ for each $i \neq j$. If there were some i and j such that $V_i = V_j$, we just replace $(O_i \cap V_i) \cup (O_j \cap V_j)$ by $(O_i \cup O_j) \cap V_i$. Thus, we may assume that condition *iii*) holds. Finally, it suffices to take the maximum of the Zariski open subsets $U_i \subseteq \mathbb{A}^n$ such that $U_i \cap V_i \subseteq C$ to finish the proof. The existence of this maximum is guaranteed by the fact that the union of open sets is open in any topology. $\qquad\square$

Example 2.3 (**La Croix de Berny**). We first observe that the decomposition of constructible sets into irreducible locally closed subsets is not unique. In addition, we see that even if polynomial images of algebraic varieties are always constructible sets (Chevalley's Theorem, cf. [Ch, 64-65]), they are not always locally closed. Let us consider the following cubic hyper-surface of $\mathbb{A}^3(\mathbb{C})$:

$$(2.3) \qquad\qquad W := \{(x, y, z) \in \mathbb{A}(\mathbb{C})^3 \ : \ zxy + (x^2 + y^2 - 1) = 0\}.$$

Note that this hyper-surface is irreducible since the polynomial $h(X, Y, Z) = ZXY + (X^2 + Y^2 - 1) \in \mathbb{C}[X, Y][Z]$ is a primitive polynomial (as $gcd(XY, X^2 + Y^2 - 1) = 1$ in $\mathbb{C}[X, Y]$) of degree 1. The degree of this hyper-surface is 3 according to the notion of degree in [He, 83].

Let $\pi : \mathbb{A}^3(\mathbb{C}) \longrightarrow \mathbb{A}^2(\mathbb{C})$ be the projection that forgets the coordinate z (i.e. $\pi(x, y, z) := (x, y)$, for all $(x, y, z) \in \mathbb{A}^3(\mathbb{C})$). We then observe that $\pi(W)$ is the following constructible set:

$$C := \pi(W) = \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \ : \ xy \neq 0\} \cup \{(0, 1), (0, -1), (1, 0), (-1, 0)\}.$$

This is a decomposition of C into five locally closed irreducible sets which satisfies the properties of the precedent Lemma 2.2:

$$C := C_1 \cup \{(1, 0)\} \cup \{(-1, 0)\} \cup \{(0, 1)\} \cup \{(0, -1)\},$$

where $C_1 \subseteq \mathbb{A}^2(\mathbb{C})$ is the following Zariski open subset:

$$C_1 := \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \ : \ xy \neq 0\}.$$

We also have another decomposition of $C = \pi(W)$ as the union of two locally closed irreducible subsets:

$$C := C_1 \cup \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x^2 + y^2 - 1 = 0\}.$$

This happens because C is not locally closed. Moreover, the irreducible components of the Zariski closure $\overline{C}^z$ of C, which is the irreducible variety $\mathbb{A}^2(\mathbb{C})$, are not in bijection with the

Zariski closures of the irreducible sets occuring in such decompositions. In particular, the irreducible components of C as Noetherian topological space (in the sense of Definition 9, Proposition 9 and pages 22-23 of [Ch, 64-65]) are not always locally closed sets.

Before to proceed, let us see a basic problem with dimension in constructible sets:

Example 2.4 (**Local versus global dimension in constructible sets**). We reconsider the example of La Croix de Berny introduced in Example 2.3 above. There, we considered the following constructible set:

$$C := \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ xy \neq 0\} \cup \{(0,1),(0,-1),(1,0),(-1,0)\}.$$

Let C_x be the local germ of C at the point $x = (1,0)$ with respect to the Zariski topology (the arguments also hold for the Euclidean topology in $\mathbb{A}^2(\mathbb{C})$). It is obvious that the dimension of C at x is 2: Any neighborhood of x contains a piece of dimension 2 of C. In particular, C has *local* and *global* (at any point $z \in C$) dimension equal to 2, however, it cannot be represented as a finite union of locally closed irreducible varieties of dimension 2. If C were the union of several locally closed irreducible subsets of dimension 2, then C would be a Zariski open subset of $\mathbb{A}^2(\mathbb{C})$, which is not the case as we have seen in Example 2.3.

Uniqueness of locally closed irreducible "components" is only granted for highest dimension components.

Proposition 2.5 (**Components of higher dimension of a constructible set**). *With the same notations and assumptions as above, if $C \subseteq \mathbb{A}^n$ is a constructible set, then C admits a decomposition satisfying i), ii) and iii) of Lemma 2.2 above:*

$$C := (U_1 \cap V_1) \cup \cdots \cup (U_s \cap V_s),$$

such that there exists $r \leq s$, verifying:

$$\dim(C) = \dim(V_i) \Longleftrightarrow 1 \leq i \leq r.$$

The varieties $V_1, \ldots, V_r$ are uniquely determined and they are the irreducible components of higher dimension of the Zariski closure of C. The varieties $V_{r+1}, \ldots, V_s$ are called embedded components of C.

Definition 2 (**Globally equi-dimensional constructible sets**). *Let $C \subseteq \mathbb{A}^n$ be a constructible subset. We say that C is* globally equi-dimensional *if there is a decomposition of C as finite union of locally closed irreducible subsets:*

$$C := (U_1 \cap V_1) \cup \cdots \cup (U_s \cap V_s),$$

that satisfies the conditions of Lemma 2.2 and such that the dimension also verifies:

$$\dim(C) = \dim(U_i \cap V_i) = \dim(V_i), \ 1 \leq i \leq s.$$

As we have seen, the constructible set described in Example 2.3 is not globally equi-dimensional, although it is locally equi-dimensional and it is the projection of a hyper-surface. In particular, locally closed subsets such that their Zariski closure is equi-dimensional are globally equi-dimensional.

Remark 2.6 (**Decompositions into equal dimension globally equi-dimensional pieces**). Given a decomposition of a constructible set $C = W_1 \cap \cdots \cap W_s \subseteq \mathbb{A}^n(K)$, with $W_i = U_i \cap V_i$, as in Lemma 2.2, we may also decompose C as a finite union of globally equi-dimensional constructible sets:

$$C := C_r \cup \cdots \cup C_0,$$

where $r = \dim(C)$ and

$$C_k := \bigcup_{\dim(W_i)=k} W_i.$$

We call such decomposition a *equal dimension decomposition of C*. As we have seen in Example 2.3, equal dimension decompositions are not unique. The example described there admits several equal dimension decompositions:

$$C := \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ xy \neq 0\} \cup \{(\pm 1, 0), (0, \pm 1)\},$$

and

$$C := \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ xy \neq 0\} \cup \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x^2 + y^2 - 1 = 0\}.$$

2.2. **Degree of locally closed sets according to [He, 83] and their Bézout's Inequality.**
We now resume some of the statements of [He, 83] which hold for locally closed sets. Let
$V \subseteq \mathbb{A}^n(K)$ be a locally closed irreducible subset of (Krull) dimension r. Let $\mathbb{A}^{nr} := \mathbb{A}^{nr}(K) = \mathcal{M}_{r \times n}(K)$ be the space of $r \times n$ matrices with coordinates in K. Let $\mathbb{A}^r := \mathbb{A}^r(K)$ be the affine
space of dimension r over K. As in [He, 83], we consider the following polynomial mapping:

$$(2.4) \qquad \begin{array}{rccc} \Phi : & \mathbb{A}^{nr} \times V & \longrightarrow & \mathbb{A}^{nr} \times \mathbb{A}^r \\ & (M, x) & \longmapsto & (M, Mx) \end{array}$$

The following statement was proved in [He, 83] (cf. also [BGHLMPS, 19]):

Proposition 2.7. *With the previous notations, we have:*

  i) The morphism Φ is a dominant morphism and the following is a finite and separable field extension:

$$\Phi^* : K(\mathbb{A}^{rn} \times \mathbb{A}^r) \hookrightarrow K(\mathbb{A}^{rn} \times V).$$

  ii) For every point $(M, b) \in \mathbb{A}^{rn} \times \mathbb{A}^r$, if the fiber $\Phi^{-1}(\{(M, b)\})$ is finite, then we have:

$$\sharp \left(\Phi^{-1}(\{(M, b)\}) \right) \leq [K(\mathbb{A}^{rn} \times V) : K(\mathbb{A}^{rn} \times \mathbb{A}^r)].$$

  iii) There is a Zariski open subset $\mathcal{U} \subseteq \mathbb{A}^{rn} \times \mathbb{A}^r$ such that for every $(M, b) \in \mathcal{U}$, the fiber $\Phi^{-1}(\{(M, b)\})$ is finite and satisfies:

$$\sharp \left(\Phi^{-1}(\{(M, b)\}) \right) = [K(\mathbb{A}^{rn} \times V) : K(\mathbb{A}^{rn} \times \mathbb{A}^r)].$$

Let us now consider $GL(n, r) \subseteq \mathbb{A}^{r(n+1)}$ the Zariski subset of all pairs $(M, b) \in \mathbb{A}^{r(n+1)}$ such
that $\mathrm{rank}(M) = r$. Namely, given a pair $(M, b) \in \mathbb{A}^{r(n+1)}$ we consider the linear affine variety
$\mathbb{G}(M, b)$ given by the following identity:

$$\mathbb{G}(M, b) := \{x \in \mathbb{A}^n : Mx^t - b = 0\},$$

where x^t is the transpose of $x = (x_1, \ldots, x_n)$. Then, $GL(n, r)$ is the set of all pairs (M, b) such
that the co-dimension satisfies $\mathrm{codim}(\mathbb{G}(M, b)) = r$. We then consider the "Grassmannian"
$\mathbb{G}(n, r)$ of all linear affine varieties in $\mathbb{A}^n$ of co-dimension r and we have the following onto
mapping:

$$\begin{array}{rccc} \mathscr{G} : & \mathbb{A}^{rn} \times \mathbb{A}^r & \longrightarrow & \mathbb{G}(n, r) \\ & (M, b) & \longmapsto & \mathbb{G}(M, b). \end{array}$$

Note that *the Zariski topology in $\mathbb{G}(n, r)$ is defined as the final topology induced in $\mathbb{G}(n, r)$ by
$\mathscr{G}$ and the Zariski topology in $GL(n, r)$.* Let $V \subseteq \mathbb{A}^n(K)$ be a locally closed irreducible subset
of dimension r and let us introduce the class:

$$\mathbb{G}(V) := \{A \in \mathbb{G}(r, n) : \sharp(V \cap A) < \infty\}.$$

The following properties immediately follow from [He, 83]:

Proposition 2.8. *With the same notations and assumptions, we have:*

  i) The class $\mathbb{G}(V)$ is non-empty and contains an open subset of $\mathbb{G}(n, r)$.
  ii) The maximum $\max\{\sharp(A \cap V) : A \in \mathbb{G}(V)\}$ is finite.
  iii) There is a Zariski open subset $\mathcal{U} \subseteq \mathbb{G}(n, r)$ such that for all $A \in \mathcal{U}$ we have:

$$\sharp(A \cap V) = \max\{\sharp(T \cap V) : T \in \mathbb{G}(V)\}.$$

Definition 3 (Degree of a locally closed subset). *Let $V \subseteq \mathbb{A}^n(K)$ be a locally closed
irreducible subset. We define the degree of V as the following quantity:*

$$\deg(V) := \max\{\sharp(A \cap V) : A \in \mathbb{G}(n, r), \sharp(A \cap V) < \infty\}.$$

*Let $W \subseteq \mathbb{A}^n(K)$ be any locally closed subset and let $C_1, \ldots, C_s$ its locally closed irreducible
components. The degree of W is defined as:*

$$\deg(W) := \sum_{i=1}^{s} \deg(C_i).$$

Some immediate properties are resumed on the following Proposition:

Proposition 2.9. *With the same notations and assumptions as above, we have:*

i) *For every locally closed subset $V \subseteq \mathbb{A}^n$, its degree agrees with the degree of its Zariski closure, i.e.*

$$\deg(V) = \deg(\overline{V}^z).$$

ii) *The degree of a finite set $C \subseteq \mathbb{A}^n$ equals its cardinal:*

$$\deg(C) = \sharp(C).$$

iii) *The number of irreducible components of a locally closed set is bounded by its degree.*

iv) *The degree of any linear affine variety is 1.*

v) *The degree of locally closed sets is invariant by linear or affine isomorphisms.*

vi) *For every non-constant $f \in K[X_1, \ldots, X_n]$, the degree of the hyper-surface $V_{\mathbb{A}}(f)$ is at most the degree of the polynomial $\deg(f)$ and $\deg(V_{\mathbb{A}}(f)) = \deg(f)$ if and only if f is square-free.*

As in [He, 83], the following Lemmata also hold:

Lemma 2.10. *Let $V \subseteq \mathbb{A}^n(K)$ be a locally closed subset and $A \subseteq \mathbb{A}^n(K)$ be a linear affine variety. Then, we have:*

$$\deg(V \cap A) \leq \deg(V).$$

Lemma 2.11. *Let $V \subseteq \mathbb{A}^n$ be an equi-dimensional locally closed set of dimension r. Then, we have:*

$$\deg(V) = \max\{\sharp(A \cap V) \ : \ A \in \mathbb{G}(n, r), \ \sharp(A \cap V) < \infty\}.$$

Moreover, there is a non-empty Zariski open subset $\mathcal{U} \subseteq \mathbb{A}^{nr+r}$ such that for all $(M, b) \in \mathcal{U}$ the following holds:

$$\sharp(\mathbb{G}(M, b) \cap V) = \deg(V),$$

where, as above, $\mathbb{G}(M, b) := \{x \in \mathbb{A}^n \ : \ Mx^t = b\}$.

As in Remark 2 (2) of [He, 83], the degree of the Zariski closure is preserved by taking images by linear transformations:

Proposition 2.12. *Let $\ell : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$ be a linear mapping and $V \subseteq \mathbb{A}^n(K)$ a locally closed subset. Then, we have:*

$$\deg(\overline{\ell(V)}^z) \leq \deg(V).$$

Moreover, if $\ell(V)$ is locally closed we obtain:

$$\deg(\ell(V)) \leq \deg(V).$$

The heart of the new outcomes in [He, 83] is the fact that the degree of locally closed sets perfectly behaves with respect to Cartesian products:

Theorem 2.13. *Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be two locally closed sets. Let $V \times W \subseteq \mathbb{A}^{n+m}$ be its Cartesian product, which is also locally closed. Then, we have:*

$$\deg(V \times W) = \deg(V) \deg(W).$$

The previous results allow us to exhibit the *Bézout's Inequality for locally closed sets* of [He, 83]. The original proof is correct and its main ingredient is to consider $V \cap W$ as the projection of $(V \times W) \cap \Delta^{(2n)}$, where $\Delta^{(2n)} \subseteq \mathbb{A}^n \times \mathbb{A}^n$ is the diagonal subvariety in the Cartesian product space. As the image $V \cap W$ is locally closed, using Proposition 2.12 combined with Lemma 2.10 and Theorem 2.13, the following statement naturally follows:

Theorem 2.14 (**Bézout's Inequality for locally closed sets,** [He, 83])**.** *Let $V, W \subseteq \mathbb{A}^n(K)$ be two locally closed subsets. Then, we have:*

$$\deg(V \cap W) \leq \deg(V) \deg(W).$$

2.3. **Two notions of degree and two Bézout's Inequalities for constructible sets.**
A first notion of degree for constructible sets was introduced in [He, 83]: The "degree" of a constructible set $C \subseteq \mathbb{A}^n(K)$ was there defined as the degree of its Zariski closure. Let us call it the $Z-degree$ of C, which we denote by $\deg_z(C) := \deg(\overline{C}^z)$. That notion of degree does not satisfy a Bézout's Inequality for constructible sets. The following example shows that fact.

Example 2.15 ($Z-$**degree does not satisfy a Bézout's Inequality for constructible sets**).
Let us consider again the Example 2.3 above. We had the cubic irreducible hyper-surface:

$$W := \{(x, y, z) \in \mathbb{A}(\mathbb{C})^3 \ : \ zxy + (x^2 + y^2 - 1) = 0\}$$

and its image $C := \pi(W)$ under the canonical projection $\pi : \mathbb{A}^3(\mathbb{C}) \longrightarrow \mathbb{A}^2(\mathbb{C})$. We observed that $\overline{C}^z = \mathbb{A}^2(\mathbb{C})$ and, hence, the degree of its Zariski closure satisfies $\deg_z(C) = 1$. We may also consider the pair of lines $V := \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \ : \ xy = 0\}$, which is a degree 2 algebraic variety. We consider its intersection $C \cap V$ and we see that $C \cap V$ are the following four points in the plane:

$$C \cap V = \{(0, 1), (0, -1), (1, 0), (-1, 0)\},$$

Therefore, $\deg_z(C \cap V) = \deg(C \cap V) = 4$. Nevertheless, we have that:

$$4 \not\leq \deg_z(C) \deg_z(V) = 2.$$

This Example basically means that statements in [He, 83] concerning constructible sets are *either wrong or incomplete while using $Z-$degree of a constructible set as notion of degree.* This was already observed in [He, 85], where the author restricted the correctness of all statements in [He, 83] to the case of locally closed sets (as we did in Subsection 2.2 above). We have not found in the literature a notion of degree of constructible sets that generalizes the notion of degree of locally closed sets and also satisfies a Bézout's Inequality. This pushed us to find a good notion of degree of constructible sets that satisfies a Bézout's Inequality and this lead us to the following two notions of degree of a constructible set: The minimal degree of a presentation as union of locally closed irreducible sets (*LCI-degree*) and the minimal degree of a presentation as projection of a locally closed set ($\pi-degree$).

Definition 4 (*LCI*-**degree of a constructible set**). *Let $C \subseteq \mathbb{A}^n$ be a constructible subset. Let $\mathscr{C} := \{U_1 \cap V_1, \ldots, U_r \cap V_r\}$ be a decomposition of C as finite union of locally closed irreducible sets that satisfies Lemma 2.2. We define the degree of C relative to this decomposition as:*

$$\deg(C, \mathscr{C}) := \sum_{i=1}^{r} \deg(V_i).$$

We finally define the LCI-degree of C as the minimum of all the degrees of all decompositions of this kind:

$$\deg_{\mathrm{lci}}(C) := \min\{\deg(C, \mathscr{C}) \ : \ \mathscr{C} \text{ is a decomposition of } C \text{ that satisfies Lemma 2.2}\}.$$

We say that a decomposition $\mathscr{C} := \{U_1 \cap V_1, \ldots, U_r \cap V_r\}$ of a constructible set $C \subseteq \mathbb{A}^n$ is a minimum LCI-degree decomposition of C if $\mathscr{C}$ satisfies Lemma 2.2 and also:

$$\deg_{\mathrm{lci}}(C) = \sum_{i=1}^{r} \deg(V_i).$$

Definition 5 ($\pi-$**degree of a constructible set**). *As above, let $C \subseteq \mathbb{A}^n$ be a constructible set and we consider the class of all locally closed subsets that project onto C. Namely, for every $m \in \mathbb{N}$, $m \geq n$, we define:*

$$\Pi_m(C) := \{V \subseteq \mathbb{A}^m \ : V \text{ is locally closed and } \pi(V) = C\},$$

where $\pi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ is the canonical projection. We then define:

$$\Pi(C) := \bigcup_{m \geq n} \Pi_m(C),$$

and we define the projection degree (also $\pi-$degree) of C as the following minimum:

$$\deg_{\pi}(C) := \min\{\deg_z(V) \ : \ V \in \Pi(C)\}.$$

We obviously observe, taking $m = n$, that if C is locally closed, then using the "projection" $\pi := Id_n : \mathbb{A}^n \longrightarrow \mathbb{A}^n$ we obtain:

$$(2.5) \qquad\qquad \deg_\pi(C) \leq \deg(C) = \deg_z(C).$$

The three notions of degree are sub-additive functions:

Proposition 2.16. *The three notions* $\deg_z$, $\deg_\pi$ *and* $\deg_{\mathrm{lci}}$ *are sub-additive functions. Namely, given $C, C' \subseteq \mathbb{A}^n$ two constructible subsets. We have:*

$$\deg_z(C \cup C') \leq \deg_z(C) + \deg_z(C'),$$
$$\deg_\pi(C \cup C') \leq \deg_\pi(C) + \deg_\pi(C')$$

and,

$$\deg_{\mathrm{lci}}(C \cup C') \leq \deg_{\mathrm{lci}}(C) + \deg_{\mathrm{lci}}(C').$$

Proof. As the closure of a finite union is the union of the closures, the first inequality obviously holds and $\deg_z$ is sub-additive. As for the second inequality, it also follows almost immediately. We proof it for completeness. Assume $V \subseteq \mathbb{A}^{m_1}$ and $V' \subseteq \mathbb{A}^{m_2}$ are two locally closed subsets such that $m_1 \geq m_2 \geq n$ and $C := \pi_1(V)$, and $C' := \pi_2(V')$, where $\pi_1 : \mathbb{A}^{m_1} \longrightarrow \mathbb{A}^n$ and $\pi_2 : \mathbb{A}^{m_2} \longrightarrow \mathbb{A}^n$ are the two canonical projections. Assume also that $\deg_\pi(C) = \deg_z(V)$ and $\deg_\pi(C') = \deg_z(V')$. As $m_1 \geq m_2$, we may also define $V'' := V' \times \mathbb{A}^{m_1 - m_2}$ and by Theorem 2.13 we know that $\deg(V'') = \deg(V')$. It is also clear that $\pi_1(V'') = \pi_2(V') = C'$ and that $\pi_1(V \cup V'') = C \cup C'$. Hence, we have:

$$\deg_\pi(C \cup C') \leq \deg_z(V \cup V'') \leq \deg_z(V) + \deg_z(V'') = \deg_\pi(C) + \deg_\pi(C').$$

The third inequality is an immediate consequence of Definition 4. From two minimum *LCI*-degree decompositions of C and C' we may reconstruct a decomposition of $C \cup C'$ satisfying the properties described in Lemma 2.2. The degree of such decomposition is obviously greater than the degree of the union $C \cup C'$. $\qquad\qquad \square$

Example 2.17 (**Three different "degrees"**). The three notions $\deg_z$, $\deg_\pi$ and $\deg_{\mathrm{lci}}$ are different. In order to simplify the arguments, we slightly modify the constructible set exhibited in Example 2.3. We first consider the following quadratic hyper-surface:

$$(2.6) \qquad\qquad W' := \{(x,y,z) \in \mathbb{A}^3(\mathbb{C}) \ : \ xz + (y^2 - 1) = 0\},$$

and the constructible subset $C := \pi(W') \subseteq \mathbb{A}^2(\mathbb{C})$, where $\pi : \mathbb{A}^3(\mathbb{C}) \longrightarrow \mathbb{A}^2(\mathbb{C})$ is the canonical projection that forgets the variable z. Since C is Zariski dense in $\mathbb{A}^2(\mathbb{C})$, we obviously have that $\deg_z(C) = 1$.
As C is the projection of W' and $\deg(W') = 2$, we have $\deg_\pi(C) \leq 2$. Moreover, $\deg_\pi(C) \neq 1$ since, otherwise, C would be the projection of a non-empty Zariski open subset of a linear affine variety, which cannot be possible because C is not an open subset of $\mathbb{A}^2(\mathbb{C})$.
Additionally, we claim that $\deg_{\mathrm{lci}}(C) = 3$. We have the following decomposition of C:

$$(2.7) \qquad C := \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x \neq 0\} \cup \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x^2 + y^2 - 1 = 0\}.$$

Hence, we conclude that $\deg_{\mathrm{lci}}(C) \leq 3$. Let us see now that $2 < \deg_{\mathrm{lci}}(C)$. For if $\deg_{\mathrm{lci}}(C) = 2$, as the open set $C_1 = \mathbb{A}^2(\mathbb{C}) \setminus V_\mathbb{A}(X)$ is maximal (C is not locally closed), then C would decompose as a union of at most two locally closed irreducible sets:

$$C = \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x \neq 0\} \cup B,$$

where B is locally closed irreducible of degree 1 (namely, B is a Zariski open subset of a linear affine subvariety of $\mathbb{A}^2(\mathbb{C})$). We may now consider the following intersection:

$$C \cap \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x = 0\} = B \cap \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x = 0\}.$$

Since $C_1 \cap \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x = 0\} = \emptyset$, $C \cap \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x = 0\} = \{(0,1), (0,-1)\}$ and Bézout's Inequality for locally closed subsets holds, we would conclude:

$$2 = \sharp\big(B \cap \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x = 0\}\big) \leq \deg(B) \deg\big(\{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x = 0\}\big) = 1 \cdot 1 = 1,$$

which is false. Thus, we have proven that $\deg(B) \geq 2$ and, hence, $3 \geq \deg_{\mathrm{lci}}(C) = 1 + \deg(B) \geq 3$ as wanted. Thus, there are constructible sets $C \subseteq \mathbb{A}^2(\mathbb{C})$ such that the three notions of degree above take different values:

$$1 = \deg_z(C) < 2 = \deg_\pi(C) < \deg_{\mathrm{lci}}(C) = 3.$$

There is no uniqueness in the embedded components of a decomposition of constructible sets that minimize LCI-degree:

Remark 2.18 (**Non-uniqueness of embedded components minimizing $LCI-$degree**). As in Example 2.17 above, we have a constructible set $C \subseteq \mathbb{A}^2(\mathbb{C})$, dense in $\mathbb{A}^2(\mathbb{C})$ for the Zariski topology and of LCI-degree 3, which is given by the following decomposition as finite union of locally closed irreducible subsets that minimize the degree:

$$C = \{(x,y) \in \mathbb{C}^2 \ : \ x \neq 0\} \cup \{(x,y) \in \mathbb{C}^2 \ : \ x^2 + y^2 - 1 = 0\}.$$

For every $a \in \mathbb{C}$, we may consider the polynomial $h_a(X,Y) := X^2 + Y^2 + aXY - 1$. Then, we see that there are infinitely many decompositions of C as finite union of locally closed sets that minimize the LCI-degree as in the following equality:

$$C = \{(x,y) \in \mathbb{C}^2 \ : \ x \neq 0\} \cup \{(x,y) \in \mathbb{C}^2 \ : \ h_a(x,y) = 0\}.$$

This is because the ideals $(X, X^2 + Y^2 - 1)$ and $(X, h_a(X,Y))$ are the same ideal in $\mathbb{C}[X,Y]$ for every $a \in \mathbb{C}$.

Our LCI-degree generalizes the notion of degree for locally closed sets introduced in [He, 83]. We resume this fact in the next Proposition of straightforward proof:

Proposition 2.19. *Let $C \subseteq \mathbb{A}^n(K)$ be a constructible set which is either locally closed set or globally equi-dimensional. Then, $\deg_z(C)$ and $\deg_{\mathrm{lci}}(C)$ agree. Namely,*

$$\deg_z(C) = \deg(\overline{C}^z) = \deg_{\mathrm{lci}}(C).$$

Remark 2.20 (**LCI-degree and equal dimension decomposition**). We may also consider an equal dimensional decomposition of a constructible set $C \subseteq \mathbb{A}^n(K)$ of dimension r as in Remark 2.6. As in that Remark, let $\mathscr{D} := \{C_r, \ldots, C_0\}$ be a decomposition of C as finite union of globally equi-dimensional constructible sets. We consider the following quantity associated to this decomposition:

$$\deg_z(C, \mathscr{D}) := \sum_{i=0}^{r} \deg_z(C_i).$$

As $\deg_{\mathrm{lci}}$ is sub-additive and because of Proposition 2.19, we have:

$$\deg_{\mathrm{lci}}(C) \leq \deg_z(C, \mathscr{D}).$$

Moreover, taking a decomposition of C into locally closed irreducible sets that minimize the degree:

$$C := W_1 \cup \cdots \cup W_s,$$

such that

$$\deg_{\mathrm{lci}}(C) := \sum_{i=1}^{s} \deg(W_i),$$

and reorganizing this decomposition into equal degree components, we obtain a decomposition $\mathscr{W} := \{D_r, \ldots, D_0\}$ such that:

$$\deg_{\mathrm{lci}}(C) := \sum_{i=0}^{r} \deg_{\mathrm{lci}}(D_i) = \sum_{i=0}^{r} \deg_z(D_i).$$

Hence, the $LCI-$degree could have been defined in terms of equal dimension components as follows:

$$\deg_{\mathrm{lci}}(C) := \min\{\deg_z(C, \mathscr{D}) \ : \ \mathscr{C} \text{ is a globally equi-dimensional decomp. of } C \text{ as in Rk. 2.6}\}.$$

Proposition 2.21. *For every constructible subset $C \subseteq \mathbb{A}^n(K)$ of dimension r, the following inequalities hold:*

$$\deg_z(C) \leq \deg_\pi(C) \leq \deg_{\mathrm{lci}}(C).$$

Moreover, given an equal dimension decomposition of C into globally equi-dimensional constructible sets $C := C_r \cup \cdots \cup C_0$, we have:

$$\deg_{\mathrm{lci}}(C) \leq (\dim(C) + 1) \max\{\deg_z(C_i) \ : \ 0 \leq i \leq r\}.$$

Proof. Let $V \in \Pi_m(C)$ be a locally closed subset of $\mathbb{A}^m$ such that $\pi(V) := C$, where $\pi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ is the canonical projection, and $\deg_\pi(C) = \deg_z(V)$. Because of Proposition 2.12, we have:

$$\deg_z(C) = \deg(\overline{\pi(V)}^z) \leq \deg(V) = \deg_\pi(C),$$

which proves the first inequality. As for the second inequality, assume a decomposition of C as finite union of locally closed irreducible subsets:

$$C := W_1 \cup \cdots \cup W_r,$$

such that

$$\deg_{\mathrm{lci}}(C) = \sum_{i=1}^r \deg(W_i).$$

As $\deg_\pi$ is sub-additive, we obtain:

$$\deg_\pi(C) \leq \sum_{i=1}^r \deg_\pi(W_i).$$

Thus, as W_i is locally closed, from Inequality 2.5, we conclude $\deg_\pi(W_i) \leq \deg(W_i)$ and the second inequality holds. The last inequality easily follows from Remark 2.20 above. $\square$

Remark 2.22. In general, it is not true that $\deg_{\mathrm{lci}}(C) \leq (\dim(C) + 1)\deg_z(C)$. Just consider the following example which extends the constructible set introduced in Example 2.17:

$$C' := \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x \neq 0\} \cup \{(0, \pm 1)\} \cup \{(0, \pm 2)\}.$$

One may prove that $\deg_{\mathrm{lci}}(C') = 5$ with similar arguments to those used in Example 2.17. Hence, this example proves that

$$5 = \deg_{\mathrm{lci}}(C') \not\leq (\dim(C') + 1)\deg_z(C') = 3 \cdot 1 = 3.$$

Also our π-degree generalizes the notion of degree for locally closed sets (and globally equi-dimensional constructible sets):

Corollary 2.23. *Let $C \subseteq \mathbb{A}^n(K)$ be a constructible set. If C is either locally closed or globally equi-dimensional, we have:*

$$\deg_z(C) = \deg(\overline{C}^z) = \deg_\pi(C) = \deg_{\mathrm{lci}}(C).$$

Moreover, if $C \subseteq \mathbb{A}^n(K)$ is a globally equi-dimensional constructible set of dimension r, then there is a non-empty Zariski open subset $\mathbb{G}(C) \subseteq \mathbb{G}(n, r)$ such that the following holds for every $A \in \mathbb{G}(C)$:

$$\sharp(A \cap C) = \deg_z(C) = \deg_\pi(F) = \deg_{\mathrm{lci}}(C).$$

Proof. Combining Propositions 2.21 and Proposition 2.19 the equality immediately follows. The second claim also follows immediately from the definitions and Proposition 2.8. $\square$

In the general case, all what we have for intersections with linear affine varieties is the following statement:

Corollary 2.24. *Let $C \subseteq \mathbb{A}^n(K)$ be a constructible set of dimension r and let $V_1, \ldots, V_s$ be the irreducible components of higher dimension of the Zariski closure of C (as in Proposition 2.5). Then, there is a non-empty Zariski open subset $\mathbb{G}(C) \subseteq \mathbb{G}(n, r)$ such that the following holds for every $A \in \mathbb{G}(C)$:*

$$\sharp(A \cap C) = \sum_{i=1}^s \deg(V_i) \leq \deg_z(C) \leq \deg_\pi(C) \leq \deg_{\mathrm{lci}}(C).$$

The following statements correct Remark 2 (2) and explains Lemma 2 of [He, 83] about degree of linear images of constructible sets. Again, we begin with the *LCI*-degree:

Proposition 2.25. *Let $C \subseteq \mathbb{A}^n$ be a constructible set and $\ell : \mathbb{A}^n \longrightarrow \mathbb{A}^m$ be a linear map. We have:*

i) The degree of the Zariski closure of the image is bounded as follows:

$$\deg_z(\ell(C)) = \deg\left(\overline{\ell(C)}^z\right) \leq \deg_{\mathrm{lci}}(C).$$

ii) *If $\ell(C)$ is locally closed or globally equi-dimensional, we also have:*

$$\deg_z(\ell(C)) = \deg_{\mathrm{lci}}(\ell(C)) \leq \deg_{\mathrm{lci}}(C).$$

iii) *In general, it is not true that given a linear affine variety $A \subseteq \mathbb{A}^m$ the following holds:*

$$\sharp(A \cap \ell(C)) \leq \deg_z(C).$$

iv) *In general, it is not true that $\deg_{\mathrm{lci}}(\ell(C)) \leq \deg_{\mathrm{lci}}(C)$.*

Proof. The first Claim is an immediate consequence of Proposition 2.12 combined with the sub-additivity of the LCI-degree (Proposition 2.16 above).

Claim $ii)$ follows from the fact that $\deg_{\mathrm{lci}}(C) = \deg_z(C)$ for every subset $C \subseteq \mathbb{A}^n$ that is either locally closed or globally equi-dimensional.

For Claim $iii)$, just consider the constructible set $C \subseteq \mathbb{A}^2(\mathbb{C})$ described in Example 2.17 above and the Identity $Id : C \longrightarrow \mathbb{A}^2(\mathbb{C})$ as linear functional. Let $A := \{(x, y) \in \mathbb{A}^2 \ : \ x = 0\}$ be the line in the plane. Then, we have that $A \cap Id(C)$ is made of two points, whereas $\deg_z(C) = 1$. Hence,

$$2 = \sharp(A \cap Id(C)) \not\leq \deg_z(C) = 1.$$

For Claim $iv)$, we use the same constructible subset $C \subseteq \mathbb{A}^2(\mathbb{C})$ introduced in Example 2.17 above. There, we proved that C is a constructible set such that $\deg_{\mathrm{lci}}(C) = 3$ and, at the same time, it is the projection of an algebraic variety $W' \subseteq \mathbb{A}^3(\mathbb{C})$ of degree 2. Hence, we have that the following holds and proves Claim $iv)$:

$$3 = \deg_{\mathrm{lci}}(\pi(W')) \not\leq \deg_{\mathrm{lci}}(W') = \deg(W') = 2.$$

$$\square$$

On the other hand, $\deg_\pi$ is well-behaved for linear images of constructible sets. This is resumed in the following statement:

Proposition 2.26. *Let $C \subseteq \mathbb{A}^n$ be a constructible subset. For every $m \geq n$, let us consider the class $\mathscr{L}_m(C)$ of all pairs (V, ℓ), where $V \subseteq \mathbb{A}^m$ is a locally closed set, $\ell : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ is a linear mapping and $\ell(V) = C$. Finally, let us consider the class:*

$$\mathscr{L}(C) := \bigcup_{m \geq n} \mathscr{L}_m(C).$$

Then, we have:

i) *The $\pi-$degree satisfies:*

$$\deg_\pi(C) = \min\{\deg_z(V) \ : \ \exists \ell : \mathbb{A}^m \longrightarrow \mathbb{A}^n, \ (V, \ell) \in \mathscr{L}(C)\}.$$

ii) *For every linear function $\lambda : \mathbb{A}^n \longrightarrow \mathbb{A}^r$, we have:*

$$\deg_z(\lambda(C)) \leq \deg_\pi(\lambda(C)) \leq \deg_\pi(C) \leq \deg_{\mathrm{lci}}(C).$$

Proof.

- *Proof of Claim i):* Let $(V, \ell) \in \mathscr{L}(C)$ be one of such pairs. We may consider $G \subseteq \mathbb{A}^{m+n}$ the graph of the restriction $\ell|_V$. We observe that G is also a locally closed set since:

  $$G := \{(z, y) \in \mathbb{A}^m \times \mathbb{A}^n \ : \ z \in V, \ \ell(z) - y = 0\}.$$

  Clearly, G is the intersection of $V \times \mathbb{A}^n$ with the linear affine variety:

  $$A := \mathbb{A}^m \times \{(z, y) \in \mathbb{A}^{m+n} \ : \ \ell(z) - y = 0\}.$$

  Hence, because of the Bézout's Inequality for locally closed sets (Theorem 2.14 above) we know that:

  $$\deg_z(G) = \deg(G) \leq \deg(V \times \mathbb{A}^n) \deg(A) = \deg(V) \cdot 1.$$

  Moreover, let $\pi : \mathbb{A}^{m+n} \longrightarrow \mathbb{A}^n$ be the canonical projection given by:

  $$\pi(z, y) := y, \ \forall(z, y) \in \mathbb{A}^{m+n}.$$

  We obviously have that $C := \pi(G)$ and, hence, we conclude:

  $$\deg_\pi(C) \leq \deg_z(V), \ \forall(V, \ell) \in \mathscr{L}(C).$$

The other inequality is obvious since projections are particular instances of linear mappings. Therefore, the first Claim is proved.

- *Proof of Claim ii):* If $\lambda : \mathbb{A}^n \longrightarrow \mathbb{A}^r$ is a linear mapping, then we have:

$$\mathscr{L}(\lambda(C)) \supseteq \{(V, \lambda \circ \ell) \; : \; (V, \ell) \in \mathscr{L}(C)\}.$$

Hence, as:

$$\deg_\pi(\lambda(C)) = \min\{\deg_z(V) \; : \; \exists \rho, \; (V, \rho) \in \mathscr{L}(\lambda(C))\},$$

we immediately conclude:

$$\deg_\pi(\lambda(C)) \leq \min\{\deg_z(V) \; : \; \exists \ell, \; (V, \ell) \in \mathscr{L}(C), \; (V, \lambda \circ \ell) \in \mathscr{L}(\lambda(C))\} = \deg_\pi(C),$$

and Claim *ii)* follows.

$\square$

In what respect to other properties, both the LCI-degree and the $\pi-$degree behave as expected for the natural operations between constructible sets:

Proposition 2.27. *Let $C \subseteq \mathbb{A}^n$ and $D \subseteq \mathbb{A}^m$ be two constructible sets.*

i) For every linear affine variety $A \subseteq \mathbb{A}^n$ the following two inequalities hold:

$$\deg_{\mathrm{lci}}(A \cap C) \leq \deg_{\mathrm{lci}}(C), \;\; \deg_\pi(A \cap C) \leq \deg_\pi(C).$$

ii) The degrees of the Cartesian product satisfy the following inequalities:

$$\deg_{\mathrm{lci}}(C \times D) \leq \deg_{\mathrm{lci}}(C) \deg_{\mathrm{lci}}(D), \;\; \deg_\pi(C \times D) \leq \deg_\pi(C) \deg_\pi(D).$$

iii) For every Zariski open subset $U \subseteq \mathbb{A}^n$, we have:

$$\deg_{\mathrm{lci}}(C \cap U) \leq \deg_{\mathrm{lci}}(C), \;\; \deg_\pi(C \cap U) \leq \deg_\pi(C).$$

Proof. We prove every inequality first for $\deg_{\mathrm{lci}}$ and then for $\deg_\pi$:

- *Inequalities for* $\deg_{\mathrm{lci}}$*:* Claims *i)* and *ii)* easily follow from the sub-additivity of $\deg_{\mathrm{lci}}$ and the corresponding properties for locally closed sets. As for Claim *iii)*, suppose C is decomposed as a finite union of locally closed irreducible sets:

$$C = W_1 \cup \cdots \cup W_s,$$

such that $\deg_{\mathrm{lci}}(C) = \sum_{i=1}^s \deg(W_i)$. As U is Zariski open, then for every i, $1 \leq i \leq s$, we have just two options: Either $U \cap W_i = \emptyset$ or $U \cap W_i \neq \emptyset$, in which case $U \cap W_i$ is locally closed and Zariski dense in $\overline{W_i}^z$. Hence, we would have:

$$\deg_{\mathrm{lci}}(C \cap U) \leq \sum_{i=1}^s \deg(U \cap W_i) = \sum_{i=1}^s \deg(W_i) = \deg_{\mathrm{lci}}(C).$$

- *Inequalities for* $\deg_\pi$*:* For Claim *i)*, assume there is a locally closed subset $V \subseteq \mathbb{A}^m$ such that $\pi(V) := C$ and $\deg_\pi(C) = \deg_z(V)$, where $\pi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ is the canonical projection. We thus consider the linear affine subvariety $B := \pi^{-1}(A) \subseteq \mathbb{A}^m$. We have that $\pi(V \cap B) = C \cap A$ and, hence,

$$\deg_\pi(C \cap A) \leq \deg_z(V \cap B) \leq \deg_z(V).$$

For Claim *ii)*, assume that there exist two locally closed sets $V \subseteq \mathbb{A}^{m_1}$ and $W \subseteq \mathbb{A}^{m_2}$ such that $m_1 \geq n$ and $m_2 \geq m$, and $\pi_1(V) := C$, $\pi_2(W) := D$, where $\pi_1 : \mathbb{A}^{m_1} \longrightarrow \mathbb{A}^n$ and $\pi_2 : \mathbb{A}^{m_2} \longrightarrow \mathbb{A}^m$ are the canonical projections, $\deg_\pi(C) = \deg_z(V)$ and $\deg_\pi(D) = \deg_z(W)$. Therefore, we consider the affine space $\mathbb{A}^{m_1+m_2} := \mathbb{A}^{m_1} \times \mathbb{A}^{m_2}$ and the product projection:

$$\overline{\pi} := \pi_1 \times \pi_2 : \quad \begin{array}{ccc} \mathbb{A}^{m_1} \times \mathbb{A}^{m_2} & \longrightarrow & \mathbb{A}^n \times \mathbb{A}^m \\ (z_1, z_2) & \longmapsto & (\pi_1(z_1), \pi_2(z_2)). \end{array}$$

Then, $\overline{\pi}(V \times W) = C \times D$ and, as $V \times W$ is locally closed, we conclude:

$$\deg_\pi(C \times D) \leq \deg(V \times W) = \deg_z(V) \deg_z(W) = \deg_\pi(C) \deg_\pi(D).$$

Finally, for Claim *iii)* we have that there exists $V \subseteq \mathbb{A}^m$ locally closed such that $\pi(V) := C$ and $\deg(V) = \deg_\pi(C)$, where $\pi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ is the canonical projection.

Taking the open subset $\widetilde{U} := \pi^{-1}(U) \subseteq \mathbb{A}^m$, we have that $C \cap U = \pi(V \cap \widetilde{U})$ and the following inequalities hold because V is locally closed:

$$\deg_\pi(C \cap U) \leq \deg_z(V \cap \widetilde{U}) \leq \deg_z(V) = \deg_\pi(C).$$

$\square$

Finally, both $\deg_{\mathrm{lci}}$ and $\deg_\pi$ satisfy a Bézout's Inequality.

Theorem 2.28 (Bézout's Inequalities for constructible sets). *Let $C, D \subseteq \mathbb{A}^n$ be two constructible sets. We have:*

$$\deg_{\mathrm{lci}}(C \cap D) \leq \deg_{\mathrm{lci}}(C) \deg_{\mathrm{lci}}(D), \quad \deg_\pi(C \cap D) \leq \deg_\pi(C) \deg_\pi(D).$$

Proof. We first prove the inequality for $\deg_\pi$ and, then, for $\deg_{\mathrm{lci}}$. For $\deg_\pi$ the statement is almost obvious. Let us first consider the Cartesian product $C \times D \subseteq \mathbb{A}^{2n}$. Next, let $\Delta^{(2n)} \subseteq \mathbb{A}^{2n}$ be the linear affine subvariety given by the following identity:

$$\Delta^{(2n)} := \{(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{A}^{2n} \ : \ x_i - y_i = 0, 1 \leq i \leq n\}.$$

Let $\pi : \mathbb{A}^{2n} \longrightarrow \mathbb{A}^n$ be the projection onto the first n variables. We have:

$$\pi\left((C \times D) \cap \Delta^{(2n)}\right) = C \cap D.$$

From Claim ii) of Proposition 2.26, we have that:

$$\deg_\pi(C \cap D) \leq \deg_\pi\left((C \times D) \cap \Delta^{(2n)}\right).$$

As $\Delta^{(2n)}$ is a linear affine subvariety, we deduce from Claim i) of Proposition 2.27 that:

$$\deg_\pi(C \cap D) \leq \deg_\pi(C \times D).$$

And, finally, Claim ii) of Proposition 2.27 yields the final inequality:

$$\deg_\pi(C \cap D) \leq \deg_\pi(C \times D) \leq \deg_\pi(C) \deg_\pi(D).$$

In the case of $\deg_{\mathrm{lci}}$, the trouble is that degree is not preserved by linear transformations (as observed in Claim iii) of Proposition 2.25). Therefore, we have to make some subtle changes into the proof scheme used for $\deg_\pi$. As above, we consider the diagonal subvariety $\Delta^{(2n)} \subseteq \mathbb{A}^{2n}$ and its intersection with the Cartesian product:

$$C' := (C \times D) \cap \Delta^{(2n)}.$$

By Proposition 2.27, we conclude:

$$\deg_{\mathrm{lci}}(C') \leq \deg_{\mathrm{lci}}(C \times D) \leq \deg_{\mathrm{lci}}(C) \deg_{\mathrm{lci}}(D).$$

Then, we consider a minimum LCI-degree decomposition of C' in locally closed subsets as in Definition 4. Namely, a decomposition:

$$C' = W_1 \cup \ldots \cup W_s$$

where $W_i = U_i \cap V_i \neq \emptyset$, $U_i \subseteq \Delta^{(2n)}$ is a Zariski open set in $\Delta^{(2n)}$, $V_i \subseteq \Delta^{(2n)}$ is an irreducible subvariety for the Zariski topology and such that:

$$\deg_{\mathrm{lci}}(C') = \sum_{i=1}^{s} \deg(W_i) = \sum_{i=1}^{s} \deg(V_i).$$

For every i, $1 \leq i \leq s$, we consider:

- $O_i \subseteq \mathbb{A}^n$ given by:

$$O_i := \{\underline{x} \in \mathbb{A}^n \ : \ (\underline{x}, \underline{x}) \in U_i\},$$

- $Q_i \subseteq \mathbb{A}^n$ given by:

$$Q_i := \{\underline{x} \in \mathbb{A}^n \ : \ (\underline{x}, \underline{x}) \in V_i\}.$$

We immediately see that if $\pi : \mathbb{A}^{2n} \longrightarrow \mathbb{A}^n$ is the projection onto the first n coordinates, then $\pi\big|_{\Delta^{(2n)}} : \Delta^{(2n)} \longrightarrow \mathbb{A}^n$ is a biregular isomorphism. Hence, we conclude that O_i is a Zariski open set in $\mathbb{A}^n$, Q_i is a Zariski closed subset of $\mathbb{A}^n$ and we have:

$$\pi(W_i) = O_i \cap Q_i.$$

As $\pi(W_i)$ is locally closed, by Proposition 2.12 we conclude:

$$\deg(\pi(W_i)) = \deg(\overline{\pi(W_i)}^z) = \deg(Q_i) = \deg(O_i \cap Q_i) \le \deg(W_i).$$

Additionally, we have:

$$C \cap D = \pi((C \times D) \cap \Delta^{(2n)}) = (O_1 \cap Q_1) \cup \ldots \cup (O_s \cap Q_s).$$

Finally, because of Proposition 2.16 we conclude:

$$\deg_{\mathrm{lci}}(C \cap D) \le \sum_{i=1}^{s} \deg(O_i \cap Q_i) \le \sum_{i=1}^{s} \deg(W_i) = \deg_{\mathrm{lci}}(C') \le \deg_{\mathrm{lci}}(C) \deg_{\mathrm{lci}}(D).$$

$\square$

3. Upper Bounds for the intersection of several constructible sets

In this Section we exhibit a generalization of Proposition 2.3 in [HeSc, 82] for constructible sets, as promised at the Introduction. Observe that a literal application of Bézout's Inequality puts the co-dimension at the exponent of bounds for the degree. Namely, given $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ such that $V := V_{\mathbb{A}}(f_1, \ldots, f_m)$ has dimension $n - m$, and let $W \subseteq \mathbb{A}^n$ be an algebraic variety. Bézout's Inequality yields the following upper bound:

$$\deg(W \cap V_{\mathbb{A}}(f_1, \ldots, f_m)) \le \deg(W) \prod_{i=1}^{m} \deg(f_i) \le \deg(W) \left(\max\{\deg(f_1), \ldots, \deg(f_m)\}\right)^{\mathrm{codim}(V)}.$$

Nevertheless, Proposition 2.3 in [HeSc, 82] replaces co-dimension of V by dimension of W, emphasizing the role of dimension of W in this kind of upper bounds. Namely, Proposition 2.3 in [HeSc, 82] yields:

$$\deg(W \cap V_{\mathbb{A}}(f_1, \ldots, f_m)) \le \deg(W) \left(\max\{\deg(f_1), \ldots, \deg(f_m)\}\right)^{\dim(W)}.$$

The trade-off between these two upper bounds is the key ingredient to prove the existence of short correct test sequences (see Theorem 5.1 in Section 5).

3.1. **Main statement of this Section.** Proposition 2.3 in [HeSc, 82] provides an elegant upper bound for the intersection of several algebraic varieties. We want to extend it for constructible sets but, obviously, it cannot be possible if we use $\deg_z$ by the same reason why Bézout's Inequality is not true for $\deg_z$. Hence, we first extend that result, using similar inductive arguments as in the original proof, for the intersection of a constructible set with several locally closed sets for both $\deg_{\mathrm{lci}}$ and $\deg_\pi$. Then, we try to exhibit a similar upper bound for the general case for $\deg_{\mathrm{lci}}$. We have not been able to stablish a similar result for $\deg_\pi$.

Proposition 3.1 (Extension of Proposition 2.3 of [HeSc, 82]). *Let $\Omega \subseteq \mathbb{A}^n$ be a constructible set and let $C_1, \ldots, C_s \subseteq \mathbb{A}^n$ be a finite sequence of locally closed sets. Then, we have:*

$$\deg_{\mathrm{lci}}\left(\Omega \cap \left(\bigcap_{i=1}^{s} C_i\right)\right) \le \deg_{\mathrm{lci}}(\Omega) \left(\max\{\deg_{\mathrm{lci}}(C_i) \ : \ 1 \le i \le s\}\right)^{\dim(\Omega)}.$$

Proof. The argument goes by induction on s as in [HeSc, 82]. The case $s = 2$ is just the Bézout's Inequality for constructible sets, then we assume $s \ge 3$. First of all, suppose that Ω is a locally closed irreducible set (i.e. a non-empty open set in some irreducible algebraic variety). Then, we decompose the intersection as:

$$\Omega \cap \left(\bigcap_{i=1}^{s} C_i\right) = (\Omega \cap C_1) \cap \left(\bigcap_{i=2}^{s} C_i\right).$$

We observe that $\Omega \cap C_1$ is locally closed and we may consider two options:

- Either $\dim(\Omega \cap C_1) = \dim(\Omega)$. In this case, as Ω is locally closed irreducible, then $\Omega \cap C_1$ is a locally closed set dense in $\overline{\Omega}^z$ and, we have:

$$\deg(\Omega \cap C_1) = \deg(\overline{(\Omega \cap C_1)}^z) \deg(\overline{\Omega}^z) = \deg(\Omega),$$

where the last equality is true since Ω is locally closed. Applying the inductive hypothesis, we conclude:

$$\deg\left(\Omega \cap \left(\bigcap_{j=1}^{s} C_j\right)\right) \leq \deg(\Omega \cap C_1)\left(\max\{\deg(C_i) \ : \ 2 \leq i \leq s\}\right)^{\dim(\Omega)},$$

which implies the statement.

- Or $\dim(\Omega \cap C_1) < \dim(\Omega)$. In this case, just using the inductive hypothesis we have:

$$\deg\left(\Omega \cap \left(\bigcap_{j=1}^{s} C_j\right)\right) \leq \deg(\Omega \cap C_1)\left(\max\{\deg(C_i) \ : \ 2 \leq i \leq s\}\right)^{\dim(\Omega \cap C_1)}.$$

Using the Bézout's Inequality for constructible sets we stated in previous sections, we obtain:

$$\deg\left(\Omega \cap \left(\bigcap_{j=1}^{s} C_j\right)\right) \leq \deg(\Omega) \deg(C_1)\left(\max\{\deg(C_i) \ : \ 2 \leq i \leq s\}\right)^{\dim(\Omega)-1},$$

and this also yields the wanted inequality.

As for the general case, let us consider a minimum LCI-degree decomposition of Ω into locally closed irreducible subsets. Namely, we consider a decomposition:

$$\Omega := (U_1 \cap V_1) \cup \cdots \cup (U_t \cap V_t),$$

where $U_i \cap V_i \neq \emptyset$, $U_i \subseteq \mathbb{A}^n$ is a Zariski open set, $V_i \subseteq \mathbb{A}^n$ is an irreducible closed subset for the Zariski topology and such that the following holds:

$$\deg_{\mathrm{lci}}(\Omega) = \sum_{i=1}^{t} \deg(V_i).$$

As the degree is sub-additive we have:

$$\deg_{\mathrm{lci}}\left(\Omega \cap \left(\bigcap_{j=1}^{s} C_j\right)\right) \leq \sum_{i=1}^{t} \deg\left((U_i \cap V_i) \cap \left(\bigcap_{j=1}^{s} C_j\right)\right).$$

As $(U_i \cap V_i)$ is locally closed irreducible, the previous arguments apply and we conclude:

$$\deg_{\mathrm{lci}}\left(\Omega \cap \left(\bigcap_{j=1}^{s} C_j\right)\right) \leq \sum_{i=1}^{t} \deg(V_i)\left(\max\{\deg(C_j) \ \ 1 \leq j \leq s\}\right)^{\dim(U_i \cap V_i)}.$$

As $\dim(\Omega) = \max\{\dim(U_i \cap V_i) \ : \ 1 \leq i \leq t\}$, we conclude the proof of the statement. $\qquad\square$

For the π-degree, we have a similar upper bound for globally equi-dimensional constructible sets:

Corollary 3.2. *Let $\Omega \subseteq \mathbb{A}^n$ be a globally equi-dimensional constructible set and let $C_1, \ldots, C_s \subseteq \mathbb{A}^n$ be a finite sequence of locally closed sets. Then, we have:*

$$\deg_\pi\left(\Omega \cap \left(\bigcap_{i=2}^{s} C_i\right)\right) \leq \deg_\pi(\Omega)\left(\max\{\deg_\pi(C_i) \ : \ 2 \leq i \leq s\}\right)^{\dim(\Omega)}$$

Proof. Essentially the same proof of the previous Proposition, just note that since Ω is globally equi-dimensional it admits a decomposition into locally closed irreducible sets $\Omega = W_1 \cup \cdots \cup W_s$ such that the following property holds:

$$\deg_\pi(\Omega) = \deg_{\mathrm{lci}}(\Omega) = \sum_{i=1}^{s} \deg(W_i).$$

$\qquad\square$

Proposition 3.1 also applies to have estimates on the degree of images of constructible sets under polynomial mappings as shown in the following Corollary.

Corollary 3.3. *Let* $\varphi := (\varphi_1, \ldots, \varphi_m) : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$ *be a polynomial mapping, where K is an algebraically closed field. Assume that for every i, $1 \leq i \leq m$, $\varphi_i \in K[X_1, \ldots, X_n]$ is a polynomial of degree at most d, where $d \geq 1$. Let $C \subseteq \mathbb{A}^n(K)$ be a constructible subset. Then, we have:*

$$\deg_z(\varphi(C)) \leq \deg_{\mathrm{lci}}(C) d^{\dim(C)},$$

$$\deg_z(\varphi(C)) \leq \deg_\pi(C) d^m \leq \deg_{\mathrm{lci}}(C) d^m.$$

The bounds are not always true if we replace $\deg_{\mathrm{lci}}$ by $\deg_z$ on the right hand side of the inequality. Moreover, if either $\varphi(C)$ is locally closed or globally equi-dimensional, we also have:

$$\deg_z(\varphi(C)) = \deg_\pi(\varphi(C)) = \deg_{\mathrm{lci}}(\varphi(C)) \leq \deg_{\mathrm{lci}}(C) d^{\dim(C)},$$

$$\deg_z(\varphi(C)) = \deg_\pi(\varphi(C)) = \deg_{\mathrm{lci}}(\varphi(C)) \leq \deg_\pi(C) d^m \leq \deg_{\mathrm{lci}}(C) d^m.$$

Proof.

- Inequality $\deg_z(\varphi(C)) \leq \deg_{\mathrm{lci}}(C) d^{\dim(C)}$: Let us first assume that C is locally closed and irreducible. Then, the Zariski closure $W := \overline{\varphi(C)}^z \subseteq \mathbb{A}^m(K)$ of $\varphi(C)$ is an irreducible variety. Let $D := \deg(W)$ be the degree of W and let $s := \dim(W) \leq \dim(V)$. Then, there is a linear affine subvariety $A \subseteq \mathbb{A}^m(K)$ of co-dimension s such that:

  $$\sharp(A \cap W) = \sharp(A \cap \varphi(C)) = \deg(W) = D.$$

  Let us now consider the algebraic variety $\varphi^{-1}(A) \subseteq \mathbb{A}^n(K)$. As A is given by s linear equations, then $\varphi^{-1}(A)$ is also given by s polynomial equations of degree at most d (combining the coordinates $\varphi_1, \ldots, \varphi_s$ of φ with the equations defining A in $\mathbb{A}^m$). From Proposition 3.1, we conclude:

  $$\deg_{\mathrm{lci}}(C \cap \varphi^{-1}(A)) \leq \deg_{\mathrm{lci}}(C) d^{\dim(C)}.$$

  Let $\mathscr{C}$ be the class of locally closed irreducible components of $C \cap \varphi^{-1}(A)$. As the number of irreducible components of a locally closed set is bounded by its degree, we conclude:

  $$\sharp(\mathscr{C}) \leq \deg_{\mathrm{lci}}(C \cap \varphi^{-1}(A)) \leq \deg_{\mathrm{lci}}(C) d^{\dim(C)}.$$

  However, let $V \in \mathscr{C}$ be one of such irreducible components of $C \cap \varphi^{-1}(A)$. We know that its Zariski closure $\overline{\varphi(V)}^z$ is irreducible and, at the same time, we have:

  $$\varphi(V) \subseteq A \cap \varphi(C).$$

  As $A \cap \varphi(C)$ is a finite number of points, $\varphi(V)$ has to be a point in $\mathbb{A}^m$. Additionally, as $\varphi(C \cap \varphi^{-1}(A)) = \varphi(C) \cap A$, there is an onto mapping between the following two finite sets:

  $$\begin{array}{cccc} \Phi: & \mathscr{C} & \longrightarrow & \varphi(C) \cap A \\ & V & \longmapsto & \Phi(V) := \varphi(V). \end{array}$$

  Then, we conclude that if C is a locally closed irreducible set we have:

  $$\deg(\overline{\varphi(C)}^z) = \deg(W) = \sharp(\varphi(C) \cap A) \leq \sharp(\mathscr{C}) \leq \deg(C) d^{\dim(C)}.$$

  For any constructible set $C \subseteq \mathbb{A}^n$, we just have to consider a minimum degree decomposition of C as in Definition 4, i.e. a decomposition of C as finite union of locally closed irreducible sets satisfying Lemma 2.2:

  $$C := (U_1 \cap V_1) \cup \cdots \cup (U_s \cap V_s),$$

  where $U_i \cap V_i \neq \emptyset$, $U_i \subseteq \mathbb{A}^n$ is open, $V_i \subseteq \mathbb{A}^n$ is closed irreducible in the Zariski topology and they satisfy:

  (3.1)
  $$\deg(C) = \sum_{i=1}^s \deg(V_i).$$

  Then, we have:

  $$\overline{\varphi(C)}^z = \overline{\left(\bigcup_{i=1}^s \varphi(U_i \cap V_i)\right)}^z = \bigcup_{i=1}^s \overline{\varphi(U_i \cap V_i)}^z.$$

As deg is sub-additive when applied to algebraic varieties, we would have:

$$\deg\left(\overline{\varphi(C)}^z\right) \leq \sum_{i=1}^s \deg\left(\overline{\varphi\left(U_i \cap V_i\right)}^z\right) \leq$$

$$\leq \sum_{i=1}^s \deg_{\text{lci}}(V_i \cap U_i)d^{\dim(V_i)} = \sum_{i=1}^s \deg(V_i)d^{\dim(V_i)}.$$

As $\dim(C) := \max\{\dim(V_1), \ldots, \dim(V_s)\}$, from Identity (3.1) we conclude:

$$\deg_z(\varphi(C)) \leq \left(\sum_{i=1}^s \deg(V_i)\right) d^{\dim(C)} = \deg_{\text{lci}}(C)d^{\dim(C)}.$$

- Inequality $\deg_z(\varphi(C)) \leq \deg_\pi(C)d^m \leq \deg_{\text{lci}}(C)d^m$: First, we consider the graph of the polynomial map φ:

$$Gr(\varphi) := \{(x,y) \in C \times \mathbb{A}^m \ : \ y_i - \varphi_i(x) = 0,\ i = 1, \ldots, m\} =$$

$$= (C \times \mathbb{A}^m) \cap (\bigcap_{i=1}^m \{Y_i - \varphi_i(X) = 0\}).$$

Then, let Φ be the following polynomial map:

$$\Phi: \quad C \quad \longrightarrow \quad Gr(\varphi)$$
$$x \quad \longmapsto \quad (x, \varphi(x)).$$

Obviously we have $\Phi(C) = Gr(\varphi)$, therefore $Gr(\varphi)$ is a constructible set. Let $\pi : \mathbb{A}^n \times \mathbb{A}^m \to \mathbb{A}^m$ be the canonical projection that forgets the first n variables. Thus, we have that $\varphi(C) = \pi(Gr(\varphi))$ and $\deg_z(\varphi(C)) = \deg_z(\pi(Gr(\varphi)))$. From Proposition 2.26, we conclude:

$$\deg_z(\pi(Gr(\varphi))) \leq \deg_\pi(\pi(Gr(\varphi))) \leq \deg_\pi(Gr(\varphi)).$$

Applying Bézout's inequality (for the π-degree), we deduce:

$$\deg_\pi(Gr(\varphi)) = \deg_\pi\left((C \times \mathbb{A}^m) \cap (\bigcap_{i=1}^m \{Y_i - \varphi_i(X) = 0\})\right) \leq$$

$$\leq \deg_\pi(C \times \mathbb{A}^m) \prod_{i=1}^m \deg_\pi(\{Y_i - \varphi_i(X) = 0\}).$$

As $\deg_\pi(C \times \mathbb{A}^m) \leq \deg_\pi(C)\deg_\pi(\mathbb{A}^m) = \deg_\pi(C)$ and for all i, $1 \leq i \leq m$, we have that $\deg_\pi(\{Y_i - \varphi_i(X) = 0\}) = \deg(Y_i - \varphi_i(X)) = \max\{deg(\varphi_i), 1\} \leq d$, we obtain:

$$deg_\pi(C \times \mathbb{A}^m) \prod_{i=1}^m \deg_\pi(\{Y_i - \varphi_i(X) = 0\}) \leq \deg_\pi(C)d^m.$$

Finally, from Proposition 2.21 we conclude:

$$\deg_z(\varphi(C)) \leq \deg_\pi(C)d^m \leq \deg_{\text{lci}}(C)d^m.$$

As for the counterexample, we just need to recall the one exhibited in Claim *iii*) of Proposition 2.25. The rest of the claims are obvious in the case $\varphi(C)$ is either locally closed or globally equi-dimensional. □

The remaining pages of this section are devoted to prove its main outcome:

Theorem 3.4 (Bounds for the LCI-degree of the intersection of several constructible sets). *Let $C_1, \ldots, C_s \subseteq \mathbb{A}^n$ be a sequence of constructible sets. Let $r := \dim(C_1)$ be the dimension of the constructible set C_1. The following inequalities hold:*

    i) First upper bound:

$$\deg_\pi\left(\bigcap_{i=1}^s C_i\right) \leq \deg_{\text{lci}}\left(\bigcap_{i=1}^s C_i\right) \leq \binom{s+r-1}{r} \deg_{\text{lci}}(C_1)\left(\max\{\deg_{\text{lci}}(C_j) \ : \ 2 \leq j \leq s\}\right)^r.$$

ii) Second upper bound:

$$\deg_\pi\left(\bigcap_{i=1}^s C_i\right) \le \deg_{\mathrm{lci}}\left(\bigcap_{i=1}^s C_i\right) \le \deg_{\mathrm{lci}}(C_1)\left(1 + \sum_{i=2}^s \deg_{\mathrm{lci}}(C_i)\right)^{\dim(C_1)}.$$

iii) Upper bound in terms of the average degree: *Given a family of constructible sets* $C_1, \ldots, C_s \subseteq \mathbb{A}^n$, *we define its average degree as:*

$$\deg_{\mathrm{av}}^{(E)}(C_1, \ldots, C_s) := \frac{1}{s}\sum_{i=1}^s \deg_{\mathrm{lci}}(C_i).$$

Then, we also have:

$$\deg_\pi\left(\bigcap_{i=1}^s C_i\right) \le \deg_{\mathrm{lci}}\left(\bigcap_{i=1}^s C_i\right) \le \deg_{\mathrm{lci}}(C_1)s^{\dim(C_1)}\left(\deg_{\mathrm{av}}^{(E)}(C_1, \ldots, C_s)\right)^{\dim(C_1)}.$$

First upper bound in the previous statement generalizes the main bound of Proposition 2.3 in [HeSc, 82], but the constant coefficient is exponential in $s-1$ because

$$\left(\frac{r+s-1}{s-1}\right)^{s-1} \le \binom{r+s-1}{r} \le \left(\frac{e(r+s-1)}{s-1}\right)^{s-1},$$

where e is the basis of the natural logarithm. The reader may also think that the constant is also exponential in r since

$$\left(\frac{r+s-1}{r}\right)^r \le \binom{r+s-1}{r} \le \left(\frac{e(r+s-1)}{r}\right)^r.$$

In any case it is not the constant 1 one would expected according to Proposition 2.3. of [HeSc, 82]. Third upper bound is simply obtained by rewriting second upper bound since $\deg_{\mathrm{lci}}(C_1) \ge 1$ always hold. Hence, second and third upper bounds are exponential in r, but polynomial in s which may be helpful in some applications. Note that the left hand side inequalities for the π-degree are an immediate consequence of Proposition 2.21.

The rest of the Section is devoted to prove this Theorem: First we prove Claim *i)* in Subsection 3.2 and, then, we prove Claim *ii)* in Subsection 3.3. Finally, some immediate applications of these discussions are exhibited in Subsection 3.4.

3.2. **Proof of the first bound of Theorem 3.4.** We begin with the case $s = 2$. Then, Bézout's Inequality for constructible sets yields:

$$\deg_{\mathrm{lci}}(C_1 \cap C_2) \le \deg_{\mathrm{lci}}(C_1)\deg_{\mathrm{lci}}(C_2) \le \binom{r+1}{r}\deg_{\mathrm{lci}}(C_1)\deg_{\mathrm{lci}}(C_2).$$

We thus apply induction and assume that $C_1 = W$ is a locally closed irreducible subset. Then, we have:

$$W \cap C_2 \cap \left(\bigcap_{i=3}^s C_i\right) = W \cap \left(\bigcap_{i=2}^s C_i\right).$$

We distinguish two cases:

- Assume that $\dim(W \cap C_2) < \dim(W)$. Then, applying the inductive hypothesis we have:

$$\deg_{\mathrm{lci}}\left(W \cap \left(\bigcap_{i=2}^s C_i\right)\right) \le \binom{\dim(W \cap C_2) + s - 2}{\dim(W \cap C_2)}$$
$$\deg_{\mathrm{lci}}(W \cap C_2)\left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 3 \le j \le s\}\right)^{\dim(W \cap C_2)}.$$

Now, observe that if $a \le b$ are two positive integers, we have:

$$\binom{a + (s-2)}{a} \le \binom{b + (s-2)}{b} \le \binom{b + (s-1)}{b}.$$

As $\dim(W \cap C_2) \leq \dim(W) - 1 \leq \dim(W)$ we have:

$$\deg_{\mathrm{lci}}\left(W \cap \left(\bigcap_{i=2}^{s} C_i\right)\right) \leq \binom{\dim(W) + s - 2}{\dim(W)}$$

$$\deg_{\mathrm{lci}}(W \cap C_2) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 3 \leq j \leq s\}\right)^{\dim(W)-1}.$$

Moreover, by Bézout's Inequality for constructible sets we would have:

$$\deg_{\mathrm{lci}}\left(W \cap \left(\bigcap_{i=2}^{s} C_i\right)\right) \leq \binom{\dim(W) + s - 2}{\dim(W)}$$

$$\deg(W) \deg_{\mathrm{lci}}(C_2) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 3 \leq j \leq s\}\right)^{\dim(W)-1}.$$

Putting everything together we conclude the wanted inequality:

$$\deg_{\mathrm{lci}}\left(W \cap \left(\bigcap_{i=2}^{s} C_i\right)\right) \leq \binom{\dim(W) + s - 1}{\dim(W)}$$

$$\deg(W) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 2 \leq j \leq s\}\right)^{\dim(W)}.$$

- Otherwise, assume that $\dim(W \cap C_2) = \dim(W)$. Let us consider a decomposition of C_2 as finite union of locally closed irreducible subsets:

$$C_2 = W_1 \cup W_2 \cup \cdots \cup W_m,$$

such that the degree of C_2 satisfies:

$$\deg_{\mathrm{lci}}(C_2) = \sum_{i=1}^{m} \deg(W_i).$$

Up to some reordering of the W_i's, as $\dim(W \cap C_2) = \dim(W)$, there must exist some integer r, with $1 \leq r \leq m$ such that the following holds:
  - For all i, $1 \leq i \leq r$, $\dim(W \cap W_i) = \dim(W)$.
  - For all i, $r + 1 \leq i \leq s$, $\dim(W \cap W_i) < \dim(W)$.

Next, we observe that the following set is a Zariski open subset in W and, hence, a locally closed irreducible set:

$$W \cap \left(\bigcup_{i=1}^{r} W_i\right).$$

Recall that both W and W_i are locally closed irreducible. Then, there are Zariski open subsets $U_1, U_2 \subseteq \mathbb{A}^n$ and irreducible algebraic varieties $V, V_i \subseteq \mathbb{A}^n$ such that:

$$W = U_1 \cap V, \ W_i = U_2 \cap V_i.$$

As $\dim(W) = \dim(W \cap W_i)$, then $W \cap W_i \neq \emptyset$ and, hence,

$$W \cap W_i = U_1 \cap U_2 \cap V \cap V_i.$$

In particular, $U_1 \cap U_2 \cap V$ is a non-empty Zariski open subset in V of dimension equal to $\dim(V)$. Moreover, the dimension of the intersection $U_1 \cap U_2 \cap V \cap V_i$ is also $\dim(V)$. Thus,

$$\dim(W \cap W_i) = \dim(U_1 \cap U_2 \cap V \cap V_i) = \dim(U_1 \cap U_2 \cap V) = \dim(V).$$

The Zariski closure of $W \cap W_i$ is then a closed subvariety of V of the same dimension than V. As V is irreducible:

$$\overline{W \cap W_i}^{z} = V.$$

On the other hand, it is obvious that $\overline{W \cap W_i}^{z} \subseteq V_i$ and, hence, we conclude $V \subseteq V_i$. Thus, we have:

$$W \cap W_i = U_i \cap V,$$

for some open subset $U_i \subseteq \mathbb{A}^n$. In conclusion, we have that:

$$W \cap \left(\bigcup_{i=1}^{r} W_i\right) = \left(\bigcup_{i=1}^{r} U_i\right) \cap V,$$

and this is a locally closed set.

Let us then define the following two constructible subsets:

$$C_2' := \bigcup_{i=1}^{r} W_i, \ \widetilde{C_2} := \bigcup_{j=r+1}^{s} W_j.$$

As $C_2' \cap W$ is a Zariski open subset of the Zariski closure of W, we conclude:

$$\deg(W \cap C_2') = \deg(W).$$

On the other hand, we have that:

$$\deg_{\mathrm{lci}}\left(\widetilde{C_2}\right) = \deg_{\mathrm{lci}}(C_2) - \sum_{i=1}^{r} \deg(W_i) \le \deg_{\mathrm{lci}}(C_2).$$

Hence, Bézout's Inequality for constructible sets yields:

$$\deg_{\mathrm{lci}}\left(W \cap \widetilde{C_2}\right) \le \deg(W)(\deg_{\mathrm{lci}}(C_2) - \sum_{i=1}^{r} \deg(W_i)) \le \deg(W)\deg_{\mathrm{lci}}(C_2).$$

Next, let us consider:

$$W \cap \left(\bigcap_{i=2}^{s} C_i\right) = \left((W \cap C_2') \cap \left(\bigcap_{i=3}^{s} C_i\right)\right) \cup \left((W \cap \widetilde{C_2}) \cap \left(\bigcap_{i=3}^{s} C_i\right)\right).$$

So, as $\deg_{\mathrm{lci}}$ is sub-additive for constructible sets, we conclude:

$$\deg_{\mathrm{lci}}\left(W \cap \left(\bigcap_{i=2}^{s} C_i\right)\right) \le I_1 + I_2,$$

where

$$I_1 := \deg_{\mathrm{lci}}\left((W \cap C_2') \cap \left(\bigcap_{i=3}^{s} C_i\right)\right),$$

and

$$I_2 := \deg_{\mathrm{lci}}\left((W \cap \widetilde{C_2}) \cap \left(\bigcap_{i=3}^{s} C_i\right)\right).$$

We bound both quantities separately:

– Taking $r := \dim(W) = \dim(W \cap C_2')$ and, knowing that $\deg(W) = \deg(W \cap C_2')$, the application of the induction hypothesis yields:

$$I_1 \le \binom{r+s-2}{r} \deg(W) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 3 \le j \le s\}\right)^r.$$

– On the other hand, let us consider $t := \dim(W \cap \widetilde{C_2}) \le r - 1$, knowing that $\deg_{\mathrm{lci}}(W \cap \widetilde{C_2}) \le \deg(W)\deg_{\mathrm{lci}}(C_2)$, the application of the induction hypothesis yields:

$$I_2 \le \binom{t+s-2}{t} \deg(W) \deg_{\mathrm{lci}}(C_2) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 3 \le j \le s\}\right)^t.$$

As $t \le r - 1$, we also have:

$$\binom{t+s-2}{t} \le \binom{r-1+s-2}{r-1} \le \binom{r-1+s-1}{r-1},$$

and, hence, we conclude:

$$I_2 \le \binom{r+s-2}{r-1} \deg(W) \deg_{\mathrm{lci}}(C_2) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 3 \le j \le s\}\right)^{r-1}.$$

Putting the two previous inequalities in a single one, we have:

$$I_1 + I_2 \le \deg(W) \left(\max\{\deg(C_j) \ : \ 3 \le j \le s\}\right)^{r-1}$$
$$\left(\binom{r+s-2}{r} \max\{\deg_{\mathrm{lci}}(C_j) \ : \ 3 \le j \le s\} + \binom{r+s-2}{r-1} \deg_{\mathrm{lci}}(C_2)\right).$$

Thus,

$$I_1 + I_2 \leq \deg(W) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 3 \leq j \leq s\} \right)^{r-1}$$
$$\max\{\deg_{\mathrm{lci}}(C_i) \ : \ 2 \leq i \leq s\} \left(\binom{r+s-2}{r} + \binom{r+s-2}{r-1} \right).$$

Using Pascal's Triangle equality we obtain:

$$I_1 + I_2 \leq \deg(W) \left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 2 \leq j \leq s\} \right)^r \binom{r+s-1}{r},$$

as wanted.

In order to conclude the general inequality, assume that C_1 admits a decomposition into locally closed irreducible varieties:

$$C_1 := V_1 \cup V_2 \cup \cdots \cup V_t,$$

such that

(3.2)
$$\deg_{\mathrm{lci}}(C_1) = \sum_{j=1}^{t} \deg(V_j).$$

Since $\deg_{\mathrm{lci}}$ is sub-additive, we obtain:

$$\deg_{\mathrm{lci}}\left(C_1 \cap \left(\bigcap_{i=2}^{s} C_i \right) \right) \leq \sum_{j=1}^{t} \deg_{\mathrm{lci}}\left(V_j \cap \left(\bigcap_{i=2}^{s} C_i \right) \right).$$

Applying the previous discussion, taking $r_j = \dim(V_j) \leq \dim(V)$ we conclude:

$$\deg_{\mathrm{lci}}\left(C_1 \cap \left(\bigcap_{i=2}^{s} C_i \right) \right) \leq \sum_{j=1}^{t} \binom{r_j+s-1}{r_j} \deg(V_j) \left(\max\{\deg_{\mathrm{lci}}(C_i) \ : \ 2 \leq i \leq s\} \right)^{r_j}.$$

As $r_j \leq r$ for each j, $1 \leq j \leq t$, we have:

$$\binom{r_j+s-1}{r_j} \leq \binom{r+s-1}{r},$$

and, hence, we deduce:

$$\deg_{\mathrm{lci}}\left(C_1 \cap \left(\bigcap_{i=2}^{s} C_i \right) \right) \leq \binom{r+s-1}{r} \left(\sum_{j=1}^{t} \deg(V_j) \right) \left(\max\{\deg_{\mathrm{lci}}(C_i) \ : \ 2 \leq i \leq s\} \right)^r.$$

Using Identity (3.2) we conclude the statement.

3.3. **Proof of the second bound of Theorem 3.4.** Here, we adapt some of the proof strategies of Section 3 of [He, 83], to produce a proof for the degree of the intersection of several constructible sets. Before going into the proof, we need of some preparatory results.

3.3.1. *Preparatory results.*

Definition 6. *Let $C \subseteq \mathbb{A}^n$ be a constructible set and $V \subseteq \mathbb{A}^n$ an irreducible variety. We say that V is an irreducible component of C with respect to the LCI-degree of C if there is some minimum LCI-degree decomposition of C into locally closed irreducible sets:*

$$C := W_1 \cup \cdots \cup W_s,$$

such that there exists i with $V = \overline{W_i}^z$.

Observe that if C is locally closed or globally equi-dimensional, then the class $\mathscr{D}(C)$ of all irreducible components of C with respect to the degree of C is a finite set and it is completely determined by C. This is not true for general constructible sets as we have shown in Remark 2.18.

Lemma 3.5. *Let $D \subseteq \mathbb{A}^n$ be a locally closed subset. Let $\mathscr{V}_1, \ldots, \mathscr{V}_s$ be several finite families of locally closed sets. Let $\mathscr{W}$ be the set of all locally closed subsets of $\mathbb{A}^n$ that may be defined as intersections with D of some locally closed sets chosen according to the list $\mathscr{V}_1, \ldots, \mathscr{V}_s$. Namely, let $\mathscr{W}$ be the set of locally closed sets given by the following identity:*

$$\mathscr{W} := \{D \cap \left(\bigcap_{i \in S} V_i \right) \ : \ S \subseteq \{1, \ldots, s\}, \ V_i \in \mathscr{V}_i\}$$

Let $\mathscr{C}$ be the set of algebraic varieties defined by the following identity:

$\mathscr{C} := \{V \ : \ V \text{ irreducible variety and } \exists W \in \mathscr{W}, \text{a non-empty open subset of } V \text{ is a component of } W\}.$

Then, we have:
(3.3)

$$\sum_{V \in \mathscr{C}} \deg(V) \leq \deg(D) \left(1 + \sum_{V \in \bigcup_{i=1}^s \mathscr{V}_i} \deg(V) \right)^{\dim(D)} \leq \deg(D) \left(1 + \sum_{i=1}^s \sum_{V \in \mathscr{V}_i} \deg(V) \right)^{\dim(D)}.$$

Moreover, there is a degree preserving bijection between $\mathscr{C}$ and the following set:
(3.4)
$$\mathscr{D} := \{C \ : \ \exists W \in \mathscr{W}, C \text{ is an irreducible component } \overline{W}^z\}.$$

and the same upper bound holds:
(3.5)

$$\sum_{C \in \mathscr{D}} \deg(C) \leq \deg(D) \left(1 + \sum_{V \in \bigcup_{i=1}^s \mathscr{V}_i} \deg(V) \right)^{\dim(D)} \leq \deg(D) \left(1 + \sum_{i=1}^s \sum_{V \in \mathscr{V}_i} \deg(V) \right)^{\dim(D)}.$$

Proof. First of all, as the degree is a sub-additive function, it will be enough to prove the Lemma for D locally closed irreducible. We assume it from now on.

Secondly, observe that all elements in $\mathscr{W}$ are locally closed sets. Hence, for every $W \in \mathscr{W}$, its locally closed irreducible components are in bijection with the irreducible components of $\overline{W}^z$. This bijection is given by the fact that locally closed irreducible components are simply Zariski open subsets on irreducible components of $\overline{W}^z$ and the degree is preserved. Conversely, irreducible components of $\overline{W}^z$ are simply the Zariski closures of the locally closed irreducible components of W. We proceed by proving the upper bound of Identity (3.5).

Let $d = \dim(D)$ be the dimension of D. Each $W \in \mathscr{W}$ and each $C \in \mathscr{D}$ also have dimension smaller than d. For each k, $0 \leq k \leq n$, let us define $\mathscr{D}(k)$ as the set of elements in $\mathscr{D}$ of dimension k, i.e.

$$\mathscr{D}(k) := \{C \in \mathscr{D} \ : \ \dim(C) = k\},$$

where $\mathscr{D}(r) = \emptyset$ for $d + 1 \leq r \leq n$. As D is locally closed irreducible, we have $\mathscr{D}(d) = \{\overline{D}^z\}$. For $k < d$ we have the following Claim:

Claim. *For each $C \in \mathscr{D}(k)$ there exist $C^* \in \mathscr{D}$ and $W \in \mathscr{V}_1 \cup \cdots \cup \mathscr{V}_s$ such that the following properties hold:*

- *i) The dimension of C^* is greater than $k + 1$ (i.e. $C^* \in \bigcup_{r=k+1}^d \mathscr{D}(r)$).*
- *ii) The irreducible variety C is an irreducible component of the Zariski closure of the intersection $C^* \cap W$.*

Proof of the Claim. Let $C \in \mathscr{D}(k)$ be an irreducible component and let $S \subseteq \{1, \ldots, s\}$ be a subset of minimal cardinal such that a Zariski open subset $U \cap C$ of C is a locally closed irreducible component of some intersection:

$$D \cap \left(\bigcap_{i \in S} V_i \right),$$

where $V_i \in \mathscr{V}_i$. As $k < d$, S cannot be the empty set. Let us define $S' := S \setminus \{j\}$ for some $j \in S$. Then, $U \cap C$ must be a locally closed irreducible component of

$$(D \cap W') \cap V_j,$$

where $W' := \left(\bigcap_{i \in S'} V_i \right)$.

Then, there exists a locally closed irreducible component C^* of W' such that some Zariski open subset of C is a locally closed irreducible component of $C^* \cap V_j$. Moreover, the dimension of C^* must be bigger than $k+1$ since, otherwise, C^* and C would agree on a Zariski open subset and, hence, S would not be of minimal cardinal. This proves the Claim. ∎

This Claim allows us to define the following mapping:

$$\Phi_k : \quad \mathscr{D}(k) \quad \longrightarrow \quad \left(\bigcup_{r=k+1}^{d} \mathscr{D}(r) \right) \times \left(\bigcup_{i=1}^{s} \mathscr{V}_i \right),$$
$$C \quad \longmapsto \quad (C^*, V)$$

given by the following rule:

To every $C \in \mathscr{D}(k)$ we associated a pair (C^*, V) such that a non-empty Zariski open subset of C is a locally closed irreducible component of $C^* \cap V$.

Let us define:

$$D(k) := \sum_{r=k}^{d} \sum_{C \in \mathscr{D}(r)} \deg(C),$$

we then prove by induction on $m = d - k$ the following inequality:

$$(3.6) \qquad D(k) = D(d-m) \leq \deg(D) \left(1 + \sum_{V \in \bigcup_{i=1}^{s} \mathscr{V}_i} \deg(V) \right)^m.$$

The case $m = 0$ is obviously true since $\mathscr{D}(d) = \{\overline{D}^z\}$ and D is locally closed. We have $D(d) = \deg(D)$.

Assume now that $m \geq 1$ and we have the following inequality:

$$\sum_{C \in \mathscr{D}(k)} \deg(C) \leq \sum_{(C^*, V) \in \left(\bigcup_{r=k+1}^{d} \mathscr{D}(r) \right) \times \left(\bigcup_{i=1}^{s} \mathscr{V}_i \right)} \sum_{C \in \Phi_k^{-1}(C^*, V)} \deg(C).$$

As all involved subsets are locally closed, for each $C^* \in \left(\bigcup_{r=k+1}^{d} \mathscr{D}(r) \right)$ and for each $V \in \left(\bigcup_{i=1}^{s} \mathscr{V}_i \right)$, from Theorem 2.14 we obtain:

$$\sum_{C \in \Phi_k^{-1}(C^*, V)} \deg(C) \leq \deg(C^*) \deg(V).$$

Therefore, we have:

$$\sum_{C \in \mathscr{D}(k)} \deg(C) \leq \sum_{(C^*, V) \in \left(\bigcup_{r=k+1}^{d} \mathscr{D}(r) \right) \times \left(\bigcup_{i=1}^{s} \mathscr{V}_i \right)} \deg(C^*) \deg(V).$$

Rearranging the sums, we get:

$$\sum_{C \in \mathscr{D}(k)} \deg(C) \leq \left(\sum_{C^* \in \left(\bigcup_{r=k+1}^{d} \mathscr{D}(r) \right)} \deg(C^*) \right) \left(\sum_{V \in \left(\bigcup_{i=1}^{s} \mathscr{V}_i \right)} \deg(V) \right) = D(k+1)R,$$

where $R = \sum_{V \in \left(\bigcup_{i=1}^{s} \mathscr{V}_i \right)} \deg(V)$. As $D(k) = D(k+1) + \sum_{C \in \mathscr{D}(k)} \deg(C)$, we finally conclude:

$$D(k) = D(d-m) \leq D(d-(m-1))R + D(d-(m-1)) = D(k+1)(R+1).$$

Applying the inductive hypothesis one concludes Inequality (3.6) and hence the proof of the Lemma. □

3.3.2. *The wanted proof of the second upper bound for the degree in Theorem 3.4.* We may assume that C_1 is a constructible set. If the result is true in the locally closed irreducible case, we can decompose C_1 as a finite union of locally closed irreducible sets as in Lemma 2.2:

$$C_1 := W_1 \cup \cdots \cup W_s,$$

that minimize the degree, i.e.:

$$\deg_{\mathrm{lci}}(C_1) := \sum_{i=1}^{s} \deg(W_i).$$

As the degree is sub-additive (see Proposition 2.16) and $\dim(C_1) = \max\{\dim(W_i) \ : \ 1 \leq i \leq s\}$, we would conclude the second upper bound from the case of locally closed irreducible sets by the following chain of inequalities:

$$\deg_{\mathrm{lci}}\left(C_1 \cap \left(\bigcap_{i=2}^{s} C_i\right)\right) \leq \sum_{i=1}^{s} \deg_{\mathrm{lci}}\left(W_i \cap \left(\bigcap_{i=2}^{s} C_i\right)\right) \leq$$

$$\leq \sum_{i=1}^{s} \deg\left(W_i\right)\left(1 + \sum_{i=1}^{s} \deg_{\mathrm{lci}}(C_i)\right)^{\dim(W_i)} \leq$$

$$\leq \left(\sum_{i=1}^{s} \deg(W_i)\right)\left(1 + \sum_{i=1}^{s} \deg_{\mathrm{lci}}(C_i)\right)^{\dim(C_1)} = \deg_{\mathrm{lci}}(C_1)\left(1 + \sum_{i=1}^{s} \deg_{\mathrm{lci}}(C_i)\right)^{\dim(C_1)},$$

which proves the Proposition for any constructible set C_1.

We denote by $d := \dim(C_1)$ the dimension of C_1 and we assume that C_1 is locally closed irreducible. We also consider for each constructible set C_i, $2 \leq i \leq s$, a decomposition according to Lemma 2.2:

$$C_i := W_{i,1} \cup \ldots \cup W_{i,s(i)},$$

where each $W_{i,j}$ is a Zariski open subset of an irreducible variety that we denote by $V_{i,j}$. Assume also that these decompositions minimize the degree of the C_i's, i.e.

$$\deg_{\mathrm{lci}}(C_i) := \sum_{i=1}^{s(i)} \deg(W_{i,j}) = \sum_{i=1}^{s(i)} \deg(V_{i,j}), \ 2 \leq i \leq s.$$

We now introduce classes of locally closed irreducible sets $\mathscr{V}_1, \ldots, \mathscr{V}_s$ given by the following identities:

$$\mathscr{V}_i := \{W_{i,1}, \ldots, W_{i,s(i)}\}, \ 2 \leq i \leq s.$$

We define the class $\mathscr{V}$ of locally closed sets:

$$\mathscr{V} := \{W \ : \ \forall i, \ 2 \leq i \leq s, \ \exists W_i \in \mathscr{V}_i, \ W = C_1 \cap \left(\bigcap_{i=2}^{s} W_i\right)\}.$$

And, finally, we define the class $\mathscr{C}$ of the irreducible algebraic varieties given by the following equality:

$$\mathscr{C} := \{C \ : \ C \text{ is irreducible}, \ \exists W \in \mathscr{V}, \text{ a non-empty open subset of } C \text{ is a component of } W\}.$$

For each $C \in \mathscr{C}$, let $U_C \subseteq \mathbb{A}^n$ be a Zariski open subset, maximal with the property $\emptyset \neq U_C \cap C \subseteq (C_1 \cap (\bigcap_{i=2}^{s} C_i))$.

Claim. *With these notations, we have:*

$$C_1 \cap \left(\bigcap_{i=2}^{s} C_i\right) = \bigcup_{C \in \mathscr{C}} U_C \cap C.$$

Proof of the Claim. For each $C \in \mathscr{C}$, there exists a Zariski open subset $U_0 \subseteq \mathbb{A}^n$ such that $U_0 \cap C \neq \emptyset$ and $U_0 \cap C$ is a locally closed irreducible component of a locally closed subset of the following form:

$$C_1 \cap (W_2 \cap \cdots \cap W_s),$$

where $W_i \in \mathscr{V}_i$. Thus, $U_0 \cap C \subseteq (C_1 \cap (\bigcap_{i=2}^{s} C_i))$ and, by the definition of U_C we conclude $U_C \cap C \subseteq (C_1 \cap (\bigcap_{i=2}^{s} C_i))$.

On the other hand, fix some point $x \in (C_1 \cap (\bigcap_{i=2}^{s} C_i))$. Since the equality

$$C_1 \cap \left(\bigcap_{i=2}^{s} C_i\right) = \bigcup_{(W_2, \ldots, W_s) \in \mathscr{V}_1 \times \cdots \times \mathscr{V}_s} C_1 \cap \left(\bigcap_{i=2}^{s} W_i\right),$$

holds, we conclude that there exist $W_2 \in \mathscr{V}_2, \ldots, W_s \in \mathscr{V}_s$ such that $x \in (C_1 \cap (\bigcap_{i=2}^{s} W_i))$. In particular, x must belong to some locally closed irreducible component of $(C_1 \cap (\bigcap_{i=1}^{s} W_i))$ and, hence, there must exist some $C \in \mathscr{C}$ such that $x \in U_C \cap C$. ∎

By Proposition 2.16 (*LCI*-degree is sub-additive), we conclude:

$$(3.7) \qquad \deg_{\mathrm{lci}}\left(C_1 \cap \left(\bigcap_{i=2}^{s} C_i\right)\right) \le \sum_{C \in \mathscr{C}} \deg(C).$$

Now we consider the family $\mathscr{W}$ of locally closed sets (as that of Lemma 3.5 above) given by the following identity:

$$\mathscr{W} := \{W \ : \ \exists S \subseteq \{2, \dots, s\}, \ \forall i \in S, \ \exists W_i \in \mathscr{V}_i, \ W = C_1 \cap \left(\bigcap_{i \in S} W_i\right)\}.$$

We also define a new family of irreducible varieties:

$$\mathscr{D} := \{C \ : \ C \text{ is irreducible and, } \exists W \in \mathscr{W}, \text{a non-empty open subset of } C \text{ is a component of } W\}.$$

Obviously $\mathscr{C} \subseteq \mathscr{D}$ and, because of Lemma 3.5, we conclude:

$$\sum_{C \in \mathscr{C}} \deg(C) \le \sum_{C \in \mathscr{D}} \deg(C) \le \deg(C_1)\left(1 + \sum_{i=2}^{s} \sum_{V \in \mathscr{V}_i} \deg(V)\right)^{\dim(C_1)}.$$

As we have $\deg_{\mathrm{lci}}(C_i) := \sum_{V \in \mathscr{V}_i} \deg(V)$, according to the Inequality (3.7) we finally conclude the second upper bound of Theorem 3.4:

$$\deg_{\mathrm{lci}}\left(\bigcap_{i=1}^{s} C_i\right) \le \deg(C_1)\left(1 + \sum_{i=2}^{s} \deg_{\mathrm{lci}}(C_i)\right)^{\dim(C_1)}.$$

3.4. A couple of immediate applications to show bounds for multiple intersections of constructible sets.

Example 3.6 (**Counting $\mathbb{F}_q$−rational points in constructible sets**). Let $\mathbb{F}_q$ be a finite field and $\overline{\mathbb{F}_q}$ be its algebraic closure. For each constructible subset $C \subseteq \mathbb{A}^n(\overline{\mathbb{F}_q})$, we denote by $C_{\mathbb{F}_q} := C \cap \mathbb{F}_q^n$ the set of its $\mathbb{F}_q$−rational points. The following generalizes to constructible sets a classical result for hyper-surfaces due to Ø. Ore (cf. [Ore, 22]).

Corollary 3.7. *With the above notations, for every constructible subset $C \subseteq \mathbb{A}^n(\overline{\mathbb{F}_q})$, the number of $\mathbb{F}_q$−rational points satisfies:*

$$\sharp\left(C_{\mathbb{F}_q}\right) = \sharp\left(C \cap \mathbb{F}_q^n\right) \le \deg_{\mathrm{lci}}(C) q^{\dim(C)}.$$

In particular, for every non-zero polynomial $f \in \overline{\mathbb{F}_q}[X_1, \dots, X_n]$, whose degree satisfies $\deg(f) \le q - 1$, there is some point $x \in \mathbb{F}_q^n$ such that $f(x) \ne 0$. Moreover, the number of non-zeros of f in $\mathbb{F}_q^n$ satisfies:

$$\sharp\{x \in \mathbb{F}_q^n \ : \ f(x) \ne 0\} \ge (q - \deg(V(f))) q^{n-1}.$$

Proof. Firstly, let us consider for every j, $1 \le j \le n$, the algebraic varieties:

$$W_j := \overline{\mathbb{F}_q}^{j-1} \times \{x_j \in \overline{\mathbb{F}_q} \ : \ x_j^q - x_j = 0\} \times \overline{\mathbb{F}_q}^{n-j} \subseteq \mathbb{A}^n(\overline{\mathbb{F}_q}).$$

Each $W_j \subseteq \mathbb{A}^n(\overline{\mathbb{F}_q})$ is a hyper-surface of degree q and we obviously have:

$$\mathbb{F}_q^n = \bigcap_{j=1}^{n} W_j.$$

As $W_1, \dots, W_n$ are algebraic varieties of degree at most q, from Proposition 3.1 we conclude:

$$\deg_{\mathrm{lci}}(C \cap \mathbb{F}_q^n) = \deg_{\mathrm{lci}}(C \cap \left(\bigcap_{j=1}^{n} W_j\right)) \le \deg_{\mathrm{lci}}(C) q^{\dim(C)}.$$

Since $C \cap \mathbb{F}_q^n$ is a zero-dimensional variety (see Proposition 2.9), we have:

$$\sharp\left(C_{\mathbb{F}_q}\right) = \sharp\left(C \cap \mathbb{F}_q^n\right) = \deg_{\mathrm{lci}}(C \cap \mathbb{F}_q^n).$$

As for the second claim, since $V(f)$ is a non-empty hyper-surface (of dimension $n-1$ in $\mathbb{A}(\overline{\mathbb{F}_q})$), Proposition 2.9 implies that the degree of $V(f)$ is at most $\deg(f)$. Therefore, we have:

$$\sharp\left(V(f) \cap \mathbb{F}_q^n\right) \le \deg(V(f)) q^{n-1} \le \deg(f) q^{n-1} \le (q-1) q^{n-1}.$$

Hence, we obviously conclude:

$$\sharp\{x \in \mathbb{F}_q^n \ : \ f(x) \neq 0\} \geq (q - \deg(V(f))q^{n-1}.$$

$\square$

The results of Weil, Lang and Stepanov (cf. [We,49], [LW, 54] and [St, 69]) show that the bound of the previous Corollary is essentially optimal if C is an algebraic variety.

Example 3.8 (**Evasive zero-dimensional varieties of constructible sets**).

Corollary 3.9. *Let κ be a field, $Q \subseteq \kappa$ a finite subset and K the algebraic closure of κ. Let $C \subseteq \mathbb{A}^n(K)$ be a constructible subset. Then, the number of points of the intersection of C and Q^n satisfies:*

$$\sharp(C \cap Q^n) \leq \deg_{\mathrm{lci}}(C)\sharp(Q)^{\dim(C)}.$$

In other terms, the probability that a random point $x \in Q^n$ satisfies $x \notin C$ is greater than

$$1 - \frac{\deg_{\mathrm{lci}}(C)}{\sharp(Q)^{\mathrm{codim}(C)}},$$

where $\mathrm{codim}(C) = n - \dim(C)$ is the co-dimension of C in $\mathbb{A}^n(K)$.

Proof. The proof is similar to that of the preceding Corollary by replacing $\mathbb{F}_q$ by Q, and replacing the equation of degree q that defines $\mathbb{F}_q$ in $\overline{\mathbb{F}_q}$ by an univariate polynomial of degree $\sharp(Q)$ whose zeros in K are exactly Q. In what concerns to the lower bound for the probability, it is a consequence of the following chain of inequalities:

$$\mathrm{Prob}_{Q^n}[x \in Q^n \ : \ x \notin C] \geq 1 - \frac{\deg_{\mathrm{lci}}(C)\sharp(Q)^{\dim(C)}}{\sharp(Q)^n} = 1 - \frac{\deg_{\mathrm{lci}}(C)}{\sharp(Q)^{\mathrm{codim}(C)}}.$$

$\square$

Observe that in the case $C = V(f)$, where C is a hyper-surface defined by a non-zero polynomial, this last Corollary is the foundation of the classical *Demillo-Lipton-Schwartz-Zippel Lemma* (cf. [DML, 78], [Zp, 79] and [Sch, 80]).

4. Correct Test Sequences

In this Section we revise the notion of correct test sequence (introduced in [HeSc, 82]) and see that it is almost omnipresent, by exhibiting its presence in many scientific contexts. We do not want to be exhaustive here, but to exhibit different equivalent terms in the mathematical literature. We also prove some elementary and immediate properties.

4.1. **The notion, some equivalent notions and first properties.**

Definition 7 (**Correct Test Sequences for vector functions**). *Let X be a set, K a field and let $\mathscr{F}(X) \subseteq K^X$ be a subgroup of the abelian group $(K^X, +)$. Let $m \in \mathbb{N}$ be a positive integer and let $\Omega \subseteq \mathscr{F}(X)^m$ be a set of lists of such functions. Let $\Sigma \subsetneq \Omega$ be a proper subset of Ω, which we call the discriminant.*
A correct test sequence (CTS) of length L for Ω with discriminant Σ is a finite set of L elements $\mathbf{Q} := \{x_1, \ldots, x_L\} \subseteq X$ such that the following formula holds:

$$(4.1) \qquad \forall f \in \Omega, \ f(x_1) = \cdots = f(x_L) = 0 \in K^m \Longrightarrow f \in \Sigma.$$

In the case $\Sigma = \{0\} \subsetneq \Omega$, we say that $\mathbf{Q}$ is a correct test sequence for Ω.

Given $\Omega \subseteq \mathscr{F}(X)^m$ we denote by $\Omega - \Omega$ the subset of $(\mathscr{F}(X)^m, +)$ given by the differences between elements in Ω. Namely,

$$\Omega - \Omega := \{f - g \ : \ f, g \in \Omega\} \subseteq \mathscr{F}(X)^m.$$

Observe that if Ω is a semi-group in $(\mathscr{F}(X)^m, +)$, then $\Omega - \Omega$ is simply the abelian subgroup of $(\mathscr{F}(X)^m, +)$ generated by Ω.
For a list of points $\mathbf{Q} := \{x_1, \ldots, x_L\}$ we define the evaluation map at the points of $\mathbf{Q}$ as the mapping:

$$\mathrm{ev}_{\mathbf{Q}} : \quad \begin{matrix} \mathscr{F}(X)^m & \longrightarrow & K^{mL} \\ (f_1, \ldots, f_m) & \longmapsto & (f_1(x_1), \ldots, f_m(x_1), \ldots, f_1(x_L), \ldots, f_m(x_L)), \end{matrix}$$

which is a $K-$linear mapping when $\mathscr{F}(X)^m$ is a vector subspace of $(K^m)^X$.

Proposition 4.1 (**CTS and Function Identity Tests**). *With the notations of the previous definition, let Ω be a subset of $\mathscr{F}(X)^m$. Then, the following properties are equivalent for every finite subset $\mathbf{Q} := \{x_1, \ldots, x_L\} \subseteq X$:*

   i) $\mathbf{Q}$ *is a correct test sequence for $\Omega - \Omega$ (with respect to $\Sigma := \{0\}$).*
   ii) *The following formula holds:*

$$\forall f, g \in \Omega, \;\; f(x_1) = g(x_1), \ldots, f(x_L) = g(x_L) \Longrightarrow f = g.$$

If, additionally, $\mathscr{F}(X)^m$ is a vector subspace of $(K^m)^X$, both properties are equivalent to the following ones:

   iii) *The evaluation map* $\mathrm{ev}_{\mathbf{Q}}$ *at the points in $\mathbf{Q}$ is a $K-$linear mapping such that its restriction to Ω is injective.*
   iv) *If $L := \sharp(\mathbf{Q})$, there is a linear map $\Lambda : K^{mL} \longrightarrow \mathscr{F}(X)^m$ such that the following two properties hold:*
      (a) *For all $f \in \mathscr{F}(X)^m$, $f - \Lambda(\mathrm{ev}_{\mathbf{Q}}(f)) \in \ker(\mathrm{ev}_{\mathbf{Q}})$ and,*
      (b) $\mathrm{ev}_{\mathbf{Q}}(\Omega) \cap \ker(\Lambda) = \{0\}$.

Proof. The equivalences between $i)$, $ii)$ and, in the case $\mathscr{F}(X)$ is a vector space, with $iii)$ are immediate. As for the equivalence between $iii)$ and $iv)$ simply assume that Λ is some extension to K^{mL} of the right inverse of the epimorphism between $\mathscr{F}(X)^m$ and $\mathrm{ev}_{\mathbf{Q}}(\mathscr{F}(X)^m) \subseteq K^{mL}$. $\square$

Correct test sequences viewed as identity tests is the most common interpretation in the mathematical literature. When $\mathscr{F}(X)$ is a group of polynomials defined on some algebraic variety X, correct test sequences are called *Polynomial Identity Tests* (as in [Sax, 14] and references therein). These Polynomial Identity Tests have been used in Elimination Theory for years to compute Noether's normalizations, Kronecker's birational descriptions of equi-dimensional varieties and for many other purposes (see, for instance, [GHHMMP, 97], [GHMP, 97], [Pa, 95] and references therein). We return to this polynomial case in the next subsection.

With the same notations as above, assume that $\mathscr{F}(X)$ is a $K-$algebra. Then, for every $x \in X$, the following is a maximal ideal in $\mathscr{F}(X)$:

$$\mathfrak{m}_x := \{f \in \mathscr{F}(X) \; : \; f(x) = 0\} \in \mathrm{MaxSpec}(\mathscr{F}(X)).$$

In fact, $\mathfrak{m}_x$ is the kernel of the onto map $\mathrm{ev}_x : \mathscr{F}(X) \longrightarrow K$ given by $\mathrm{ev}_x(f) := f(x)$, for all $f \in \mathscr{F}(X)$. For every $\mathbf{Q} \subseteq X$ let us denote by $I(\mathbf{Q})$ the radical ideal given by the following identity:

$$I(\mathbf{Q}) := \bigcap_{x \in \mathbf{Q}} \mathfrak{m}_x.$$

Proposition 4.2. *With the same notations as above, assume $\mathscr{F}(X)$ is a $K-$algebra and $\Omega \subseteq \mathscr{F}(X)$ a subset. The following properties are equivalent:*

   i) *A finite subset $\mathbf{Q} \subseteq X$ is a correct test sequence for $\Omega - \Omega$.*
   ii) *The canonical projection $\pi : \mathscr{F}(X) \longrightarrow \mathscr{F}(\mathbf{Q}) := \mathscr{F}(X)/I(\mathbf{Q})$ satisfies that its restriction $\Omega\big|_{\mathbf{Q}}$ is injective.*
   iii) *There is a $K-$vector subspace $W(\mathbf{Q})$ of $\mathscr{F}(X)$ of dimension $\sharp(\mathbf{Q})$ such that the following properties hold:*
      • *For every $f \in \Omega$ there is one and only one $g \in W(\mathbf{Q})$ such that $f - g \in I(\mathbf{Q})$.*
      • *For every $g \in W(\mathbf{Q})$ there is at most one $f \in \Omega$ such that $f - g \in I(\mathbf{Q})$.*

Proof. By the Chinese Remainder Theorem, we have the following ring isomorphism:

$$\varphi : \mathscr{F}(X)/I(\mathbf{Q}) \longrightarrow \prod_{i=1}^{L} \mathscr{F}(X)/\mathfrak{m}_{x_i} \cong K^L,$$

where $\mathbf{Q} := \{x_1, \ldots, x_L\}$. Noting that:

$$\varphi(f + I(\mathbf{Q})) := (f + \mathfrak{m}_{x_1}, \ldots, f + \mathfrak{m}_{x_L}),$$

we obviously conclude the equivalence between $i)$ and $ii)$. Moreover, the Chinese Remainder Theorem means that there is interpolation in $\mathscr{F}(X)$. Namely, there are functions $\chi_1, \ldots, \chi_L \in \mathscr{F}(X)$ such that $\chi_i(x_j) = \delta_{i,j}$, for every i, j, $1 \leq i, j \leq L$, where $\delta_{i,j}$ is Kronecker's delta.

Then, taking $W(\mathbf{Q}) := \mathrm{Span}(\{\chi_1, \ldots, \chi_L\})$, the $K-$vector space spanned by $\{\chi_1, \ldots, \chi_L\}$, we obviously have that for every $f \in \Omega$, the function

$$g := \sum_{i=1}^{L} f(x_i)\chi_i \in W(\mathbf{Q}),$$

satisfies the requirements of the statement. Moreover, given any $g \in W(\mathbf{Q})$ there is at most one element $f \in \Omega$ such that $f - g \in I(\mathbf{Q})$. □

Example 4.3 (**Finite Norming sets**). With the same notations as above, assume that $(K, |\cdot|)$ is a field with some absolute value. And for any positive integer $m \in \mathbb{N}$, let $||\cdot||$ be any norm in K^m induced by $|\cdot|$. Assume that $\mathscr{F}(X)$ is a $K-$vector space and $\Omega \subseteq \mathscr{F}(X)$ is a subset, a *finite norming set* for Ω is a finite subset $\mathbf{Q} := \{x_1, \ldots, x_L\} \subseteq X$ such that the following is a norm in Ω:

$$||f||_\infty^{(\mathbf{Q})} := \max\{|f(x_i)| \ : \ 1 \le i \le L\}.$$

As Ω is not always a vector subspace, we use the term "norm" in a wide sense here. Just for completeness, a norm for Ω is a function $||\cdot|| : \Omega \longrightarrow \mathbb{R}_+$ such that the following properties hold:

- $||f|| \ge 0$, $\forall f \in \Omega$.
- For all $f \in \Omega$, $||f|| = 0$ if and only if $f = 0$.
- Given $f, g \in \Omega$, if $f + g \in \Omega$, then we have

$$||f + g|| \le ||f|| + ||g||.$$

- Given $f \in \Omega$ and $\lambda \in K$, if $\lambda f \in \Omega$, then $||\lambda f|| \le |\lambda|||f||$.

Obviously, if Ω is a vector subspace, this is the usual notion of norm. See [AK, 06] and references therein for the term *norming set*.

Proposition 4.4. *With the same notations and assumptions as in the former example, given* $\mathbf{Q} := \{x_1, \ldots, x_L\} \subseteq X$ *a finite set and* $\Omega \subseteq \mathscr{F}(X)$ *a subgroup of the additive group* $(\mathscr{F}(X), +)$, *the following are equivalent:*

   i) The set $\mathbf{Q}$ *is a correct test sequence for* Ω.
   ii) The set $\mathbf{Q}$ *is a finite norming set for* Ω.
   iii) The restriction to the evaluation map $\mathrm{ev}_\mathbf{Q}$ *to* Ω *is a group monomorphism.*
   iv) There exists p, $1 \le p \le \infty$, *such that the following is a norm on* Ω:

$$||f||_p^{(\mathbf{Q})} := \left(\sum_{i=1}^{L} |f(x_i)|^p\right)^{1/p}.$$

   v) For every p, $1 \le p \le \infty$, *the following is a norm on* Ω:

$$||f||_p^{(\mathbf{Q})} := \left(\sum_{i=1}^{L} |f(x_i)|^p\right)^{1/p}.$$

   vi) Ω *is a metric space with the distance function:*

$$d_\infty^{(\mathbf{Q})}(f, g) := ||f - g||_\infty^{(\mathbf{Q})}.$$

   vii) For every p, $1 \le p \le \infty$, Ω *is a metric space with the distance function:*

$$d_p^{(\mathbf{Q})}(f, g) := ||f - g||_p^{(\mathbf{Q})}.$$

In particular, Ω *has a finite length correct test sequence if and only if it admits a finite norming set. If, additionally,* Ω *were a linear subspace of* $\mathscr{F}(X)$, *then* Ω *admits a correct test sequence of finite length if and only if* Ω *is a normed linear space of finite dimension.*

Proof. It is obvious from the definitions. □

The interesting cases are then restricted to subsets (not necessarily linear) of some finite dimension vector spaces.

Example 4.5 (**CTS's and the ring of continuous functions**). Assume X is a compact topological space, $\kappa = \mathbb{R}$ and $\mathscr{F}(X) \subseteq \mathscr{C}(X)$ is a vector subspace of the $\mathbb{R}-$algebra of continuous functions defined on X with values in $\mathbb{R}$. Assume that $\mathscr{C}(X)$ is endowed with the topology defined by the maximum norm, which is a Banach $\mathbb{R}-$algebra. Because of the Theorem of Banach-Stone-Čech-Gel'fand-Kolmogorov (cf. [GHJ, 54]), we know that there exists a bijection between the maximal ideals in the spectrum of $\mathscr{C}(X)$ (which we denote by $\mathrm{MaxSpec}(\mathscr{C}(X))$) and the set of points in X. This bijection is given by the following identification:

$$x \longmapsto \mathfrak{m}_x := \{f \in \mathscr{C}(X) \ : \ f(x) = 0\}.$$

With these notations and assumptions, a finite subset $\mathbf{Q} := \{x_1, \ldots, x_L\} \subseteq X$ of cardinality L is a correct test sequence for $\Omega \subseteq \mathscr{F}(X)$ with respect to a discriminant $\Sigma \subsetneq \Omega$ if and only if the following holds:

$$\Omega \cap \left(\bigcap_{i=1}^{L} \mathfrak{m}_{x_i} \right) \subseteq \Sigma,$$

or, equivalently, if and only if the following is true:

$$\Omega \setminus \Sigma \subseteq \left(\bigcup_{i=1}^{L} \mathfrak{m}_{x_i}^c \right),$$

where $\mathfrak{m}_{x_i}^c = \mathscr{C}(X) \setminus \mathfrak{m}_{x_i}$.

Proposition 4.6. *With the same notations as above, assume that X is a compact Hausdorff space, $\mathscr{F}(X) = \mathscr{C}(X)$, $\Omega \subseteq \mathscr{C}(X)$ and $\Sigma \subsetneq \Omega$. Let (Σ) be the ideal in $\mathscr{C}(X)$ generated by Σ and assume that:*

(4.2) $$\sqrt[J]{(\Sigma)} \cap \Omega = \Sigma,$$

where $\sqrt[J]{\cdot}$ means Jacobson radical. Then, if $\Omega \setminus \Sigma$ is quasi-compact in $\mathscr{C}(X)$ (i.e. every open covering has a finite sub-covering), then there is a finite length correct test sequence for Ω with respect to Σ.

In particular, if $\Sigma = \{0\}$ and $\Omega \setminus \{0\}$ is quasi-compact, then there is a correct test sequence of finite length for Ω or, equivalently, Ω has a finite norming set.

Proof. From Banach-Stone-Čech-Gel'fand-Kolmogorov Theorem, as X is compact and Hausdorff, we know that there is an identification:

$$X \cong \mathrm{MaxSpec}(\mathscr{C}(X)).$$

Let us also consider the following closed subset of X:

$$V(\Sigma) = \{x \in X \ : \ f(x) = 0, \ \forall f \in \Sigma\} = \{x \in X \ : \ f(x) = 0, \ \forall f \in (\Sigma)\}.$$

Then, the following equalities hold:

$$\sqrt[J]{(\Sigma)} = \bigcap_{\substack{\mathfrak{m} \in \mathrm{MaxSpec}(\mathscr{C}(X)) \\ \mathfrak{m} \supseteq \Sigma}} \mathfrak{m} = \bigcap_{x \in V(\Sigma)} \mathfrak{m}_x.$$

The first equality is simply the definition of Jacobson radical of an ideal. As for the second, we obviously have:

$$\bigcap_{\substack{\mathfrak{m} \in \mathrm{MaxSpec}(\mathscr{C}(X)) \\ \mathfrak{m} \supseteq \Sigma}} \mathfrak{m} \subseteq \bigcap_{x \in V(\Sigma)} \mathfrak{m}_x.$$

Conversely, let $\mathfrak{m}$ be a maximal ideal in $\mathscr{C}(X)$ that contains Σ. Then, there is some $x \in X$ such that $\mathfrak{m} = \mathfrak{m}_x$. As $\mathfrak{m}_x \supseteq \Sigma$, then $f(x) = 0$ for all $f \in \Sigma$ and, hence, $x \in V(\Sigma)$. This implies the converse inclusion. Thus, our hypothesis implies that:

$$\sqrt[J]{(\Sigma)} \cap \Omega = \left(\bigcap_{x \in V(\Sigma)} \mathfrak{m}_x \right) \cap \Omega = \Sigma.$$

Thus,

$$\Omega \setminus \Sigma \subseteq \bigcup_{x \in V(\Sigma)} \mathfrak{m}_x^c.$$

As $\mathfrak{m}_x^c$ is open in $\mathscr{C}(X)$, we have an open covering of $\Omega \backslash \Sigma$, which is quasi-compact by hypothesis. Then, there is a finite sub-covering:

$$\Omega \setminus \Sigma \subseteq \bigcup_{i=1}^{L} \mathfrak{m}_{x_i}^c,$$

for some finite subset $\mathbf{Q} := \{x_1, \ldots, x_L\}$. But this last inclusion just means that $\mathbf{Q}$ is a correct test sequence of length L for Ω with respect to Σ, and the first claim of our statement holds. The particular case holds simply because $V(\{0\}) = X$ and $\sqrt[j]{(0)} = \{0\}$.   □

Similarly, we also have:

Corollary 4.7. *Let $r \in \mathbb{N} \cup \{\infty\}$ be a positive integer or ∞. Let X be a compact $\mathscr{C}^r-$ manifold. Then, for every $\Omega \subseteq \mathscr{C}^r(X)$ such that $0 \in \Omega$, if $\Omega \setminus \{0\}$ is quasi-compact, then there is a correct test sequence for Ω of finite length or, equivalently, Ω has a finite norming set.*

Proof. Essentially the same proof after observing that:

$$\mathrm{MaxSpec}(\mathscr{C}^r(X)) \cong X.$$

□

Note that the hypothesis described in Identity (4.2) may be rewritten as:

$$\overline{(\Sigma)} \cap \Omega \subseteq \Sigma,$$

where $\overline{(\Sigma)} = \sqrt[j]{(\Sigma)}$ is the closure of the ideal (Σ) in $\mathscr{C}(X)$ with respect to the Hewitt $m-$topology (cf. [GHJ, 54] and [Hew, 48]).

A typical example where the hypothesis "$\Omega \setminus \Sigma$ *is quasi-compact*" holds is the case where Σ is closed in Ω for the topology induced by that of $\mathscr{F}(X)$ and Ω is a Noetherian topological space. Inspired by the case of continuous functions, we introduce the following notion:

Definition 8 (**CTS covering numbers**). *With the same notations as above, the covering number for $\Omega \subseteq \mathscr{F}(X)$ with respect to Σ is the minimum length of a finite correct test sequence for Ω with respect to Σ. We denote this quantity by:*

$\mathscr{N}_{\mathrm{cts}}(\Omega, \Sigma) := \min\{L \in \mathbb{N} \ : \ \exists \text{ a correct test sequence } \mathbf{Q} \text{ of length } L \text{ for } \Omega \text{ with respect to } \Sigma\}.$

We denote by $\mathscr{N}_{\mathrm{cts}}(\Omega) := \mathscr{N}_{\mathrm{cts}}(\Omega, \{0\})$.

Example 4.8 (**Correct Test Sequences in Reproducing Kernel Hilbert spaces**). Let $K : X \times X \longrightarrow \mathbb{C}$ be a kernel and let $(\mathscr{H}_K, \langle \cdot, \cdot \rangle_K)$ be its associated Hilbert space. Recall that $\mathscr{H}_K \subseteq \mathbb{C}^X$ and, in the case that X is a metric space and that K is a Mercer kernel, $\mathscr{H}_K \subseteq \mathscr{C}(X, \mathbb{C}) \cong \mathscr{C}(X)[i] := \mathscr{C}(X)[T]/(T^2 + 1)$ is made by continuous functions with complex values. For every $x \in X$, let $K_x : X \longrightarrow \mathbb{C}$ be the element in $\mathscr{H}_K$ given by:

$$K_x(y) := K(x, y), \ \forall y \in X.$$

Then, it is well-known that for every $f \in \mathscr{H}_K$ and for every $x \in X$, the following equality holds:

$$f(x) = \langle f, K_x \rangle.$$

Proposition 4.9. *With these last notations, let $\Omega \subseteq \mathscr{H}_K$ be a subset and let $\Sigma \subsetneq \Omega$ be a discriminant. A finite subset of points $\mathbf{Q} = \{x_1, \ldots, x_L\} \subseteq X$ is a correct test sequence of length L for Ω with respect to Σ if and only if:*

$$\Omega \cap (\mathrm{Span}(\{K_{x_1}, \ldots, K_{x_L}\}))^{\perp} \subseteq \Sigma,$$

where $\mathrm{Span}(\{K_{x_1}, \ldots, K_{x_L}\})$ is the vector subspace of $\mathscr{H}_K$ generated by $\{K_{x_1}, \ldots, K_{x_L}\}$ and $^{\perp}$ means orthogonal complement in $\mathscr{H}_K$.

Proof. Note that this is simply another way to express Identity (4.1).   □

Observe also that the condition of being a correct test sequence is hereditary. Namely, we obviously have the following statement:

Proposition 4.10. *Let $\Omega \subseteq \widetilde{\Omega} \subseteq \mathscr{F}(X)^m$ be two subsets and let $\Sigma \subsetneq \widetilde{\Omega}$ be a discriminant. Let $\mathbf{Q} \subseteq X$ be a correct test sequence for $\widetilde{\Omega}$ with respect to Σ. Then, $\mathbf{Q}$ is a correct test sequence for Ω with respect to $\Sigma \cap \Omega$.*

4.2. **The case of polynomials and lists of polynomials.** For every positive number $d \in \mathbb{N}$ we denote by $P_d^K(X_1, \ldots, X_n)$ the class of all polynomials of degree at most d with coefficients in K in the set of variables $\{X_1, \ldots, X_n\}$ (when both the field K and the set of variables $\{X_1, \ldots, X_n\}$ are clear from the context we simply write P_d). For a list of degrees $(d) := (d_1, \ldots, d_m)$, with $m \leq n$, we introduce the class $\mathscr{P}_{(d)}^K(X_1, \ldots, X_n)$ of all lists of polynomials $f := (f_1, \ldots, f_m)$ such that each $f_i \in P_{d_i}^K$. Namely, $\mathscr{P}_{(d)}^K$ is the Cartesian product:

$$\mathscr{P}_{(d)}^K(X_1, \ldots, X_n) := \prod_{i=1}^m P_{d_i}^K(X_1, \ldots, X_n).$$

If both K and the set of variables are clear from the context, we write $\mathscr{P}_{(d)}$.
Obviously, $\mathscr{P}_{(d)}$ is a finite dimension affine space over K. We denote by $N_{(d)}$ this dimension, which is given by the following identity:

$$N_{(d)} := \sum_{i=1}^m \binom{d_i + n}{n}.$$

In [HeSc, 82], the authors considered correct test sequences for a constructible subset $\Omega \subseteq P_d$ with respect to $\{0\}$ as discriminant. Here, we also consider constructible sets $\Omega \subseteq \mathscr{P}_{(d)}$.
For every constructible set $\Omega \subseteq \mathscr{P}_{(d)}$ and for every point $x \in \mathbb{A}^n$ we denote by $\Omega_x \subseteq \mathbb{A}^n$ the following constructible subset:

$$\Omega_x := \Omega \cap \{f \in \mathscr{P}_{(d)} \ : \ f(x) = 0\}.$$

Thus, we may also rewrite the notion of correct test sequence as a list $\mathbf{Q} := (x_1, \ldots, x_L) \in V^L$, where $V \subset \mathbb{A}^n$, of points such that:

$$\Omega_{x_1} \cap \cdots \cap \Omega_{x_L} \subseteq \Sigma.$$

Proposition 4.11. *Let* $\mathbf{Q} = \{x_1, \ldots, x_L\}$ *be a correct test sequence of* Ω *with respect to* Σ. *Then, we have:*

$$\deg_{\mathrm{lci}}(\Omega_{x_1} \cap \cdots \cap \Omega_{x_L}) \leq \deg_{\mathrm{lci}}(\Omega).$$

Moreover, if Σ *is zero-dimensional, the intersection* $\Omega_{x_1} \cap \cdots \cap \Omega_{x_L}$ *is a finite set and we have:*

$$\sharp(\Omega_{x_1} \cap \cdots \cap \Omega_{x_L}) \leq \deg_{\mathrm{lci}}(\Omega).$$

In particular, if $\deg_{\mathrm{lci}}(\Sigma) > \deg_{\mathrm{lci}}(\Omega)$, *we have an strict inclusion:*

$$\Omega_{x_1} \cap \cdots \cap \Omega_{x_L} \subsetneq \Sigma.$$

Proof. Observe that for every point $x \in \mathbb{A}^n$, the set Ω_x is the intersection of Ω with a linear affine variety. Then, all the claims are immediate consequences of Proposition 2.27. □

The following Proposition shows the limits of length of correct test sequences in terms of the Krull dimension of the given constructible set:

Proposition 4.12. *With the same notations as above, let* $\Omega \subseteq \mathscr{P}_{(d)}$ *be a constructible subset,* $\Sigma \subseteq \Omega$ *be a discriminant in* Ω *and* $\mathbf{Q} \in V^L$ *be a correct test sequence of length* L *for* Ω *with respect to* Σ. *Then, we have:*

$$\sharp(\mathbf{Q}) = L \geq \mathrm{codim}_\Omega(\Sigma) = \dim(\Omega) - \dim(\Sigma).$$

In particular, the CTS covering number satisfies:

$$\mathscr{N}_{\mathrm{cts}}(\Omega, \Sigma) \geq \dim(\Omega) - \dim(\Sigma).$$

Proof. The intersection $\Omega_{x_1} \cap \cdots \cap \Omega_{x_L}$ is the intersection of Ω with a sequence of L linear equations whose variables are the coefficients of the elements in $\mathscr{P}_{(d)}$. Then, by Krull's Hauptidealsatz, the dimension of this intersection satisfies:

$$\dim(\Omega \cap \{f \in \mathscr{P}_{(d)} \ : \ f(x_1) = 0\} \cap \cdots \cap \{f \in \mathscr{P}_{(d)} \ : \ f(x_L) = 0\}) \geq \dim(\Omega) - L.$$

However, if $\mathbf{Q} := (x_1, \ldots, x_L)$ is a correct test sequence for Ω with respect to Σ, we also have:

$$\Omega \cap \{f \in \mathscr{P}_{(d)} \ : \ f(x_1) = 0\} \cap \cdots \cap \{f \in \mathscr{P}_{(d)} \ : \ f(x_L) = 0\} \subseteq \Sigma.$$

Hence, we conclude the Proposition since we have:

$$\dim(\Omega) - L \leq \dim(\Sigma).$$

□

From this statement, we will say that *a correct test sequence for* Ω *is of optimal length* if its length is in $O(\dim(\Omega))$.

5. HIGH PROBABILITY OF EXISTENCE OF SHORT CORRECT TEST SEQUENCES IN EQUI-DIMENSIONAL LOCALLY CLOSED SETS FOR CONSTRUCTIBLE SETS OF LISTS OF POLYNOMIALS

With the same notations as in previous sections, let $\Omega \subseteq \mathscr{P}_{(d)}^K$ be a constructible set of polynomials with $(d) = (d_1, \ldots, d_m)$, $m \leq n$. We generalize the main probability outcome of [HeSc, 82] by showing that the "grid" requirement is not a must and that we may find (with high probability) correct test sequences in many locally closed sets of accurate dimension and degree. Additionally, we see that correct test sequences are well-suited not only for zero tests but also to decide membership to proper subvarieties of Ω.

As in Subsection 2.2, given $n, r \in \mathbb{N}$ two positive integers such that $r \leq n$, we consider the "Grassmannian" $\mathbb{G}(n, r)$ of all linear affine varieties in $\mathbb{A}^n$ of co-dimension r. We assume that $\mathbb{G}(n, r)$ is endowed with its Zariski topology as introduced in Subsection 2.2.

Let $\Sigma \subseteq \Omega$ be a constructible subset of co-dimension at least 1. Let $C \subseteq \mathbb{A}^n$ be a constructible subset and $L \geq 0$ a positive integer. We denote by $R(\Omega, \Sigma, C, L)$ the constructible set of all sequences $\mathbf{Q} \in C^L$ of length L which are correct test sequences for Ω with respect to Σ.

We have added an hypothesis (Hypothesis (5.1)) on the dimension of the varieties defined by lists of polynomials in $\Omega \setminus \Sigma$. Observe that this simply generalizes the case of $\Sigma = \{0\}$ and explains that the main subject in correct test sequences is *dimension* and not only zero tests. For locally closed sets $C \subseteq \mathbb{A}^n$ we just denote by $\deg(C)$ the degree of C, as discussed in previous sections.

Theorem 5.1. *Let $m, n \in \mathbb{N}$ be two positive integers, with $m \leq n$, and let $(d) := (d_1, \ldots, d_m)$ be a list of degrees and $d := \max\{d_1, \ldots, d_m\}$. Let $\Sigma \subseteq \Omega$ be two constructible subsets of $\mathscr{P}_{(d)}^K$ such that Σ has co-dimension at least 1 in Ω. Assume that $\Omega \setminus \Sigma$ satisfies the following property:*

$$(5.1) \qquad \forall f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma, \ \dim(V_{\mathbb{A}}(f_1, \ldots, f_m)) = n - m.$$

Let $C \subseteq \mathbb{A}^n$ be an equi-dimensional locally closed set of co-dimension $r \geq (n - m) + m/2 + 1/2$. Assume that there are locally closed subsets $C_1, \ldots, C_s \subseteq \mathbb{A}^n$ such that $C := C_1 \cap \ldots \cap C_s$. Let $D := \max\{\deg(C_1), \ldots, \deg(C_s)\} \geq 1$ be the maximum of their degrees. Let $L \in \mathbb{N}$ be a positive integer and assume that the following properties hold:

i) $L \geq 6 \dim(\Omega)$,
ii) $\log(\deg(C)) \geq r \max\{2(1 + \log(d + 1)), \frac{2\log(\deg_{\mathrm{lci}}(\Omega))}{\dim(\Omega)}\}$,
iii) $D \leq (1 + \frac{1}{n-m}) \deg(C)^{\frac{1}{\mathrm{codim}(C)}}$,

where $\log$ *stands for the natural logarithm. Then, there is a non-empty Zariski open subset $\mathbb{G}(C) \subseteq \mathbb{G}(n, n - r)$ such that for every $A \in \mathbb{G}(C)$, the probability that a randomly chosen list $\mathbf{Q} \in (C \cap A)^L$ is in $R := R(\Omega, \Sigma, C, L)$ satisfies:*

$$\mathrm{Prob}_{(C \cap A)^L}[R] \geq 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega) e^{\dim(\Omega) + (m-1)L}},$$

where $(A \cap C)^L$ is endowed with its uniform probability distribution.

Proof. First of all, let us denote by δ the following quantity:

$$\delta := \deg(C)^{\frac{1}{\mathrm{codim}(C))}}.$$

We obviously have $\deg(C) := \delta^r$ and our hypothesis yield the following inequalities:

- $\log(\delta) \geq \max\{2(1 + \log(d + 1)), \frac{2\log(\deg_{\mathrm{lci}}(\Omega))}{\dim(\Omega)}\}$,
- $D \leq (1 + \frac{1}{n-m})\delta$.

Then, we introduce the following incidence constructible set:

$$V(\Omega, L) := \{(f, x_1, \ldots, x_L) \in \Omega \times (\mathbb{A}^n)^L \ : \ f = (f_1, \ldots, f_m) \in \mathscr{P}_{(d)}^K, \ f_i(x_j) = 0, 1 \leq i \leq m, 1 \leq j \leq L\}.$$

We also consider the following two canonical projections:

- The projection onto the set of lists of consistent equations: $\pi_1 : V(\Omega, L) \longrightarrow \Omega$.
- The projection onto the possible zeros: $\pi_2 : V(\Omega) \longrightarrow (\mathbb{A}^n)^L$.

By the Bézout's Inequality for constructible sets (Theorem 2.28), we have:

$$\deg_{\mathrm{lci}}(V(\Omega, L)) \leq \deg_{\mathrm{lci}}(\Omega) \left(\prod_{i=1}^{m} (d_i + 1) \right)^L.$$

Let $\mathscr{D}$ be the class formed by locally closed irreducible sets $W_1, \ldots, W_M$ such that:

$$V(\Omega, L) = W_1 \cup \cdots \cup W_M,$$

and they are minimal with respect to the degree of $V(\Omega)$:

$$\deg_{\mathrm{lci}}(V(\Omega, L)) = \sum_{i=1}^{M} \deg(W_i).$$

Let $\mathscr{C} \subseteq \mathscr{D}$ be the class of those locally closed irreducible components of $V(\Omega, L)$ such that its projection by π_1 is not completely included in Σ:

$$\mathscr{C} := \{W \in \mathscr{D} \ : \ \pi_1(W) \setminus \Sigma \neq \emptyset\}.$$

As π_1 is the restriction of a projection, for all $W \in \mathscr{C}$, we may consider the following mapping:

$$\pi_1\big|_{\overline{W}^z} := \overline{W}^z \longrightarrow \overline{\pi_1(W)}^z.$$

It is a dominant morphism between two irreducible algebraic varieties. Then, by the Theorem on the Dimension of the Fibers (cf. [Sha, 77], Theorem 7, p. 60), for all $f \in \pi_1(W)$ we have:

$$(5.2) \qquad \dim\left(\pi_1\big|_{\overline{W}^z}^{-1}(\{f\})\right) \geq \dim(\overline{W}^z) - \dim(\overline{\pi_1(W)}^z) \geq \dim(W) - \dim(\Omega).$$

Observe that for every $f \in \pi_1(W)$ the following equality holds:

$$\pi_1\big|_{\overline{W}^z}^{-1}(\{f\}) = \{f\} \times (V_{\mathbb{A}}(f))^L.$$

Next, for every $W \in \mathscr{C}$, there is some system of equations $f \in \pi_1(W) \setminus \Sigma$ and, hence, we have:

$$\dim\left(\pi_1\big|_{\overline{W}^z}^{-1}(\{f\})\right) = (n - m)L,$$

And Inequality (5.2) becomes for every $W \in \mathscr{C}$:

$$(5.3) \qquad\qquad\qquad \dim(W) \leq \dim(\Omega) + (n - m)L.$$

Let us now define the constructible set:

$$B(\Omega, L) := \bigcup_{W \in \mathscr{C}} W \subseteq V(\Omega, L).$$

We have:

- $\dim(B(\Omega, L)) = \max\{\dim(W) \ : \ W \in \mathscr{C}\} \leq (n - m)L + \dim(\Omega)$ and,
- we also have:

$$\deg_{\mathrm{lci}}(B(\Omega, L)) \leq \deg_{\mathrm{lci}}(\Omega) \left(\prod_{i=1}^{m} (d_i + 1) \right)^L \leq \deg_{\mathrm{lci}}(\Omega)\, (d + 1)^{mL},$$

  where $d := \max\{d_1, \ldots, d_m\}$.

Now, as in Corollaries 2.23 and 2.24, there is a non-empty Zariski open subset $\mathbb{G}(C) \subseteq \mathbb{G}(n, n-r)$ such that for all $A \in \mathbb{G}(C)$ we have $\sharp(C \cap A) = \deg(C)$. Let us now consider $A \in \mathbb{G}(C)$ and the following constructible set:

$$\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L.$$

From Proposition 2.25 we conclude:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z\right) \leq \deg_{\mathrm{lci}}(B(\Omega, L)) \leq \deg_{\mathrm{lci}}(\Omega)(d + 1)^{mL}.$$

Next, as $C := C_1 \cap \cdots \cap C_s$ we may define the locally closed sets:

$$C_{i,j} := \mathbb{A}^{n(j-1)} \times C_i \times \mathbb{A}^{n(L-j)},$$

whose degree equals $\deg(C_i)$. We also define the class of linear affine varieties A_j, $1 \leq j \leq L$, of degree 1, given by:

$$A_j := \mathbb{A}^{n(j-1)} \times A \times \mathbb{A}^{n(L-j)},$$

Then, we have:

$$\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L = \overline{\pi_2(B(\Omega, L))}^z \cap \left(\bigcap_{i,j} C_{i,j} \right) \cap \left(\bigcap_{j=1}^{L} A_j \right).$$

From Proposition 3.1 we also conclude:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right) \leq \deg_{\mathrm{lci}}(B(\Omega, L)) D^{\dim(\pi_2(B(\Omega,L)))},$$

where, as $\deg(A_j) = 1$, we have:

$$1 \leq \max\{\deg(C_{i,j}) \ : \ 1 \leq i \leq s, \ 1 \leq j \leq L\} = D = \max\{\deg(C_i) \ : \ 1 \leq i \leq s\}.$$

Putting all together, as $\dim(\pi_2(B(\Omega, L))) \leq \dim(B(\Omega, L))$ we get:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right) \leq \deg_{\mathrm{lci}}(\Omega)(d+1)^{mL} D^{\dim(\Omega)+(n-m)L}.$$

This yields:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right) \leq \deg_{\mathrm{lci}}(\Omega) D^{\dim(\Omega)} D^{(n-m)L}(d+1)^{mL}.$$

As $\delta \geq e^2(d+1)^2$, we have:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right) \leq \deg_{\mathrm{lci}}(\Omega) D^{\dim(\Omega)} D^{(n-m)L} \left(\frac{\delta}{e^2} \right)^{\frac{m}{2}L}.$$

Then, we obtain:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right)}{\deg(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega) D^{\dim(\Omega)} D^{(n-m)L} \delta^{\frac{m}{2}L}}{e^{mL} \delta^{\mathrm{codim}(C)L}}.$$

As $\mathrm{codim}(C) \geq (n - m) + m/2 + 1/2$, we also have:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right)}{\deg(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega) D^{\dim(\Omega)}}{e^{mL} \delta^{1/2L}} \frac{D^{(n-m)L}}{\delta^{(n-m)L}}.$$

As $D \leq (1 + \frac{1}{n-m})\delta$ we get:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right)}{\deg(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega) D^{\dim(\Omega)}}{e^{mL} \delta^{1/2L}} \left(1 + \frac{1}{n-m} \right)^{(n-m)L}.$$

Hence,

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right)}{\deg(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega) D^{\dim(\Omega)}}{e^{mL} \delta^{1/2L}} \left(\left(1 + \frac{1}{n-m} \right)^{(n-m)} \right)^L.$$

And thus,

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right)}{\deg(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega) D^{\dim(\Omega)}}{\delta^{1/2L}} \left(\frac{1}{e} \right)^{(m-1)L}.$$

Again, as $D \leq (1 + \frac{1}{n-m})\delta$ and $L \geq 6\dim(\Omega)$ we also have:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right)}{\deg(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)}{\delta^{\dim(\Omega)}} \frac{1}{\delta^{\dim(\Omega)}} \left(\frac{D}{\delta} \right)^{\dim(\Omega)} \left(\frac{1}{e} \right)^{(m-1)L}.$$

Namely,

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right)}{\deg(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)}{\delta^{\dim(\Omega)}} \frac{1}{\delta^{\dim(\Omega)}} e^{\frac{\dim(\Omega)}{n-m}} \left(\frac{1}{e} \right)^{(m-1)L}.$$

As $\delta \geq e^2(d+1)^2$, this yields:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L \right)}{\deg(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)}{\delta^{\dim(\Omega)}} \left(\frac{1}{e} \right)^{\dim(\Omega)} \left(\frac{1}{e} \right)^{(m-1)L}.$$

Finally, as $\log(\delta)\dim(\Omega) \geq 2\log(\deg_{\mathrm{lci}}(\Omega))$ we also get:

$$(5.4) \qquad \frac{\deg\left(\overline{\pi_2(B(\Omega,L))}^z \cap (C\cap A)^L\right)}{\deg(C^L)} \leq \frac{1}{\deg_{\mathrm{lci}}(\Omega)} \left(\frac{1}{e}\right)^{\dim(\Omega)} \left(\frac{1}{e}\right)^{(m-1)L}.$$

Now, we consider the following constructible subset:

$$R^c(\Omega,\Sigma,C,L) = \{\mathbf{Q} := (x_1,\ldots,x_L) \in C^L \ : \ \mathbf{Q} \text{ is not a CTS for } \Omega \text{ w.r.t. } \Sigma\}.$$

Note that $R^c(\Omega,\Sigma,C,L) = (C)^L \setminus R(\Omega,\Sigma,C,L)$.

Claim. *With these notations, if $A \in \mathbb{G}(C)$, we have:*

$$\sharp\left(R^c(\Omega,\Sigma,C,L) \cap A^L\right) \leq \deg\left(\overline{\pi_2(B(\Omega,L))}^z \cap (C\cap A)^L\right).$$

Proof of the Claim. Observe that

$$R^c(\overline{\Omega}^z,\Sigma,C,L) \subseteq \pi_2(B(\Omega,L)) \cap C^L.$$

For if $\mathbf{Q} := (x_1,\ldots,x_L) \in R^c(\Omega,\Sigma,C,L)$ there is some list of polynomial equations $f \in \Omega \setminus \Sigma$, such that:

$$f(x_1) = \cdots = f(x_L) = 0.$$

Hence, $(f,x_1,\ldots,x_L) \in V(\Omega,L)$. Moreover, there must be some locally irreducible component $W \in \mathscr{D}$ of $V(\Omega,L)$ that contains $(f,x_1,\ldots,x_L)$. But $f := \pi_1(f,x_1,\ldots,x_L) \in \Omega \setminus \Sigma$ and, hence, $W \in \mathscr{C}$. Then, $(f,x_1,\ldots,x_L) \in B(\Omega,L)$ and

$$\mathbf{Q} := (x_1,\ldots,x_L) \in \pi_2(B(\Omega,L)).$$

Then, we conclude:

$$R^c(\overline{\Omega}^z,\Sigma,C,L) \subseteq \pi_2(B(\Omega,L)) \cap C^L \subseteq \overline{\pi_2(B(\Omega,L))}^z \cap C^L,$$

and

$$R^c(\overline{\Omega}^z,\Sigma,C,L) \cap A^L \subseteq \overline{\pi_2(B(\Omega,L))}^z \cap (C\cap A)^L$$

As $A \in \mathbb{G}(C)$, then $(A\cap C)$ is a zero-dimensional algebraic variety (i.e. a finite set) and, thus, $R^c(\overline{\Omega}^z,\Sigma,C,L) \cap A^L$ is also a finite set. Finally, in the zero-dimensional case degree equals cardinality and, hence, the claim follows:

$$\sharp\left(R^c(\Omega,\Sigma,C,L) \cap A^L\right) \leq \deg\left(\overline{\pi_2(B(\Omega,L))}^z \cap (C\cap A)^L\right).$$

∎

Just to conclude our statement, as for every $A \in \mathbb{G}(C)$, $\sharp(A\cap C) = \deg(C)$, then we obtain:

$$\mathrm{Prob}_{(C\cap A)^L}[R] := 1 - \mathrm{Prob}_{(C\cap A)^L}[R^c],$$

where $R^c := R^c(\Omega,\Sigma,C,L)$. Namely, we have:

$$\mathrm{Prob}_{(C\cap A)^L}[R] = 1 - \frac{1}{\sharp\left((A\cap C)^L\right)} \sum_{\zeta \in (A\cap C)^L} \chi_{R^c}(\zeta) = 1 - \frac{\sharp(R^c \cap (A\cap C)^L)}{\sharp\left((A\cap C)^L\right)}.$$

Then, from the previous Claim and Inequality (5.4) we conclude:

$$\mathrm{Prob}_{(C\cap A)^L}[R] \geq 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega)} \left(\frac{1}{e^{\dim(\Omega)+(m-1)L}}\right),$$

and the Theorem follows. □

In the complex case $(K = \mathbb{C})$ the complex Grassmannian may be equipped with a probability distribution μ such that for every Borel subset $B \subseteq \mathbb{G}(n,n-r)$ of the Zariski topology the following holds:

$$(5.5) \qquad \mu[B] := \begin{cases} 1, & B \text{ has non-empty interior in } \mathbb{G}(n,r) \\ 0 & \text{otherwise} \end{cases}$$

Then, with this measure the previous statement becomes the following:

Corollary 5.2. *Assuming $K = \mathbb{C}$, a probability distribution μ on the Borel sets $\mathcal{B}(\mathbb{G}(n, n-r))$ that satisfies Identity (5.5) above and with the same notations and assumptions as in Theorem 5.1, the following inequality holds:*

$$\frac{1}{\deg_{\mathrm{lci}}(C)^L} E_{\mathbb{G}(n,n-r)}[\sharp_R^{(L)}] \geq 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega)e^{\dim(\Omega)+(m-1)L}},$$

where $E_{\mathbb{G}(n,n-r)}$ means expectation and

$$\sharp_R^{(L)}: \quad \mathbb{G}(n, n-r) \quad \longrightarrow \quad \mathbb{R}_+ \cup \{\infty\}$$
$$A \quad \longmapsto \quad \sharp\left(R(\Omega, \Sigma, C, L) \cap A^L\right).$$

Proof. Just note that with the hypothesis of Identity (5.5),

$$E_{\mathbb{G}(n,n-r)}[\sharp_R^{(L)}] = E_{\mathbb{G}(C)}[\sharp_R^{(L)}],$$

where $\mathbb{G}(C)$ is the Zariski open subset of $\mathbb{G}(n, n-r)$ discussed in the proof of the previous Theorem. And, finally, just apply the previous Theorem on the quotient:

$$\frac{\sharp_R^{(L)}(A)}{\deg_{\mathrm{lci}}(C)^L} = \mathrm{Prob}_{(A\cap C)^L}[R].$$

$\square$

With a slight modification of the hypothesis of Theorem 5.1, we obtain the following result for the case in which C is a globally equi-dimensional constructible set:

Corollary 5.3. *Let $m, n \in \mathbb{N}$ be two positive integers, with $m \leq n$, and let $(d) := (d_1, \ldots, d_m)$ be a list of degrees and $d := \max\{d_1, \ldots, d_m\}$. Let $\Sigma \subseteq \Omega$ be two constructible subsets of $\mathscr{P}_{(d)}^K$ such that Σ has co-dimension at least 1 in Ω. Assume that $\Omega \setminus \Sigma$ satisfies the following property:*

$$(5.6) \qquad \forall f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma, \ \dim(V_\mathbb{A}(f_1, \ldots, f_m)) = n - m.$$

Let $C \subseteq \mathbb{A}^n$ be a globally equi-dimensional constructible set of co-dimension $r \geq (n-m)+m/2+ 1/2$. Assume that there are constructible subsets $C_1, \ldots, C_s \subseteq \mathbb{A}^n$ such that $C := C_1 \cap \ldots \cap C_s$. Let $D := \max\{\deg_{\mathrm{lci}}(C_1), \ldots, \deg_{\mathrm{lci}}(C_s)\} \geq 1$ be the maximum of their degrees. Let $L \in \mathbb{N}$ be a positive integer and assume that the following properties hold:

i) $L \geq 6\dim(\Omega)$,
ii) $\log(\deg_z(C)) \geq r\max\{2(1 + \log(d+1)), \frac{2\log(\deg_{\mathrm{lci}}(\Omega))+sL}{\dim(\Omega)}\}$,
iii) $D \leq \frac{1}{e}(1 + \frac{1}{n-m})\deg_z(C)^{\frac{1}{\mathrm{codim}(C)}}$,

Let $R := R(\Omega, \Sigma, C, L)$ be the constructible set of all sequences $\mathbf{Q} \in C^L$ of length L which are correct test sequences for Ω with respect to Σ. Then, there is a non-empty Zariski open subset $\mathbb{G}(C) \subseteq \mathbb{G}(n, n-r)$ such that for every $A \in \mathbb{G}(C)$, the probability that a randomly chosen list $\mathbf{Q} \in (C \cap A)^L$ is in R satisfies:

$$\mathrm{Prob}_{(C\cap A)^L}[R] \geq 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega)e^{\dim(\Omega)+(m-1)L}},$$

where $(A \cap C)^L$ is endowed with its uniform probability distribution.

Proof. With the same notations as in the proof of Theorem 5.1, we have that:

$$\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L = \overline{\pi_2(B(\Omega, L))}^z \cap \left(\bigcap_{i,j} C_{i,j}\right) \cap \left(\bigcap_{j=1}^L A_j\right),$$

where the $C_{i,j}$'s are constructible sets. From Theorem 3.4 we get:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right) \leq \binom{(sL+1) + \dim(\pi_2(B(\Omega, L))) - 1}{\dim(\pi_2(B(\Omega, L)))}$$
$$\deg_{\mathrm{lci}}(B(\Omega, L))D^{\dim(\pi_2(B(\Omega, L)))}.$$

where, as $\deg(A_j) = 1$, we have:

$$1 \leq \max\{\deg_{\mathrm{lci}}(C_{i,j}) \ : \ 1 \leq i \leq s, \ 1 \leq j \leq L\} = D = \max\{\deg_{\mathrm{lci}}(C_i) \ : \ 1 \leq i \leq s\}.$$

Note that if $a, b \in \mathbb{Z}^+$, we have:

$$\binom{a+b}{b} \leq e^{a+b}$$

Thus, putting all together, as $\dim(\pi_2(B(\Omega, L))) \leq \dim(B(\Omega, L))$, we get:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right) \leq \deg_{\mathrm{lci}}(\Omega)(d+1)^{mL} D^{\dim(\Omega)+(n-m)L} e^{sL+\dim(\Omega)+(n-m)L}.$$

This yields:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right) \leq \deg_{\mathrm{lci}}(\Omega)(De)^{\dim(\Omega)}(De)^{(n-m)L}(d+1)^{mL} e^{sL}.$$

As $\delta \geq e^2(d+1)^2$, we have:

$$\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right) \leq \deg_{\mathrm{lci}}(\Omega)(De)^{\dim(\Omega)}(De)^{(n-m)L}\left(\frac{\delta}{e^2}\right)^{\frac{m}{2}L} e^{sL}.$$

Then, we obtain:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)(De)^{\dim(\Omega)}(De)^{(n-m)L}\delta^{\frac{m}{2}L} e^{sL}}{e^{mL}\delta^{\mathrm{codim}(C)L}}.$$

As $\mathrm{codim}(C) \geq (n-m) + m/2 + 1/2$, we also have:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)(De)^{\dim(\Omega)}}{e^{mL}\delta^{1/2L}} \frac{(De)^{(n-m)L}}{\delta^{(n-m)L}} e^{sL}.$$

As $D \leq \frac{1}{e}(1 + \frac{1}{n-m})\delta$ we get:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)(De)^{\dim(\Omega)}}{e^{mL}\delta^{1/2L}} \left(1 + \frac{1}{n-m}\right)^{(n-m)L} e^{sL}.$$

Hence,

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)(De)^{\dim(\Omega)}}{e^{mL}\delta^{1/2L}} \left(\left(1 + \frac{1}{n-m}\right)^{(n-m)}\right)^L e^{sL}.$$

And thus,

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)(De)^{\dim(\Omega)}}{\delta^{1/2L}} \left(\frac{1}{e}\right)^{(m-1)L} e^{sL}.$$

Again, as $D \leq \frac{1}{e}(1 + \frac{1}{n-m})\delta$ and $L \geq 6\dim(\Omega)$ we also have:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)}{\delta^{\dim(\Omega)}} \frac{1}{\delta^{\dim(\Omega)}} \left(\frac{De}{\delta}\right)^{\dim(\Omega)} \left(\frac{1}{e}\right)^{(m-1)L} e^{sL}.$$

Namely,

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)}{\delta^{\dim(\Omega)}} \frac{1}{\delta^{\dim(\Omega)}} e^{\frac{\dim(\Omega)}{n-m}} \left(\frac{1}{e}\right)^{(m-1)L} e^{sL}.$$

As $\delta \geq e^2(d+1)^2$, this yields:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{\deg_{\mathrm{lci}}(\Omega)}{\delta^{\dim(\Omega)}} \left(\frac{1}{e}\right)^{\dim(\Omega)} \left(\frac{1}{e}\right)^{(m-1)L} e^{sL}.$$

Finally, as $\log(\delta)\dim(\Omega) \geq 2\log(\deg_{\mathrm{lci}}(\Omega)) + sL$ we also get:

$$\frac{\deg\left(\overline{\pi_2(B(\Omega, L))}^z \cap (C \cap A)^L\right)}{\deg_z(C^L)} \leq \frac{1}{\deg_{\mathrm{lci}}(\Omega)} \left(\frac{1}{e}\right)^{\dim(\Omega)} \left(\frac{1}{e}\right)^{(m-1)L}.$$

The final part of the proof is identical to that of Theorem 5.1. $\qquad \square$

Using Corollary 2.24, we can generalize the previous Corollary for any constructible set as follows:

Corollary 5.4. *Let $m, n \in \mathbb{N}$ be two positive integers, with $m \le n$, and let $(d) := (d_1, \ldots, d_m)$ be a list of degrees and $d := \max\{d_1, \ldots, d_m\}$. Let $\Sigma \subseteq \Omega$ be two constructible subsets of $\mathscr{P}_{(d)}^K$ such that Σ has co-dimension at least 1 in Ω. Assume that $\Omega \setminus \Sigma$ satisfies the following property:*

$$(5.7) \qquad \forall f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma, \ \dim(V_{\mathbb{A}}(f_1, \ldots, f_m)) = n - m.$$

Let $C \subseteq \mathbb{A}^n$ be a constructible set of co-dimension $r \ge (n - m) + m/2 + 1/2$ and let $V_1, \ldots, V_k$ be the irreducible components of higher dimension of the Zariski closure of C (as in Proposition 2.5). Assume that there are constructible subsets $C_1, \ldots, C_s \subseteq \mathbb{A}^n$ such that $C := C_1 \cap \ldots \cap C_s$. Let $D := \max\{\deg_{\mathrm{lci}}(C_1), \ldots, \deg_{\mathrm{lci}}(C_s)\} \ge 1$ be the maximum of their degrees. Let $L \in \mathbb{N}$ be a positive integer and assume that the following properties hold:

  i) $L \ge 6 \dim(\Omega)$,
  ii) $\log(\sum_{i=1}^k \deg(V_i)) \ge r \max\{2(1 + \log(d+1)), \frac{2\log(\deg_{\mathrm{lci}}(\Omega)) + sL}{\dim(\Omega)}\}$,
  iii) $D \le \frac{1}{e}(1 + \frac{1}{n-m})(\sum_{i=1}^k \deg(V_i))^{\frac{1}{\mathrm{codim}(C)}}$,

Let $R := R(\Omega, \Sigma, C, L)$ be the constructible set of all sequences $\mathbf{Q} \in C^L$ of length L which are correct test sequences for Ω with respect to Σ. Then, there is a non-empty Zariski open subset $\mathbb{G}(C) \subseteq \mathbb{G}(n, n - r)$ such that for every $A \in \mathbb{G}(C)$, the probability that a randomly chosen list $\mathbf{Q} \in (C \cap A)^L$ is in R satisfies:

$$\mathrm{Prob}_{(C \cap A)^L}[R] \ge 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega) e^{\dim(\Omega) + (m-1)L}},$$

where $(A \cap C)^L$ is endowed with its uniform probability distribution.

Proof. The proof is similar to that of Corollary 5.3. In this case, we take:

$$\delta := (\sum_{i=1}^k \deg(V_i))^{\frac{1}{\mathrm{codim}(C)}},$$

and, from Corollary 2.24, we have that there is a non-empty Zariski open subset $\mathbb{G}(C) \subseteq \mathbb{G}(n, n - r)$ such that for all $A \in \mathbb{G}(C)$ we have $\sharp(C \cap A) = \sum_{i=1}^k \deg(V_i)$. $\qquad \square$

If we assume that C is a complete intersection algebraic variety, we obtain the following statement:

Corollary 5.5. *Let $m, n \in \mathbb{N}$ be two positive integers, with $m \le n$, and let $(d) := (d_1, \ldots, d_m)$ be a list of degrees and $d := \max\{d_1, \ldots, d_m\}$. Let $\Sigma \subseteq \Omega$ be two constructible subsets of $\mathscr{P}_{(d)}(X_1, \ldots, X_n)$ such that Σ has co-dimension at least 1 in Ω. Assume that $\Omega \setminus \Sigma$ satisfies the following property:*

$$(5.8) \qquad \forall f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma, \ \dim(V_{\mathbb{A}}(f_1, \ldots, f_m)) = n - m,$$

Let $V := V_{\mathbb{A}}(h_1, \ldots, h_r) \subseteq \mathbb{A}^n$ be a complete intersection algebraic variety of co-dimension $r \ge (n - m) + m/2 + 1/2$ such that $\deg(V) \ge \delta^r$, where $\delta := \min\{\deg(h_1), \ldots, \deg(h_r)\}$. Let $L \in \mathbb{N}$ be a positive integer and assume that the following properties hold:

  i) $L \ge 6 \dim(\Omega)$,
  ii) $\log(\delta) \ge \max\{2(1 + \log(d+1)), \frac{2\log(\deg_{\mathrm{lci}}(\Omega))}{\dim(\Omega)}\}$,
  iii) $\max\{\deg(h_1), \ldots, \deg(h_r)\} \le (1 + \frac{1}{n-m})\delta$.

Let $R := R(\Omega, \Sigma, V, L)$ be the constructible set of all sequences $\mathbf{Q} \in V^L$ of length L which are correct test sequences for Ω with respect to Σ. Then, there is a non-empty Zariski open subset $\mathbb{G}(V) \subseteq \mathbb{G}(n, n - r)$ such that for every $A \in \mathbb{G}(V)$ the probability that a randomly chosen list $\mathbf{Q} \in (V \cap A)^L$ is in R satisfies:

$$\mathrm{Prob}_{(V \cap A)^L}[R] \ge 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega) e^{\dim(\Omega) + (m-1)L}},$$

where $(A \cap V)^L$ is endowed with its uniform probability distribution.

Proof. This is a straight-forward application of Theorem 5.1, just taking $C = V$, $s = r$ and $C_i := V_{\mathbb{A}}(h_i)$ for every i, $1 \le i \le s$, we obtain the statement. $\qquad \square$

We may state the previous Corollary in the case we search for correct test sequences in zero-dimensional varieties:

Corollary 5.6. *Let $m, n \in \mathbb{N}$ be two positive integers, with $m \leq n$, and let $(d) := (d_1, \ldots, d_m)$ be a list of degrees and $d := \max\{d_1, \ldots, d_m\}$. Let $\Sigma \subseteq \Omega$ be two constructible subsets of $\mathscr{P}_{(d)}(X_1, \ldots, X_n)$ such that Σ has co-dimension at least 1 in Ω. Assume that $\Omega \setminus \Sigma$ satisfies the following property:*

$$\forall f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma, \ \dim(V_{\mathbb{A}}(f_1, \ldots, f_m)) = n - m,$$

Let $V := V_{\mathbb{A}}(h_1, \ldots, h_n) \subseteq \mathbb{A}^n$ be a zero-dimensional algebraic variety given by polynomial equations of the same degree $\delta := \deg(h_i)$, $1 \leq i \leq n$. Assume that $\deg(V) = \delta^n$. Let $L \in \mathbb{N}$ be a positive integer and assume that the following properties hold:

  i) $L \geq 6 \dim(\Omega)$,
  ii) $\log(\delta) \geq \max\{2(1 + \log(d+1)), \frac{2 \log(\deg_{\text{lci}}(\Omega))}{\dim(\Omega)}\}$,

Let $R := R(\Omega, \Sigma, V, L)$ be the constructible set of all sequences $\mathbf{Q} \in V^L$ of length L which are correct test sequences for Ω with respect to Σ. Assume that V is endowed with its uniform probability distribution. Then, we have:

$$\text{Prob}_{V^L}[R] \geq 1 - \frac{1}{\deg_{\text{lci}}(\Omega) e^{\dim(\Omega) + (m-1)L}}.$$

Corollary 5.5 gives sufficient conditions to have complete intersection varieties which are evasive to any system of polynomial equations in a given constructible set (as in [DKL, 14]). Given a degree list $(d) := (d_1, \ldots, d_m)$ and a constructible set $\widetilde{\Omega} \subseteq \mathscr{P}_{(d)}$, we say that a variety $V \subseteq \mathbb{A}^n$ is evasive with respect to $\widetilde{\Omega}$ if the following holds:

$$\forall f = (f_1, \ldots, f_m) \in \widetilde{\Omega}, \ \dim(V \setminus V_{\mathbb{A}}(f_1, \ldots, f_m)) = \dim(V).$$

In the case V is equi-dimensional, the previous property simply means that for all system $f \in \widetilde{\Omega}$ there is some irreducible component of V which is not completely embedded in $V_{\mathbb{A}}(f_1, \ldots, f_m)$ or, equivalently, that there is always an irreducible component that evades any variety defined by equations in $\widetilde{\Omega}$.

Corollary 5.7 (**Evasive varieties for lists of equations in a constructible set**). *Let $m, n \in \mathbb{N}$ be two positive integers, with $m \leq n$, and let $(d) := (d_1, \ldots, d_m)$ be a list of degrees and $d := \max\{d_1, \ldots, d_m\}$. Let $\Sigma \subseteq \Omega$ be two constructible subsets of $\mathscr{P}_{(d)}(X_1, \ldots, X_n)$ such that Σ has co-dimension at least 1 in Ω. Assume that $\Omega \setminus \Sigma$ satisfies the property described in Equation (5.8).*
Let $V \subseteq \mathbb{A}^n$ be any complete intersection variety such that $V := V_{\mathbb{A}}(h_1, \ldots, h_r) \subseteq \mathbb{A}^n$ of co-dimension $r \geq (n - m) + m/2 + 1/2$ and $\deg(V) \geq \delta^r$, where $\delta := \min\{\deg(h_1), \ldots, \deg(h_r)\}$. Assume that the following properties hold:

  i) $\log(\delta) \geq \max\{2(1 + \log(d+1)), \frac{2 \log(\deg(\Omega))}{\dim(\Omega)}\}$ *and,*
  ii) $\max\{\deg(h_1), \ldots, \deg(h_r)\} \leq (1 + \frac{1}{n-m})\delta$.

Then, V evades $\Omega \setminus \Sigma$.

Proof. Suppose that V does not evade $\Omega \setminus \Sigma$. Then, there is some $f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma$ such that:

$$(5.9) \qquad \dim(V \setminus V_{\mathbb{A}}(f_1, \ldots, f_m)) < \dim(V).$$

As V is complete intersection, all irreducible components of V have the same dimension $n - r$. Hence, Inequality (5.9) implies that all irreducible components of V are included in $V_{\mathbb{A}}(f_1, \ldots, f_m)$.
By the same reason, there is a non-empty Zariski open subset $\mathbb{G}_1(V) \subseteq \mathbb{G}(n, n - r)$ such that for all $A \in \mathbb{G}_1(V)$ and for every irreducible component W of V, $\sharp(W \cap A) = \deg(W)$.
Let $\mathbb{G}(V) \subseteq \mathbb{G}(n, n - r)$ be the non-empty Zariski open subset of Corollary 5.5 above, then $\mathbb{G}_1(V) \cap \mathbb{G}(V)$ is also a non-empty Zariski open subset of $\mathbb{G}(n, n - r)$. Finally, for any positive integer number $L \in \mathbb{N}$, such that $L \geq 6 \dim(\Omega)$, and any $A \in \mathbb{G}_1(V) \cap \mathbb{G}(V)$ we would have that the following properties hold:

  • For every $\mathbf{Q} \in (A \cap V)^L$, $\mathbf{Q}$ is not a correct test sequence of Ω with respect to Σ. This holds because f vanishes identically in $\mathbf{Q}$. In particular, with the same notations as above, we would have:

$$\sharp\left(R(\Omega, \Sigma, V, L) \cap A^L\right) = 0.$$

- From Corollary 5.5, as all its hypothesis hold, we also have:

$$\frac{\sharp\left(R(\Omega, \Sigma, V, L) \cap A^L\right)}{\deg(V)^L} \geq 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega)e^{\dim(\Omega)+(m-1)L}} > 0.$$

We have then arrived to a contradiction and no such $f \in \Omega \setminus \Sigma$ exist. $\square$

A customary usage of correct test sequences is the case of constructible sets given as polynomial images of some affine space (i.e. the parameter space). We may also discuss our statements in these cases.

Corollary 5.8 (Unirational families of lists of polynomials). *With the same notations as above, let $(d) := (d_1, \ldots, d_m)$ be a degree list, $d := \max\{d_1, \ldots, d_m\}$ and $\Omega \subseteq \mathscr{P}_{(d)}$ an unirational constructible set, given as the image of a polynomial mapping:*

$$\varphi := (\varphi_1, \ldots, \varphi_N) : W \subseteq \mathbb{A}^M \longrightarrow \Omega \subseteq \mathscr{P}_{(d)},$$

where $N = N_{(d)} = \dim(\mathscr{P}_{(d)})$, $\Omega = \varphi(W)$ and W is a constructible set of dimension s. Let $t := s/\dim(\Omega) \geq 1$ be the quotient between the dimensions of W and Ω and let $D := \max\{\deg(\varphi_i) : 1 \leq i \leq N\}$ be the maximum of the degrees of the coordinates of φ. Let $\Sigma \subseteq \Omega$ be a constructible subset of co-dimension at least 1 in Ω and assume that the following property holds:

$$\forall f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma, \ \dim(V_{\mathbb{A}}(f_1, \ldots, f_m)) = n - m,$$

Let $V := V_{\mathbb{A}}(h_1, \ldots, h_r) \subseteq \mathbb{A}^n$ be a complete intersection algebraic variety of co-dimension $r \geq (n - m) + m/2 + 1/2$ such that $\deg(V) \geq \delta^r$, where $\delta := \min\{\deg(h_1), \ldots, \deg(h_r)\}$. Let $L \in \mathbb{N}$ be a positive integer and assume that the following properties hold:

  i) $L \geq 6s$,
  ii) $\log(\delta) \geq \max\{2(1 + \log(d+1)), 2t\left(\frac{\log(\deg_{\mathrm{lci}}(W))}{s} + \log(D)\right)\}$,
  iii) $\max\{\deg(h_1), \ldots, \deg(h_r)\} \leq (1 + \frac{1}{n-m})\delta$.

Let $R := R(\Omega, \Sigma, V, L)$ be the constructible set of all sequences $\mathbf{Q} \in V^L$ of length L which are correct test sequences for Ω with respect to Σ. Then, there is a non-empty Zariski open subset $\mathbb{G}(V) \subseteq \mathbb{G}(n, n-r)$ such that for every $A \in \mathbb{G}(V)$ the probability that a randomly chosen list $\mathbf{Q} \in (V \cap A)^L$ is in R satisfies:

$$\mathrm{Prob}_{(V \cap A)^L}[R] \geq 1 - \frac{1}{\deg_{\mathrm{lci}}(W)e^{s(\log(D)+1)+(m-1)L}},$$

where $(A \cap V)^L$ is endowed with its uniform probability distribution.

Proof. Obvious since correct test sequences are hereditary (cf. Proposition 4.10) and since the following inequality holds because of Corollary 3.3:

$$\deg_z(\Omega) = \deg\left(\overline{\varphi(W)}^z\right) \leq \deg_{\mathrm{lci}}(W)D^s.$$

                                                                                    $\square$

Remark 5.9. Note that if W is a linear affine subvariety and the dimension does not decrease too much through φ (for instance, $t := \frac{s}{\dim(\Omega)} \leq 2$), the hypothesis of the previous Corollary become:

  i) $L \geq 6s$,
  ii) $\log(\delta) \geq \max\{2(1 + \log(d+1)), 4(\log(D))\}$,
  iii) $\max\{\deg(h_1), \ldots, \deg(h_r)\} \leq (1 + \frac{1}{n-m})\delta$,

And the thesis thus become the same:

$$\mathrm{Prob}_{(V \cap A)^L}[R] \geq 1 - \frac{1}{e^{s(\log(D)+1)+(m-1)L}},$$

This is simply devoted to emphasize how the previous probability results apply to prove that correct test sequences of optimal length are highly dense in Demillo-Lipton-Schwartz-Zippel sampling set. We return to Corollary 3.9. As main application of that Corollary, we consider a finite subset $Q \subseteq \kappa$, a non-zero polynomial $f \in P_d^K$ and the hyper-surface $C := V_{\mathbb{A}}(f) \subseteq \mathbb{A}^n(K)$,

where K is the algebraic closure of κ. As in [DML, 78], [Zp, 79] and [Sch, 80], we proved that the probability that f does not vanishes at a random point $x \in Q^n$ is greater than:

$$1 - \frac{d}{\sharp(Q)}.$$

Thus, taking $Q \subseteq \kappa$ such that $\sharp(Q) \geq (2(d+1))^2$, we can produce a probabilistic algorithm for testing equality to zero for polynomials in the *dense input case*: Inputs moving freely in P_d^K. Now, we shall use Corollary 5.6 to prove that correct test sequences are highly distributed inside the sampling set Q^n with small changes in the cardinality of Q.

Corollary 5.10. *Let $n, d \in \mathbb{N}$ be two positive integers. Let Ω be a constructible subset of $P_d^K := P_d^K(X_1, \ldots, X_n)$. Assume that $\Omega \setminus \{0\} \neq \emptyset$.*
Let $Q \subseteq \kappa$ be a finite set. Let $L \in \mathbb{N}$ be a positive integer such that the following properties hold:

> *i) $L \geq 6 \dim(\Omega)$,*
> *ii) $\sharp(Q) \geq \max\{(2(d+1))^2, \deg_{\mathrm{lci}}(\Omega)^{\frac{2}{\dim(\Omega)}}\}$.*

Then, the probability that a random sequence $\mathbf{Q} \in V^L = (Q^n)^L$ is a correct test sequence for Ω is greater than:

$$1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega)e^{\dim(\Omega)}}.$$

In the dense input case (i.e. when $\Omega = P_d^K$), for any $L \geq 6 \dim(P_d^K)$ and $Q \subseteq \kappa$ such that:

$$\sharp(Q) \geq (2(d+1))^2,$$

the probability that a random point $\mathbf{Q} \in (Q^n)^L$ is a correct test sequence for P_d^K is greater than:

$$1 - \frac{1}{e^{\binom{d+n}{n}}}.$$

6. A $\mathbf{BPP}_K$ ALGORITHM FOR DETECTING GENERIC DIMENSION: "SUITE SÉCANTE"

In this section we exhibit an algorithmic application of the usage of correct test sequences that *differs form the usual zero tests: "Suite Sécante" Problem.* The problem may be stated as follows:

Let K be an algebraically closed field, $m, n \in \mathbb{N}$ two positive integers with $m \leq n$. Let $(d) := (d_1, \ldots, d_m)$ be a list of degrees and $\mathscr{P}_{(d)} := \mathscr{P}_{(d)}^K(X_1, \ldots, X_n)$ the $K-$vector space of lists $f := (f_1, \ldots, f_m)$ of polynomials $f_i \in K[X_1, \ldots, X_n]$ such that $\deg(f_i) \leq d_i$ for each i, $1 \leq i \leq m$. We denote by $N_{(d)}$ the dimension of $\mathscr{P}_{(d)}$.

Problem 2 ("Suite Sécante" Problem). *Design an algorithm that performs the following task:*
Given $f \in \mathscr{P}_{(d)}$ decide whether f is a "Suite Sécante". Namely, decide whether the following property holds:
The algebraic variety $V_{\mathbb{A}}(f_1, \ldots, f_m) \subseteq \mathbb{A}^n$ is a non-empty variety of dimension $n - m$.

Some authors would prefer to say that $V_{\mathbb{A}}(f_1, \ldots, f_m)$ is a set-theoretical complete intersection variety with defining equations $\{f_1, \ldots, f_m\}$.
We study not only the algorithm but also its complexity. The Model of Computation will be that of *Turing Machines over K* (in the sense of [BlCuShSm, 98] and references therein). We distinguish between the *generic case* and the *restricted input case*, where the input lists of polynomials will belong to some constructible subset $\Omega \subseteq \mathscr{P}_{(d)}$. We take into account the number of arithmetic operations required to evaluate the polynomials in the list $f := (f_1, \ldots, f_m)$. This is represented by *non-scalar straight-line program* encoding of the input list f. Note that this encoding is equivalent to *neural networks with polynomial activation functions*. See Sections 2 and 3 of [KP, 96] for details about non-scalar straight-line programs.
Many works in *Computational Algebraic Geometry* have deal with this problem. It will be too long to cite all of them. *The main novelty of our contribution is that we do not perform any operation (neither algebraic nor numeric) with the input polynomials in the list f: We just evaluate them at some given points of a correct test sequence* (see Algorithm 6.3 below).

We begin our discussion by stating some facts about "Suites Sécantes". We include proofs in order to be self-contained.

We first consider the following incidence variety $V_{(d)} \subseteq \mathscr{P}_{(d)} \times \mathbb{A}^n(K)$:

$$(6.1) \qquad V_{(d)} := \{(f, x) \in \mathscr{P}_{(d)} \times \mathbb{A}^n(K) \ : \ f(x) = 0 \in \mathbb{A}^m(K)\}.$$

We may see this incidence variety as a fiber of the natural evaluation morphism. Namely, we consider the evaluation morphism defined as follows:

$$(6.2) \qquad \begin{array}{rccc} \mathrm{ev}_{(d)}: & \mathscr{P}_{(d)} \times \mathbb{A}^n(K) & \longrightarrow & \mathbb{A}^m(K) \\ & (f, x) & \longmapsto & f(x). \end{array}$$

Obviously, $V_{(d)} := \mathrm{ev}_{(d)}^{-1}(\{0\})$. We additionally have two canonical projections defined as follows:

- The projection $\pi_1 : V_{(d)} \longrightarrow \mathscr{P}_{(d)}$ given by $\pi_1(f, x) := f$, $\forall (f, x) \in V_{(d)}$.
- The projection $\pi_2 : V_{(d)} \longrightarrow \mathbb{A}^n(K)$ given by $\pi_2(f, x) := x$, $\forall (f, x) \in V_{(d)}$.

Observe that for every $f \in \mathscr{P}_{(d)}$, the fiber $\pi_1^{-1}(\{f\})$ may be identified with the algebraic variety $V_{\mathbb{A}}(f)$ of all zeros in $\mathbb{A}^n(K)$.

The following statement contains the main properties of this incidence variety.

Theorem 6.1. *With these notations and assumptions, we have:*

  i) *The incidence variety $V_{(d)}$ is a smooth complete intersection variety of dimension $N_{(d)} + (n - m)$ and it is unmixed (i.e. all its irreducible components have the same dimension).*

  ii) *The canonical projection π_2 is onto and the fiber $\pi_2^{-1}(\{x\})$ is a linear affine variety of dimension $N_{(d)} - m$ contained in $V_{(d)}$ and isomorphic to a linear affine variety of $\mathscr{P}_{(d)}$ of the same dimension.*

  iii) *There is a Zariski open subset $U_\emptyset \subseteq \mathscr{P}_{(d)}$ contained in $\pi_1(V_{(d)})$ or, equivalently, there is a closed proper algebraic subvariety $W_\emptyset \subseteq \mathscr{P}_{(d)}$, such that for all $f \in \mathscr{P}_{(d)} \setminus W_\emptyset = U_\emptyset$, $\pi_1^{-1}(\{f\}) = V_{\mathbb{A}}(f) \neq \emptyset$.*

  iv) *The canonical projection π_1 is dominant on each irreducible component C of $V_{(d)}$ such that $\pi_1(C)$ contains a "Suite Sécante". In fact, for every irreducible component C of $V_{(d)}$ we have just two possible cases:*
    - *Either there is $f \in \pi_1(C)$ such that $\dim(\pi_1^{-1}(\{f\}) \cap C) = n - m$, in which case $\pi_1(C)$ is dense in $\mathscr{P}_{(d)}$ for the Zariski topology.*
    - *Or for all $f \in \pi_1(C)$, $\dim(\pi_1^{-1}(\{f\}) \cap C) \geq n - m + 1$ and the Zariski closure of $\pi_1(C)$ is strictly included in $\mathscr{P}_{(d)}$. In this case, $f_1, \ldots, f_m$ is not a "Suite Sécant".*

In conclusion, there is a Zariski open subset $U \subseteq \mathscr{P}_{(d)}$ such that for every $f = (f_1, \ldots, f_m) \in U$, $V_{\mathbb{A}}(f) \neq \emptyset$ and it is an algebraic variety of dimension $n - m$. Equivalently, for all $f = (f_1, \ldots, f_m) \in U$, the sequence $f_1, \ldots, f_m$ is a "Suite Sécante".

Proof. We first consider the evaluation map $\mathrm{ev}_{(d)}$. It is easy to observe that $\mathrm{ev}_{(d)}$ is onto since given $v \in \mathbb{A}^m(K)$ and given $f \in \pi_2^{-1}(\{0\})$, then $f - v \in \mathscr{P}_{(d)}$ and $\mathrm{ev}_{(d)}(f - v, 0) = v$.

By the Theorem on the Dimension of the Fibers (cf. [Sha, 77], for instance), as $\mathscr{P}_{(d)} \times \mathbb{A}^n(K)$ is irreducible, there is a Zariski open subset $\mathscr{U} \subseteq \mathbb{A}^m(K)$ such that for all $v \in \mathscr{U}$ the non-empty fiber $\mathrm{ev}_{(d)}^{-1}(\{v\})$ satisfies:

$$\dim\left(\mathrm{ev}_{(d)}^{-1}(\{v\})\right) = \dim\left(\mathscr{P}_{(d)} \times \mathbb{A}^n(K)\right) - m = N_{(d)} + (n - m).$$

Moreover, all fibers are identifiable by the obvious translation:

$$\begin{array}{rcl} \mathrm{ev}_{(d)}^{-1}(\{v\}) & \longrightarrow & \mathrm{ev}_{(d)}^{-1}(\{0\}) \\ (f, x) & \longmapsto & (f - v, x). \end{array}$$

Thus, we conclude that $V_{(d)} = \mathrm{ev}_{(d)}^{-1}(\{0\})$ is an algebraic variety of dimension $N_{(d)} + (n - m)$. We consider two sets of variables to represent the elements in $\mathscr{P}_{(d)} \times \mathbb{A}^n(K)$. On one side, we consider the set of variables $\{X_1, \ldots, X_n\}$ that represent the coordinates of the points in $\mathbb{A}^n(K)$. On the other side, we consider the family of generic coefficients of polynomials in $\mathscr{P}_{(d)}$:

$$\{U_\mu^{(i)} \ : \ 1 \leq i \leq m, \ |\mu| \leq d_i\}.$$

Thus, generic polynomials in P_{d_i} have the following descriptions:

$$F_i := \sum_{|\mu| \leq d_i} U_\mu^{(i)} X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Then, the equations defining $V_{(d)}$ may be understood as the following m equations in these two sets of variables:

$$F_i\left((U_\mu^{(i)} \ : \ 1 \leq i \leq m, |\mu| \leq d_i), X_1, \ldots, X_n\right) = 0, \ 1 \leq i \leq m,$$

where $F_i \in K[(U_\mu^{(i)} \ : \ 1 \leq i \leq m, |\mu| \leq d_i), X_1, \ldots, X_n]$ are polynomials of degree $d_i + 1$ in these two sets of variables. We may also consider the Jacobian matrix $D(F) := D(F_1, \ldots, F_m)$ of these equations with respect to all variables involved. This Jacobian matrix contains an $m \times m$ identity matrix:

$$\begin{pmatrix} \frac{\partial F_1}{\partial U_{(0)}^{(1)}} & \cdots & \frac{\partial F_1}{\partial U_{(0)}^{(m)}} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_m}{\partial U_{(0)}^{(1)}} & \cdots & \frac{\partial F_m}{\partial U_{(0)}^{(m)}} \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} = Id_m,$$

where $(0) = (0, \ldots, 0) \in \mathbb{N}^m$ is the exponent of the independent term. Hence, $\text{rank}(D(F)) = m$ and it is independent of the point $(f, x) \in V_{(d)}$ under consideration. By the Jacobian Criterion Theorem, we conclude that the variety $V_{(d)}$ is smooth and the tangent space $T_{(f,x)}V_{(d)}$ is of dimension $N_{(d)} + (n - m)$. This proves Claim $i)$.

As for Claim $ii)$ we have simply to observe that for every $x \in \mathbb{A}^n(K)$ the following is a vector subspace of co-dimension 1 of P_{d_i}:

$$\{f \in P_{d_i} \ : \ f(x) = 0\},$$

and the rest of the Claim immediately follows.

For Claim $iii)$ we recall *Generalised Pham systems* as in [PSM, 04] and references therein. Let $f := (f_1, \ldots, f_m) \in \mathscr{P}_{(d)}$ be a sequence of polynomials. We just work on the Zariski open subset $\mathscr{W}_{(d)} \subseteq \mathscr{P}_{(d)}$ of all sequences of polynomials $f = (f_1, \ldots, f_m) \in \mathscr{P}_{(d)}$ such that $\deg(f_i) = d_i$ for each i, $1 \leq i \leq m$. Given $f \in \mathscr{W}_{(d)}$, for every i, $1 \leq i \leq m$, let us consider the highest degree homogeneous component of f_i. Namely, if:

$$f_i := \sum_{|\mu| \leq d_i} a_\mu^{(i)} X_1^{\mu_1} \cdots X_n^{\mu_n},$$

then its homogeneous part of degree d_i is given by:

$$(f_i)_{d_i} := \sum_{|\mu| = d_i} a_\mu^{(i)} X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Let us now consider a matrix $M \in \mathscr{M}_{(n-m) \times n}(K)$ in the Zariski open set $G((n - m) \times n, K)$ of all matrices in $\mathscr{M}_{(n-m) \times n}(K)$ of rank $n - m$ and a vector $b \in \mathbb{A}^{n-m}(K)$. They define a sequence of degree 1 polynomials $\ell_1, \ldots, \ell_m : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^{n-m}(K)$ by the following identity:

$$\begin{pmatrix} \ell_1(x) \\ \vdots \\ \ell_{n-m}(x) \end{pmatrix} := M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + b.$$

Then, we have an enlarged system $F := (f_1, \ldots, f_m, \ell_1, \ldots, \ell_{n-m})$ of polynomial equations. We may then consider the highest degree homogeneous components of all of them:

$$F_{\text{init}} := ((f_1)_{d_1}, \ldots, (f_m)_{d_m}, (\ell_1)_1, \ldots, (\ell_{n-m})_1).$$

This is a family of homogeneous polynomials of respective degrees determined by the list $(\delta) := (d_1, \ldots, d_m, 1, \ldots, 1) \in \mathbb{N}^n$, in the set of variables $\{X_1, \ldots, X_n\}$. As in [PSM, 04], we say that F is a *Generalized Pham system* if the set of common zeros in the projective space $\mathbb{P}_{n-1}(K)$ of the polynomials in the list F_{init} is empty. Hence, the classical multivariate resultant theory (cf. [Jo, 97], [CaDi, 05], [FP, 13], [BuJo, 14] and references therein) implies that there exists a

non-zero polynomial in the coefficients $U_\mu^{(i)}$ of the polynomials $(f_i)_{d_i}$ and the coordinates $T_{r,s}$ of the matrices $M \in \mathscr{M}_{(n-m)\times n}(K)$,

$$\mathrm{Res}_{(\delta)} \in \mathbb{Z}[(U_\mu^{(i)} : 1 \le i \le m, \ |\mu| = d_i), (T_{r,s} \ : \ 1 \le r \le n-m, 1 \le s \le n)],$$

such that

$$\mathrm{Res}_{(\delta)}((f_1)_{d_1}, \ldots, (f_m)_{d_m}, (\ell_1)_1, \ldots, (\ell_{n-m})_1) = 0 \Longleftrightarrow V_{\mathbb{P}_{n-1}(K)}(F_{\mathrm{init}}) \ne \emptyset,$$

where $\mathrm{Res}_{(\delta)}((f_1)_{d_1}, \ldots, (f_m)_{d_m}, (\ell_1)_1, \ldots, (\ell_{n-m})_1)$ represents the result of evaluating $\mathrm{Res}_{(\delta)}$ at the coefficients of the polynomials in the list F_{init} and $V_{\mathbb{P}_{n-1}(K)}(F_{\mathrm{init}})$ is the set of projective zeros in $\mathbb{P}_{n-1}(K)$ of the list of homogeneous polynomial equations in F_{init}. This implies that the following set (formed by Generalized Pham systems) is a Zariski open subset in $\mathscr{P}_{(d)} \times \mathscr{M}_{(n-m)\times n}(K) \times \mathbb{A}^{n-m}(K)$:

(6.3) $$\mathscr{G}_{(d)} := \{F := (f_1, \ldots, f_m, \ell_1, \ldots, \ell_{n-m}) \in \mathscr{P}_{(d)} \times \mathscr{M}_{(n-m)\times n}(K) \times \mathbb{A}^{n-m}(K) \ : \\ (f_1, \ldots, f_m) \in \mathscr{W}_{(d)}, \text{and } F \text{ is a Generalized Pham system}\}.$$

Now we consider the homogenisation with respect to a new variable X_0 of a list of polynomials equations $F := (f_1, \ldots, f_m, \ell_1, \ldots, \ell_{n-m}) \in \mathscr{G}_{(d)}$. We denote by ${}^h F$ such new list of homogeneous polynomials equations in the set of variables $\{X_0, \ldots, X_n\}$. As the number of homogeneous equations n and the dimension of $\mathbb{P}_n(K)$ are equal, the variety of the zeros of ${}^h F$ in $\mathbb{P}_n(K)$ is non-empty and as $F \in \mathscr{G}_{(d)}$, no zero of ${}^h F$ lies at the infinity hyperplane:

$$H_\infty := \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}_n(K) \ : \ x_0 = 0\}.$$

In other words, there exists a Zariski open subset $\mathscr{G}_{(d)} \subseteq \mathscr{P}_{(d)} \times \mathscr{M}_{(n-m)\times n}(K) \times \mathbb{A}^{n-m}(K)$ such that for all $F \in \mathscr{G}_{(d)}$ the set of affine zeros in $\mathbb{A}^n(K)$ of F agree with the set of projective zeros of ${}^h F$ in $\mathbb{P}_n(K)$, which is non-empty:

$$V_{\mathbb{A}}(f_1, \ldots, f_m, \ell_1, \ldots, \ell_{n-m}) \cong V_{\mathbb{P}_n(K)}({}^h F) \ne \emptyset.$$

In particular, there is a non-zero polynomial in the list of coefficients $\mathcal{U} := (U_\mu^{(i)} \ : \ 1 \le i \le m, |\mu| \le d_i)$ of the equations in $\mathscr{P}_{(d)}$, the coordinates $\mathcal{M} := (T_{r,s} \ : \ 1 \le r \le n-m, 1 \le s \le n)$ of the matrices in $\mathscr{M}_{(n-m)\times}(K)$ and the coordinates $\mathcal{Z} := (Z_1, \ldots, Z_{n-m})$ of the points in $\mathbb{A}^{n-m}(K)$:

$$P(\mathcal{U}, \mathcal{M}, \mathcal{Z}) \in K[\mathcal{U}, \mathcal{M}, \mathcal{Z}] \setminus \{0\},$$

such that if $P(f_1, \ldots, f_m, \ell_1, \ldots, \ell_{n-m}) \ne 0$, then the variety:

$$V_{\mathbb{A}}(f_1, \ldots, f_m, \ell_1, \ldots \ell_{n-m}) \ne \emptyset.$$

Now, as K is an infinite field, there are some matrix $M \in \mathscr{M}_{(n-m)\times n}(K)$ and some point $\zeta \in \mathbb{A}^{n-m}(K)$ such that the polynomial:

$$Q(\mathcal{U}) := P(\mathcal{U}, M, \zeta) \in K[\mathcal{U}] \setminus \{0\}.$$

Hence, we have proved that:

$$\forall f := (f_1, \ldots, f_m) \in \mathscr{P}_{(d)}, \ Q(f_1, \ldots, f_m) \ne 0 \Longrightarrow V_{\mathbb{A}}(f_1, \ldots, f_m) \ne \emptyset.$$

Thus, the following Zariski open subset is contained in $\pi_1(V_{(d)})$ and Claim $iii)$ immediately follows:

$$\pi_1(V_{(d)}) \supseteq \{f = (f_1, \ldots, f_m) \in \mathscr{P}_{(d)} \ : \ Q(f_1, \ldots, f_m) \ne 0\}.$$

Let $U_\emptyset$ be a non-empty Zariski open subset of $\mathscr{P}_{(d)}$ contained in $\pi_1(V_{(d)})$. Then, for every $f \in U_\emptyset$, $V_{\mathbb{A}}(f) \ne \emptyset$.

Finally, for Claim $iv)$ we consider an irreducible component C of $V_{(d)}$ and we take its projection $\pi_1(C) \subseteq \mathscr{P}_{(d)}$. Then, we consider the restriction mapping:

$$\pi_1\big|_C : C \longrightarrow \overline{\pi_1(C)}^z.$$

This is a dominant morphism and, by the Theorem on the Dimension of the Fibers, we first conclude that for any $f \in \pi_1(C)$ we have:

$$\dim(\pi_1^{-1}(\{f\}) \cap C) = \dim(\pi_1\big|_C^{-1}(\{f\})) \ge \dim(C) - \dim(\overline{\pi_2(C)}^z).$$

If $\dim(\pi_1^{-1}(\{f\}) \cap C) = n-m$, then we have that:

$$\dim(\overline{\pi_1(C)}^z) \ge \dim(C) - (n-m) = N_{(d)} + (n-m) - (n-m) = N_{(d)},$$

and, hence $\pi_1(C)$ is Zariski dense in $\mathscr{P}_{(d)}$.

Otherwise, there is a Zariski open subset $U_C \subseteq \pi_1(C) \subseteq \overline{\pi_1(C)}^z$ such that for all $g \in U_C$ we will have:

$$\dim(\pi_1^{-1}(\{g\}) \cap C) = \dim(\pi_1\big|_C^{-1}(\{g\})) = \dim(C) - \dim(\overline{\pi_1(C)}^z).$$

If $\dim(\pi_1^{-1}(\{g\}) \cap C) \geq n - m + 1$, for all $g \in \pi_2(C)$, then we conclude

$$\dim(\overline{\pi_1(C)}^z) = \dim(C) - \dim(\pi_1^{-1}(\{g\}) \cap C) \leq N_{(d)} + (n-m) - (n-m+1) = N_{(d)} - 1,$$

and, hence, $\pi_1(C)$ will not be Zariski dense in $\mathscr{P}_{(d)}$.

As for the last claim of the Theorem, we just have to prove that the class:

$$\mathscr{S} := \{f \in \mathscr{P}_{(d)} \ : \ f \text{ is a "Suite Sécante"}\},$$

contains a non-empty Zariski open subset. Let $\mathscr{C}$ be the class of all irreducible components of $V_{(d)}$ such that there is some $f \in \pi_1(C)$ satisfying $\dim(\pi_1^{-1}(f) \cap C) = n - m$. Let $\mathscr{W}$ be the class of all irreducible components of $V_{(d)}$ such that $\pi_1(W)$ is not Zariski dense in $\mathscr{P}_{(d)}$. Then, we consider the non-emtpy Zariski open subset of $\mathscr{P}_{(d)}$ given by the following identity:

$$A := \mathscr{P}_{(d)} \setminus \left(\bigcup_{C \in \mathscr{W}} \overline{\pi_1(C)}^z \right).$$

For every $C \in \mathscr{C}$, we have that $\pi_1(C)$ is Zariski dense in $\mathscr{P}_{(d)}$. Then, because of the Theorem on the Dimension of the Fibers (cf. [Sha, 77]) for every $C \in \mathscr{C}$ there is a Zariski open $U_C \subseteq \mathscr{P}_{(d)}$ such that for all $f \in U_C$, we have:

$$\dim\left(\pi_1^{-1}(\{f\}) \cap C\right) = \dim\left(\pi_1\big|_C^{-1}(\{f\})\right) = \dim(C) - \dim(\mathscr{P}_{(d)}) = N_{(d)} + (n-m) - N_{(d)} = n-m.$$

As $\mathscr{P}_{(d)}$ is irreducible, the following open subset $U \subseteq \mathscr{P}_{(d)}$ is non-empty:

$$U := A \cap U_\emptyset \cap \left(\bigcap_{C \in \mathscr{C}} U_C \right).$$

Moreover, for every $f \in U$ we have:

- As $f \in U_\emptyset$, $V_{\mathbb{A}}(f) \neq \emptyset$.
- As $f \in A$, then $f \notin \pi_1(D)$ for any $D \in \mathscr{W}$ or, equivalently, we have $\pi_1^{-1}(\{f\}) \cap D = \emptyset$ for every $D \in \mathscr{W}$. In particular, we have that:

$$V_{\mathbb{A}}(f) = \pi_1^{-1}(\{f\}) = \left(\bigcup_{D \in \mathscr{W}} \left(\pi_1^{-1}(\{f\}) \cap D\right) \right) \bigcup \left(\bigcup_{C \in \mathscr{C}} \left(\pi_1^{-1}(\{f\}) \cap C\right) \right) =$$

$$= \bigcup_{C \in \mathscr{C}} \left(\pi_1^{-1}(\{f\}) \cap C\right).$$

- Moreover, as $f \in U_C$ for every $C \in \mathscr{C}$, $\dim(\pi_1^{-1}(\{f\}) \cap C) = n - m$. Hence, for every $f \in \mathscr{P}_{(d)}$ we have that:

$$\dim\left(V_{\mathbb{A}}(f)\right) = \dim\left(\pi_1^{-1}(\{f\})\right) = \max\{\dim\left(\pi_1^{-1}(\{f\}) \cap C\right) \ : \ C \in \mathscr{C}\} = n - m.$$

Namely, for every $f \in U$, $V_{\mathbb{A}}(f)$ is a complete intersection variety of dimension $n - m$ and, hence, f is a "Suite Sécante" and the last claim follows. $\square$

We now consider a class of fields well-suited for guessing correct test sequences.

Definition 9 (Fields which are well-suited for CTS's guessing). *We say that a field K is well-suited for CTS's guessing in zero-dimensional varieties if it satisfies the following property: For every $R \in \mathbb{N}$ and every positive integer $n \in \mathbb{N}$, there is a zero-dimensional variety $V_R \subseteq \mathbb{A}^n(K)$ of degree R^n, given by polynomial equations of degree at most R and such that the following task may be performed with at most $O(n \log_2(R))$ arithmetic operations:*

$$\textbf{guess at random } x \in V_R.$$

Fields of characteristic zero are obviously well-suited for CTS's guessing. It is enough to consider the subset $\{1, \ldots, R\} \subset \mathbb{Z} \subseteq K$ and the variety $V_R := \{1, \ldots, R\}^n$. Many other fields satisfy a similar property.

Theorem 6.2. *If K is a field well-suited for CTS's guessing, the problem "Suite Sécante" with restricted inputs is in $\mathbf{BPP}_K$. Namely, let (d) be a degree list and let $\Omega \subseteq \mathscr{P}_{(d)}$ be a constructible subset of lists of polynomials. Let $U \subseteq \mathscr{P}_{(d)}$ be the Zariski open subset described in Theorem 6.1 of lists that are "Suites Sécantes". Assume that $\Omega \setminus (\Omega \cap U)$ has dimension at most $\dim(\Omega) - 1$. Then, there is an algorithm in $\mathbf{BPP}_K$ that solves "Suite Sécante" Problem with inputs in Ω, i.e.:*

Given as input $f \in \Omega$ and the data $\dim(\Omega)$ and $\deg_{\mathrm{lci}}(\Omega)$, the algorithm decides whether f is a "Suite Sécante" or not.

The running time of the algorithm in terms of arithmetic operations is at most:

$$O\left(\dim(\Omega)n\left((T + \log(\dim(\Omega)) + \log(d)) + Tn\log(\deg_{\mathrm{lci}}(\Omega))\right)\right).$$

where T is the maximum number of arithmetic operations required to evaluate at one point any list $f := (f_1, \ldots, f_m) \in \Omega$ and $d := \max\{d_1, \ldots, d_m\}$. The error probability is bounded by:

$$\frac{1}{\deg_{\mathrm{lci}}(\Omega)e^{6m\dim(\Omega)}}.$$

Proof. The algorithm is what we expected from the notion of correct test sequence and the results described in Section 5 above and especially Corollary 5.6.

Algorithm 6.3 (**"Suite Sécante" by evaluation of input polynomials at sampling points**). INPUT: *A list of polynomials $f := (f_1, \ldots, f_m) \in \Omega \subseteq \mathscr{P}_{(d)}^K$, and the values $\dim(\Omega)$ and $\deg_{\mathrm{lci}}(\Omega)$.*
eval:

- $L := 6\dim(\Omega)$
- $R := \max\{\lfloor (6(d+1))^2 \rfloor, \lfloor \deg_{\mathrm{lci}}(\Omega)^{\frac{2}{\dim(\Omega)}} \rfloor\}$.

As K is well-suited for CTS's, let $V_R \subseteq \mathbb{A}^n(K)$ be the corresponding zero-dimensional variety of degree R^n.
guess at random *a list $\mathbf{Q} := (x_1, \ldots, x_L) \in V_R^L$*
if $f(x_1) = f(x_2) = \cdots = f(x_L) = 0 \in K^m$, **then** OUPUT: **No.**
        else, OUTPUT: **Yes.**
fi
end

The running time of this algorithm (in terms of arithmetic operations) is of the following order:

- Time $O(Ln\left(\log(\dim(\Omega)) + \log(d) + \frac{\log(\deg_{\mathrm{lci}}(\Omega))}{\dim(\Omega)}\right))$ to generate L, R and to perform the guessing of the list $\mathbf{Q} := (x_1, \ldots, x_L) \in V_R^L$, since K is well-suited for CTS's.
- Time $O(LT)$ in order to evaluate the m polynomials involved in an input $f := (f_1, \ldots, f_m)$ at the L points of the list $\mathbf{Q}$.

As $L = 6\dim(\Omega)$ the total number of arithmetic operations is bounded by:

$$O\left(\dim(\Omega)n\left((T + \log(\dim(\Omega)) + \log(d)) + Tn\log(\deg_{\mathrm{lci}}(\Omega))\right)\right).$$

The probability of error is bounded by the probability that the list $(x_1, \ldots, x_L)$ obtained in the guessing step were a correct test sequence. Hence, according to Corollary 5.6, this error probability is bounded by:

$$(6.4) \qquad \frac{1}{\deg_{\mathrm{lci}}(\Omega)e^{\dim(\Omega)+(m-1)L}} \leq \frac{1}{\deg_{\mathrm{lci}}(\Omega)e^{6m\dim(\Omega)}}.$$

Thus, the algorithm is in $\mathbf{BPP}_K$ as wanted. $\qquad\qquad\square$

Corollary 6.4 (**"Suite Sécante" with dense input polynomials**). *If K is a field well-suited for CTS's guessing, the problem "Suite Sécante" is in $\mathbf{BPP}_K$ in the case of dense encoding of input polynomials. Namely, let $(d) := (d_1, \ldots, d_m)$ be a degree list and let $\Omega = \mathscr{P}_{(d)}^K$ be the class of all sequences of polynomials of respective degrees at most (d). Then, there is an algorithm in $\mathbf{BPP}_K$ that solves the following problem:*

Given as input $f \in \mathscr{P}_{(d)}^K$, the algorithm decides whether f is a "Suite Sécante" or not.

The running time of the algorithm in terms of arithmetic operations is at most:

$$O\left(nN_{(d)}^2\right),$$

where $N_{(d)}$ is the dimension of $\mathscr{P}^K_{(d)}$ as $K-$vector space and the error probability is bounded by

$$\frac{1}{e^{6mN_{(d)}}}.$$

Proof. The statement follows from the previous one since $N_{(d)} = \dim(\Omega)$ and $\deg_{\mathrm{lci}}(\Omega) = 1$. $\square$

Remark 6.5. In the case $m = 1$, "Suite Sécante" Problem becomes the usual *Zero Test Problem* and all our algorithms become in the class $\mathbf{RP}_K$. All the bounds remain in both corollaries for this case.

Remark 6.6. In the case Ω is the class of all sequences of polynomials evaluable by some straight-line program (or neural network with polynomial activation functions), the results also hold, just replacing $\dim(\Omega)$ and $\deg_{\mathrm{lci}}(\Omega)$ by the bounds described in Sections 2 and 3 of [KP, 96], for instance.

APPENDIX A. A REMARK ON BOUNDS FOR PROJECTIONS AND IMAGES OF CONSTRUCTIBLE SETS

As we observed in Propositions 2.25 and 2.26, one of the main differences is that the projection degree $\deg_\pi$ and the degree as a decomposition $\deg_{\mathrm{lci}}$ have a different behaviour with respect to linear images of constructible sets and algebraic varieties. Given a linear map $\ell : \mathbb{A}^n \longrightarrow \mathbb{A}^m$ and any constructible subset $C \subseteq \mathbb{A}^n$, the following inequalities hold:

$$\deg_z(\ell(C)) \leq \deg_\pi(\ell(C)) \leq \deg_\pi(C) \leq \deg_{\mathrm{lci}}(C).$$

Additionally, we have seen examples such that $\deg_{\mathrm{lci}}(\ell(C)) > \deg_{\mathrm{lci}}(C)$ in Proposition 2.25. For the sake of completeness, we exhibit in this Appendix some upper bounds either for the "defect" $\deg_{\mathrm{lci}}(\ell(C)) - \deg_z(\ell(C))$ and, in terms of extrinsic bounds, upper bounds for $\deg_{\mathrm{lci}}(\ell(C))$ based of the Effective Nullstellensatz of [Je, 05].

A.1. A first bound on the defect.
First of all, we see that the defect may be controlled by the degree of the constructible set of those points whose fibers do not have the generic fiber dimension. We use the same notations as in previous sections of this manuscript.

Lemma A.1. *Let $V \subseteq \mathbb{A}^n$ be an irreducible algebraic variety and $\ell : \mathbb{A}^n \longrightarrow \mathbb{A}^m$ be a linear mapping. Let $W := \overline{\ell(V)}^z$ be the Zariski closure of the image. Let $U \subseteq \mathbb{A}^m(K)$ be any Zariski open subset such that $U \cap W \neq \emptyset$ and:*

(A.1) $$\forall y \in W \cap U, \ \dim(\ell^{-1}(\{y\})) = \dim(V) - \dim(W).$$

Thus, $U \cap W \subseteq \ell(V)$. Additionally, let $U^c := \mathbb{A}^m \setminus U$ be the algebraic variety of those points whose fibers are not granted to have the appropriate dimension. Then, we have:

$$\deg_{\mathrm{lci}}(\ell(V)) - \deg_z(\ell(V)) \leq \deg_{\mathrm{lci}}(\ell(V) \cap U^c),$$

where $\dim(\ell(V) \cap U^c) \leq \dim(\ell(V)) - 1$. We also have:

$$\deg_{\mathrm{lci}}(\ell(V)) - \deg_z(\ell(V)) \leq \deg_{\mathrm{lci}}(\ell(V \cap \ell^{-1}(U^c))).$$

Proof. Let us first observe that for each $y \in U \cap W$, $\ell^{-1}(\{y\}) \neq \emptyset$. This holds because of Identity (A.1) since $\dim(V) - \dim(W) \geq 0$. Thus, $\ell(V) \cap U = W \cap U$ is a locally closed subset. Then, we have:

$$\ell(V) = (\ell(V) \cap U) \cup (\ell(V) \cap U^c) = (W \cap U) \cup (\ell(V) \cap U^c).$$

From the sub-additivity of $\deg_{\mathrm{lci}}$, we obtain:

$$\deg_{\mathrm{lci}}(\ell(V)) \leq \deg_{\mathrm{lci}}(W \cap U) + \deg_{\mathrm{lci}}(\ell(V) \cap U^c).$$

As $W \cap U$ is locally closed $\deg_{\mathrm{lci}}(W \cap U) = \deg(W) = \deg_z(\ell(C))$ and, hence, we have:

$$\deg_{\mathrm{lci}}(\ell(V)) - \deg_z(\ell(V)) \leq \deg_{\mathrm{lci}}(\ell(V) \cap U^c).$$

Since $W \cap U$ is Zariski dense in W, we deduce that $\overline{(\ell(V) \cap U^c)}^z$ is a closed proper subvariety of the irreducible variety W. Therefore,

$$\dim(\ell(V) \cap U^c) \leq \dim(\ell(V)) - 1.$$

Finally, let us observe that the following equality holds:

$$\ell(V \cap \ell^{-1}(U^c)) = \ell(V) \cap U^c.$$

For if $x \in \ell(V \cap \ell^{-1}(U^c))$ we obviously have that $x \in \ell(V) \cap U^c$. On the other hand, if $x \in \ell(V) \cap U^c$, and $y \in V$ is such that $\ell(y) = x$, we obviously have $y \in \ell^{-1}(U^c)$ and, hence, $x \in \ell(V \cap \ell^{-1}(U^c))$. $\square$

Lemma A.2. *Let $V \subseteq \mathbb{A}^n(K)$ be an irreducible algebraic variety of dimension r and degree D. Let $\ell : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$ be a linear map. Assume that the restriction $\ell\big|_V : V \longrightarrow \mathbb{A}^m(K)$ is dominating (and, hence, $m \leq r$). Let $\{X_1, \ldots, X_n\}$ be the variables associated to $\mathbb{A}^n$ and, accordingly, $\{Y_1, \ldots, Y_m\}$ the variables associated to $\mathbb{A}^m$. Then, there is a non-zero polynomial $q \in K[Y_1, \ldots, Y_m]$ such that the following properties hold:*

i) The polynomial $p := q \circ \ell \in K[X_1, \ldots, X_n]$ is also a non-zero polynomial and their respective degrees satisfy:

$$\deg(p) \leq \deg(q) \leq (n - r)(\deg(V) - 1).$$

ii) For every $y \in \mathbb{A}^m$ such that $q(y) \neq 0$, the dimension of the fiber satisfies:

$$\dim \ell\big|_V^{-1}(\{y\}) = \dim\left(V \cap \ell^{-1}(\{y\})\right) = r - m.$$

iii) Either $V \cap V_{\mathbb{A}}(q) = \emptyset$ or the dimension satisfies $\dim(V \cap V_{\mathbb{A}}(q)) = \dim(V) - 1$.

iv) The defect of $\ell(V)$ satisfies:

$$\deg_{\mathrm{lci}}(\ell(V)) - \deg_z(\ell(V)) \leq \deg_{\mathrm{lci}}(\ell(V \cap V_{\mathbb{A}}(q))),$$

where $\deg_z(\ell(V)) = 1$ since $\ell\big|_V$ is dominating onto $\mathbb{A}^m$.

Proof. First of all, as $\ell\big|_V$ is dominating, then $\ell : \mathbb{A}^n \longrightarrow \mathbb{A}^m$ is an onto linear mapping. Let $\ell_1, \ldots, \ell_m$ be the coordinate functions of ℓ. In particular, the ring $K[\ell_1, \ldots, \ell_m]$ is a ring of polynomials in m variables with coefficients in K. Up to a generic choice of a linear change of coordinates in $\mathbb{A}^n$ we may assume that $\ell_1 = X_1, \ldots, \ell_m = X_m$. Then, we proceed in our proof as if ℓ were the canonical projection $\ell := \pi_m : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$ onto the first m coordinates of a point in $\mathbb{A}^n(K)$. Thus, let $I(V) \in \mathrm{Spec}(K[X_1, \ldots, X_n])$ be the prime ideal associated to V. As $\ell\big|_V$ is dominating, we would have the following ring extension:

$$\ell^* : K[X_1, \ldots, X_m] \hookrightarrow K[V] := K[X_1, \ldots, X_n]/I(V).$$

Let us consider the multiplicative system $S := K[X_1, \ldots, X_m] \setminus \{0\}$ and let $F := K(X_1, \ldots, X_m)$ be the quotient field of $K[X_1, \ldots, X_m]$. As $I(V) \cap K[X_1, \ldots, X_m] = (0)$ we also have the following ring extension:

$$S^{-1}\ell^* : F \hookrightarrow F[V] := S^{-1}K[V] = F[X_{m+1}, \ldots, X_n]/\mathfrak{p},$$

where $\mathfrak{p} = S^{-1}I(V)$.

As $\ell\big|_V$ is dominating, the Theorem on the Dimension of the Fibers yields that the generic dimension of a fiber $(\ell\big|_V)^{-1}(\{x\})$ has dimension $r - m$. Hence, the Krull dimension satisfies:

$$\dim\left(F[V]\right) = \dim\left(F[X_{m+1}, \ldots, X_n]/\mathfrak{p}\right) = r - m.$$

As K is an infinite field, so does F and there are generically many matrices $A \in \mathscr{M}_{n-m}(K)$ such that the following linear change of coordinates:

$$\begin{pmatrix} Y_{m+1} \\ \vdots \\ Y_n \end{pmatrix} = A \begin{pmatrix} X_{m+1} \\ \vdots \\ X_n \end{pmatrix},$$

puts the variables $\{Y_{m+1}, \ldots, Y_n\}$ in Noether position with respect to $\mathfrak{p}$, i.e. the following is an integral ring extension:

$$F[Y_{m+1}, \ldots, Y_r] \hookrightarrow F[V] := F[Y_{m+1}, \ldots, Y_n]/\mathfrak{p},$$

where we also call $\mathfrak{p}$ the transformation of $\mathfrak{p}$ under such linear change of coordinates. Then, for every j, $r + 1 \leq j \leq n$, there is a monic polynomial $h_j \in F[Y_{m+1}, \ldots, Y_r][T]$ of positive degree with respect to the variable T (i.e. $\delta_j = \deg_T(h_j) \geq 1$), such that:

$$h_j(Y_j) \in \mathfrak{p}, \ r + 1 \leq j \leq n.$$

As $\mathfrak{p}$ is a prime ideal, we may assume that h_j is irreducible. For every j, $r + 1 \leq j \leq n$, there is a primitive polynomial $H_j \in K[X_1, \ldots, X_m, Y_{m+1}, \ldots, Y_r][T]$ such that h_j and H_j are associated

in the ring $F[Y_{m+1}, \ldots, Y_r][T]$. Namely, for every j, $r + 1 \le j \le n$, there is a polynomial of the following form:

$$H_j := e_{\delta_j}^{(j)}(X_1, \ldots, X_m)T^{\delta_j} + \sum_{k=0}^{\delta_j - 1} a_k^{(j)}(X_1, \ldots, X_m, Y_{m+1}, \ldots, Y_r)T^k,$$

where $e_{\delta_j}^{(j)} \in K[X_1, \ldots, X_m] \setminus \{0\}$, $a_k^{(j)} \in K[X_1, \ldots, X_m, Y_{m+1}, \ldots, Y_r]$ and the following properties hold:

- Every H_j is a primitive polynomial,
- For every j, $r+1 \le j \le n$, the polynomial H_j is irreducible in $K[X_1, \ldots, X_m, Y_{m+1}, \ldots, Y_r][T]$ and the following equality holds:

$$h_j := \left(e_{\delta_j}^{(j)}\right)^{-1} H_j,$$

- For every j, $r + 1 \le j \le n$, $H_j(Y_j) \in \mathfrak{p}$, $e_{\delta_j}^{(j)} \notin \mathfrak{p}$.

The last property is a consequence of the fact that $e_{\delta_j}^{(j)} \neq 0$ and $\mathfrak{p}$ is a prime ideal. Let us then define the following non-zero polynomial:

$$q := \prod_{j=r+1}^{n} e_{\delta_j}^{(j)} \in K[X_1, \ldots, X_m] \setminus \{0\}.$$

Observe that, as $I(V)$ was a prime ideal, then $q \notin I(V)$. We then define the following rings and locally closed sets:

i) The distinguished open subset of $\mathbb{A}^m$ given by:

$$D(q) := \{x \in \mathbb{A}^m \; : \; q(x) \neq 0\}.$$

ii) The non-empty Zariski open subset V_q of V given by the following identity:

$$V_q := \{\zeta := (x, y, u) \in \mathbb{A}^m \times \mathbb{A}^{r-m} \times \mathbb{A}^{n-r} \; : \; \zeta \in V, \; q(x) \neq 0\}.$$

iii) The ring of regular functions defined on $D(q)$, given as the localization on the multiplicative system defined by q:

$$K[D(q)] := K[X_1, \ldots, X_m]_q.$$

iv) The ring of regular functions define on V_q, given as:

$$K[V_q] := K[X_1, \ldots, X_m]_q[Y_{m+1}, \ldots, Y_n]/\mathfrak{q},$$

where $\mathfrak{q}$ is, at the same time, the extension of $I(V)$ to $K[X_1, \ldots, X_m]_q[Y_{m+1}, \ldots, Y_n]$ and the contraction of $\mathfrak{p}$ to the same ring.

As, for every j, $r + 1 \le j \le n$, $h_j \in K[X_1, \ldots, X_m]_q[Y_{m+1}, \ldots, Y_r][T]$ and $h_j(Y_j) \in \mathfrak{p}$, the following is an integral ring extension:

(A.2) $K[D(q)][Y_{m+1}, \ldots, Y_r] \hookrightarrow K[V_q] := K[X_1, \ldots, X_m]_q[Y_{m+1}, \ldots, Y_n]/\mathfrak{q}.$

From this integral equation we immediately conclude the following first Claim:

(A.3) $\forall x \in D(q), \; \ell\big|_V^{-1}(\{x\}) \neq \emptyset.$

In fact, recalling that $\ell = \pi_m$ is a projection, the integral ring extension of (A.2) implies that the following map is onto:

$$\pi : \quad \begin{matrix} V_q & \longrightarrow & D(q) \times \mathbb{A}^{r-m} \\ \zeta = (x, y, u) & \longmapsto & (x, y). \end{matrix}$$

Let us now consider the following projection maps:

$$\Pi_j : \quad \begin{matrix} V_q & \longrightarrow & \mathbb{A}^{r+1} \\ \zeta := (x, y, u) & \longmapsto & (x, y, u_j), \end{matrix}$$

where $x \in D(q)$, $y \in \mathbb{A}^{r-m}$ and $u := (u_{r+1}, \ldots, u_n) \in \mathbb{A}^{n-r}$. We now prove the following Claim:

Claim. *With these notations and assumptions, $\Pi_j(V_q)$ is a hyper-surface in $D(q) \times \mathbb{A}^{r-m+1}$ of degree at most $\deg(V)$ and its minimal equation is the polynomial H_j introduced above, whose total degree satisfies $\deg(H_j) \le \deg(V)$.*

Proof of the Claim. It is clear that $\Pi_j(V_q) \subseteq D(q) \times \mathbb{A}^{r-m+1}$. Moreover, if $\lambda : \mathbb{A}^{r+1} \longrightarrow \mathbb{A}^r$ is the projection that forgets the last coordinate, we have that:

$$\lambda \circ \Pi_j = \pi,$$

where π is the onto map defined above. Hence, we conclude that:

$$\dim(\Pi_j(V_q)) \geq \dim(\lambda(\Pi_j(V_q))) \geq \dim(\pi(V_q)) = \dim(D(q) \times \mathbb{A}^{r-m}) = r.$$

On the other hand, the polynomial $H_j \in K[X_1, \dots, X_m, Y_{m+1}, \dots, Y_r][T]$ is a non-zero polynomial and we have:

$$\Pi_j(V_q) \subseteq \{(x, y, u_j) \in \mathbb{A}^{r+1} \ : \ q(x) \neq 0, H_j(x, y, u_j) = 0\}.$$

By Krull's Hauptidealsatz, the co-dimension of $\Pi_j(V_q)$ is at least 1 and we have proved the following inequality:

$$\dim(\Pi_j(V_q)) = r.$$

Thus, $\overline{\Pi_j(V_q)}^z$ is a hyper-surface in $\mathbb{A}^{r+1}$. It is irreducible since V was irreducible and, hence, there is an irreducible polynomial $g_j \in K[X_1, \dots, X_m, Y_{m+1}, \dots, Y_r, Y_j]$ such that $I(\overline{\Pi_j(V_q)}^z) = (g_j)$. As H_j vanishes on $\Pi_j(V_q)$ we then have $g_j \mid H_j$ and, as H_j was primitive and irreducible, we conclude that $g_j = H_j$ up to some constant in $K \setminus \{0\}$.

Finally, the degrees satisfy the following equalities and inequalities:

$$\deg(V) = \deg(V_q) \geq \deg_z(\Pi_j(V_q)) = \deg(\overline{\Pi_j(V_q)}^z) = \deg(g_j) = \deg(H_j).$$

∎

From this claim we conclude that for every j, $r + 1 \leq j \leq n$, we have:

$$\deg(e_j^{(\delta_j)}) + \delta_j \leq \deg(H_j) \leq \deg(V).$$

Thus, as $\delta_j \geq 1$ for every j, we have:

$$(A.4) \qquad \deg(q) = \sum_{j=r+1}^{n} \deg(e_j^{(\delta_j)}) \leq \sum_{j=r+1}^{n} (\deg(V) - 1) \leq (n - r)(\deg(V) - 1).$$

Combining this last inequality with the statement in Equation (A.3) and the previous Lemma we conclude that $q \in K[X_1, \dots, X_m] \setminus \{0\}$ is the polynomial claimed at the statement. $\square$

Remark A.3. This last Lemma explains the existence of the defect in the Example exhibited to prove Claim iv) of Proposition 2.25. There was a quadric hyper-surface in $\mathbb{A}^3(\mathbb{C})$ of degree 2 given by the following identity:

$$W' := \{(x, y, z) \in \mathbb{C}^3 \ : \ xz + (y^2 - 1) = 0\}.$$

We consider the canonical projection $\ell = \pi_2 : \mathbb{A}^3 \longrightarrow \mathbb{A}^2$. The polynomial q cited in the previous Lemma is the leading coefficient of the quadratic polynomial defining W', i.e. $q := Z$. Its total degree satisfies:

$$\deg(q) = 1 \leq (\mathrm{codim}(W'))(\deg(W') - 1) = (3 - 2)(2 - 1) = 1.$$

The defect is then bounded by:

$$\deg_{\mathrm{lci}}(\pi_2(W')) - \deg_z(\pi_2(W')) \leq \deg_{\mathrm{lci}}(\pi_2(W' \cap V_{\mathbb{A}}(q))).$$

However, $W' \cap V_{\mathbb{A}}(q)$ is a pair of lines given by:

$$W' \cap V_{\mathbb{A}}(q) = \{(x, y, z) \in W' \ : \ z = 0\} = \{(x, y, 0) \in \mathbb{A}^3 \ : \ y^2 - 1 = 0\}.$$

Hence, $\pi_2(W' \cap V_{\mathbb{A}}(q)) = \{(x, y) \ : \ y \in \{\pm 1\}\}$ is an algebraic variety and, hence,

$$\deg_{\mathrm{lci}}(\pi_2(W' \cap V_{\mathbb{A}}(q))) = \deg(\pi_2(W' \cap V_{\mathbb{A}}(q))) = 2.$$

We have already seen that $\deg_{\mathrm{lci}}(\pi_2(W')) = 3$ and $\deg_z(\pi_2(W')) = 1$. In particular, the bound in the previous Lemma is optimal in this example since:

$$\deg_{\mathrm{lci}}(\pi_2(W')) - \deg_z(\pi_2(W')) = 3 - 1 = 2 = \deg_{\mathrm{lci}}(\pi_2(W' \cap V_{\mathbb{A}}(q))).$$

This does not mean that the upper bound in Claim iv) of the previous Lemma is always optimal, but at least it is optimal in some examples.

A.2. **An extrinsic bound for the degree of a projection, based on the Effective Null-stellensatz.** We revise Proposition 2.25. Here we show a coarse and syntactical upper bound for the LCI-degree of the image $\pi(V)$ of some irreducible algebraic variety V with respect to the canonical projection. The bound is syntactical since we just take into account a syntactical description of V. The method we choose is based on the Effective Nullstellensatz. This simply means that $LCI-$ degree is "controlled" under linear images in terms of syntactical descriptions of the domain. Although we could have used either [Kol, 88] or [So, 99], we preferred to choose the bounds of [Je, 05]. We also use [Mu, 87] for the degree bounds, although other may also be used.

As above, K is an algebraically closed field.

Theorem A.4. *Let $V \subseteq \mathbb{A}^n(K)$ be an irreducible algebraic variety of dimension r. Let m be an integer such that $m \leq n$. Assume that there are polynomials $g_1, \ldots, g_s \in K[X_1, \ldots, X_n]$ of degrees $d_i := \deg(g_i)$, $1 \leq i \leq r$, such that $V = V_{\mathbb{A}}(g_1, \ldots, g_s)$ and the following inequalities hold:*

$$d_1 \geq d_2 \geq \ldots \geq d_s.$$

Let us consider the following quantity:

$$N := N(d_1, \ldots, d_s, n, r) := \begin{cases} \prod_{i=1}^s d_i & \text{if } s \leq n - m \\ 2d_s \left(\prod_{i=1}^{n-m-1} d_i \right) - 1 & \text{if } s > n - m \end{cases}$$

Let us define the following quantities:

$$\widetilde{N} := \binom{N + (n - m)}{n - m},$$

$$M := \sum_{i=1}^s \binom{N - d_i + (n - m)}{(n - m)},$$

and

$$\mathscr{N}' := \min\{N, M + 1\}.$$

Let $\pi : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$ be the canonical projection that forgets the last $n - m$ variables and let $W := \overline{\pi(V)}^z$ be the Zariski closure of $\pi(V)$ in $\mathbb{A}^m(K)$. Then, we have:

$$\deg_{\mathrm{lci}}(\pi(V)) \leq \deg(V) (2d_1)^{\dim(W)} (\mathscr{N}')^{\dim(W)+1}.$$

Proof. First of all, for each monomial exponent $\nu = (\nu_1, \ldots, \nu_k) \in \mathbb{N}^k$, we denote its degree by $|\nu| := \nu_1 + \cdots + \nu_k \in \mathbb{N}$. Next, for each i, $1 \leq i \leq s$, we are going to introduce a new set of variables:

$$\underline{Z}^{(i)} := \{ Z_\mu^{(i)} \ : \ \mu \in \mathbb{N}^{n-m}, |\mu| \leq N - d_i \},$$

ordered by the "degree+lexicographic" monomial ordering, and the polynomial with generic coefficients:

$$F_i := \sum_{\mu \in \mathbb{N}^{n-m}, |\mu| \leq N-d_i} Z_\mu^{(i)} X_{m+1}^{\mu_{m+1}} \cdots X_n^{\mu_n}.$$

Note that the number of variables involved in $\underline{Z}^{(i)}$ (and also the number of generic coefficients of F_i) is given by:

$$M_i := \binom{N - d_i + (n - m)}{(n - m)}.$$

Also, for each i, $1 \leq i \leq s$, we rewrite the polynomials $g_1, \ldots, g_s$ as:

$$g_i := \sum_{\nu \in \mathbb{N}^{n-m}, \ |\nu| \leq d_i} h_\nu^{(i)}(X_1, \ldots, X_m) X_{m+1}^{\nu_{m+1}} \cdots X_n^{\nu_n}.$$

Finally, we consider the column vector:

$$\mathbf{1} := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in K^{\widetilde{N}},$$

that encodes the coefficients of $1 \in K[X_{m+1}, \ldots, X_n]$ using a polynomial of degree at most $\widetilde{N}$, with respect to "degree+lexicographic" monomial order in $K[X_{m+1}, \ldots, X_n]$. The number of coordinates in $\mathbf{1}$ is given by the following quantity:

$$\widetilde{N} := \binom{N + (n - m)}{n - m}.$$

Now, we consider the following sum:

$$\sum_{i=1}^{s} F_i g_i \in K[\underline{Z}^{(1)}, \ldots, \underline{Z}^{(s)}, X_1, \ldots, X_m][X_{m+1}, \ldots, X_n].$$

Taking $R := K[\underline{Z}^{(1)}, \ldots, \underline{Z}^{(s)}, X_1, \ldots, X_m]$, the coefficients of this sum as polynomials in $R[X_{m+1}, \ldots, X_n]$ can be represented as a matrix product:

$$A(X_1, \ldots, X_m) \begin{pmatrix} \underline{Z}^{(1)} \\ \vdots \\ \underline{Z}^{(s)} \end{pmatrix}.$$

The coefficients of $A(X_1, \ldots, X_m)$, being those of the list:

(A.5) $\mathscr{H} := \{ h_\nu^{(i)} \ : \ \nu \in \mathbb{N}^{n-m}, |\nu| \leq d_i, \ 1 \leq i \leq s \},$

have all of them degree at most $D := d_1$. Moreover, the matrix $A(X_1, \ldots, X_m)$ is in

$$\mathscr{M}_{\widetilde{N} \times M}(K[X_1, \ldots, X_m]),$$

where the number of rows and columns are determined by the following rules:

- The number of rows is the quantity:

$$\widetilde{N} := \binom{N + (n - m)}{n - m}.$$

- The number of columns is given by the quantity:

$$M := \sum_{i=1}^{s} \binom{N - d_i + (n - m)}{n - m}.$$

We finally consider the system of equations:

(A.6) $\mathscr{S}(X_1, \ldots, X_m) \equiv \left\{ A(X_1, \ldots, X_m) \begin{pmatrix} \underline{Z}^{(1)} \\ \underline{Z}^{(2)} \\ \vdots \\ \underline{Z}^{(s)} \end{pmatrix} = \mathbf{1} \right\}.$

We observe that the following two claims are equivalent for every $x = (x_1, \ldots, x_m) \in \mathbb{A}^m(K)$:

   i) The fiber $\pi^{-1}(\{x\}) \cap V \neq \emptyset$,
   ii) The system of linear equations $\mathscr{S}(x_1, \ldots, x_m)$, obtained by specializing the variables X_i into the coordinates x_i, is *inconsistent*.

Now, we follow the main idea of [Mu, 87] which works in any field of any characteristic. Mulmuley's trick goes as follows. First, let $W := \overline{\pi(V)}^z$ be the Zariski closure of $\pi(V)$ in $\mathbb{A}^m(K)$ and let us consider the following two matrices:

$A(X_1, \ldots, X_m) \in \mathscr{M}_{\widetilde{N} \times M}(K[W]), B(X_1, \ldots, X_m) := (X_1, \ldots, X_m \mid \mathbf{1}) \in \mathscr{M}_{\widetilde{N} \times (M+1)}(K[W]).$

Then, we consider the following two square and symmetric matrices:

$$A^*(X_1, \ldots, X_m) := \begin{pmatrix} A(X_1, \ldots, X_m) & 0 \\ 0 & A(X_1, \ldots, X_m)^T \end{pmatrix} \in \mathscr{M}_{\widetilde{N}+M}(K[W]),$$

$$B^*(X_1, \ldots, X_m) := \begin{pmatrix} B(X_1, \ldots, X_m) & 0 \\ 0 & B(X_1, \ldots, X_m)^T \end{pmatrix} \in \mathscr{M}_{\widetilde{N}+M+1}(K[W]).$$

Moreover, the ranks satisfy the following equalities for all $x \in \mathbb{A}^m(K)$:

$$\operatorname{rank}(A^*(x)) = 2 \operatorname{rank}(A(x)), \operatorname{rank}(B^*(x)) = 2 \operatorname{rank}(B(x)).$$

For every $x \in W$, the system of linear equations $\mathscr{S}(x)$, described in (A.6), is inconsistent if and only if $\operatorname{rank}(A^*(x)) \neq \operatorname{rank}(B^*(x))$.

As $A^*(\underline{X})$ and $B^*(\underline{X})$ are symmetric, their ranks depend on the order of 0 as root of their respective characteristic polynomials. We, thus, consider their characteristic polynomials modulo $I(W)$:

- The characteristic polynomial of $A^*(X_1, \ldots, X_m)$:

$$\chi_A(T) := T^{\widetilde{N}+M} + a_{\widetilde{N}+M-1} T^{\widetilde{N}+M-1} + \cdots + a_1 T + a_0 \in K[W][T],$$

  where the coefficients a_i are of the form $A_i + I(W)$, where $A_i \in K[X_1, \ldots, X_m]$.
- Similarly, we have the characteristic polynomial of $B^*(X_1, \ldots, X_m)$:

$$\chi_B(T) := T^{\widetilde{N}+M+1} + b_{\widetilde{N}+M} T^{\widetilde{N}+M} + \cdots + b_1 T + b_0 \in K[W][T].$$

  We also conclude that the coefficients $b_i \in K[W]$ are of the form $B_i + I(W)$, where $B_i \in K[X_1, \ldots, X_m]$.

Let $\mathscr{N} := \min\{\widetilde{N}, M\}$ and $\mathscr{N}' := \min\{\widetilde{N}, M+1\}$ be the minimum between the number of rows and columns of $A(X_1, \ldots, X_m)$ and $B(X_1, \ldots, X_m)$. For every $x \in W$ we have:

$$\operatorname{rank}(A^*(x)) \leq 2\mathscr{N}, \ \operatorname{rank}(B^*(x)) \leq 2\mathscr{N}'.$$

Thus, the order of 0 in $\chi_A(T)$ and $\chi_B(T)$ satisfy in $K[W]$:

$$ord_0(\chi_A) \geq \widetilde{N} + M - 2\mathscr{N}, \ ord_0(\chi_B) \geq \widetilde{N} + M + 1 - 2\mathscr{N}'.$$

In particular, the following equalities hold:

$$\chi_A(T) := T^{\widetilde{N}+M} + a_{\widetilde{N}+M-1} T^{\widetilde{N}+M-1} + \cdots + a_{\widetilde{N}+M-2\mathscr{N}} T^{\widetilde{N}+M-2\mathscr{N}} \in K[W][T],$$

and

$$\chi_B(T) := T^{\widetilde{N}+M+1} + b_{\widetilde{N}+M} T^{\widetilde{N}+M} + \cdots + b_{\widetilde{N}+M+1-2\mathscr{N}'} T^{\widetilde{N}+M+1-2\mathscr{N}'} \in K[W][T].$$

As the coordinates of the matrices $A^*(X_1, \ldots, X_m)$ and $B^*(X_1, \ldots, X_m)$ are in the class $\mathscr{H} \cup \{0, 1\}$, where $\mathscr{H}$ is the list of polynomials introduce in Identity (A.5), and the polynomials in $\mathscr{H}$ have degree at most $D := d_1$, we conclude:

- For each i, $1 \leq i \leq 2\mathscr{N}$, there is a polynomial $A_{\widetilde{N}+M-i}(X_1, \ldots, X_m) \in K[X_1, \ldots, X_m]$ of degree at most $d_1 i$ such that $A_{\widetilde{N}+M-i} + I(W) = a_{\widetilde{N}+M-i}$.
- For each j, $1 \leq j \leq 2\mathscr{N}'$, there is a polynomial $B_{\widetilde{N}+M+1-j}(X_1, \ldots, X_m) \in K[X_1, \ldots, X_m]$ of degree at most $d_1 j$ such that $B_{\widetilde{N}+M+1-j} + I(W) = b_{\widetilde{N}+M+1-j}$.

For each $x \in W$, as $\operatorname{rank}(B^*(x)) = 2\operatorname{rank}(B(x)) \geq 2\operatorname{rank}(A(x)) = \operatorname{rank}(A^*(x))$, the system of linear equations $\mathscr{S}(x)$ of (A.6) is inconsistent if and only if there exists $k \in \{0, \ldots, \mathscr{N}\}$ such that:

$$\operatorname{rank}(A^*(x)) = 2k, \ \operatorname{rank}(B^*(x)) = 2(k+1).$$

Transforming this rank equalities into order of 0 as zero of χ_A and χ_B, for each $x \in W$, system $\mathscr{S}(x)$ of (A.6) is inconsistent if and only if there is k, $0 \leq k \leq \mathscr{N}$, such that $x \in R_k$, where R_k is the class given by the following intersection:

$$R_k := \{x \in W \ : \ ord_0(\chi_{A(x)}(T)) = \widetilde{N}+M-2k\} \cap \{x \in W \ : \ ord_0(\chi_{B(x)}(T)) = \widetilde{N}+M+1-2(k+1)\}.$$

In terms of polynomial equations and equalities, this may be written as follows:

$$R_k := \mathcal{A}_k \cap \mathcal{B}_k,$$

where

$$\mathcal{A}_k := \{x \in W \ : \ A_i(x) = 0, \widetilde{N} + M - 2\mathscr{N} \leq i \leq \widetilde{N} + M - 2k - 1, A_{\widetilde{N}+M-2k}(x) \neq 0\},$$

and

$$\mathcal{B}_k := \{x \in W \ : \ B_j(x) = 0, \widetilde{N}+M+1-2\mathscr{N}' \leq j \leq \widetilde{N}+M+1-2(k+1)-1, B_{\widetilde{N}+M+1-2(k+1)}(x) \neq 0\}.$$

In particular, the following equality holds:

$$\pi(V) := \bigcup_{k=0}^{\mathscr{N}-1} R_k,$$

Moreover, each R_k is a locally closed set given as the intersection of W with open sets and hyper-surfaces given by polynomial equations of degree at most:

$$\max\left(\{\deg(A_i) \ : \ \widetilde{N} + M - 2\mathscr{N} \leq i\} \cup \{\deg(B_j) \ : \ \widetilde{N} + M + 1 - 2\mathscr{N}' \leq j\}\right).$$

In particular, R_k is a locally closed set given by a Zariski open subset of W with hyper-surfaces of degree at most $2\mathscr{N}'$. From Proposition 3.1, we conclude:

$$\deg(R_k) \leq \deg(W)\left(2\mathscr{N}'d_1\right)^{\dim(W)}.$$

As the degree of constructible sets is sub-additive, we, then, conclude:

$$\deg_{\mathrm{lci}}(\pi(V)) \leq \deg(W)\mathscr{N}\left(2\mathscr{N}'d_1\right)^{\dim(W)}.$$

Applying Proposition 2.12 to the previous inequality we obtain the inequality of the statement.
$\square$

APPENDIX B. OTHER EXPONENTIAL LENGTH CORRECT TEST SEQUENCES IN THE MATHEMATICAL LITERATURE

B.1. Correct Test Sequences and determinantal varieties.
Let $m, n \in \mathbb{N}$ be two positive integers with $m \geq n$. We consider the *determinantal varieties* in the space $\mathscr{M}_{m \times n}(K)$ of matrices $m \times n$ with entries in an algebraically closed field K:

$$\Sigma_r := \{M \in \mathscr{M}_{m \times n}(K) \ : \ corank(M) \geq r\}.$$

It is well-known that Σ_r is an algebraic variety, given by homogeneous polynomial equations (and, hence, also a projective variety), and its co-dimension in $\Omega := \mathscr{M}_{m \times n}(K)$ is given by the following identity:

$$\mathrm{codim}_\Omega(\Sigma_r) = \dim\left(\mathscr{M}_{m \times n}(K)\right) - \dim\left(\Sigma_r\right) = (m - r)(n - r).$$

Then, for every correct test sequence $\mathbf{Q} := (x_1, \ldots, x_L) \in \mathbb{A}^{nL}$ for $\Omega := \mathscr{M}_{m \times n}(K)$ with respect to Σ_r we have (see Proposition 4.12):

$$L := \sharp(\mathbf{Q}) \geq (m - r)(n - r).$$

Indeed, we proved in 5.1 that there are correct test sequences for Ω with respect to Σ_r of length $O((m - r)(n - r))$.
Similarly, for $r < s$, we would have:

$$\mathrm{codim}_{\Sigma_r}\left(\Sigma_s\right) = (r - s)(m + n - (r + s)).$$

Thus, for every correct test sequence $\mathbf{Q} \subseteq \mathbb{A}^{nL}$ for Σ_r with respect to Σ_s we also have:

$$\sharp(\mathbf{Q}) \geq (r - s)(m + n - (r + s)).$$

B.2. Correct Test Sequences and Kakeya Sets.
The notion of Kakeya sets in the case of finite fields comes from [Wo, 99]. An exponential lower bound for the cardinal of Kakeya sets in the case of finite fields was established in [Dv, 09]. See also [Tao, 14] for other developments. In [Tao, 14], Tao claims: *"There is no known proof of the finite field Kakeya conjecture that does not go through the polynomial method"*. Here, we explain this phenomenon by observing that *Kakeya sets are correct test sequences for certain constructible sets made by polynomials*. In fact, most of the methods used in what is known as *"the Polynomial Method"* are simply the use of a correct test sequence adapted to some class (typically constructible sets) of polynomials. Nevertheless, we also prove that the converse is false: In Corollary B.3 we prove that for small and positive ε and degrees smaller than $q^{1-\varepsilon} - 1$, most correct test sequences are not Kakeya sets. Additionally, we do not know of any correct test sequence for polynomials of degree $q - 1$ which are not Kakeya sets.
Here, we just prove a small generalization of the main outcome of [Dv, 09] by using the correct test sequence terminology. Notations are the same as in previous Sections. For a projective point $v \in \mathbb{P}_{n-1}(K)$ we denote by $K\langle v \rangle \subseteq K^n$ the vector subspace of dimension 1 of K^n generated by any non-zero representant $\widetilde{v} \in K^n \setminus \{0\}$ of the projective point $v \in \mathbb{P}_{n-1}(K)$.

Definition 10 ($q-$**Kakeya set with directions in a zero-dimensional projective variety**)**.** *With these notations, let $V \subseteq \mathbb{P}_{n-1}(K)$ be a zero-dimensional projective variety and $q \in \mathbb{N}$ a positive integer. A $q-$Kakeya set with directions in V is a finite subset $E \subseteq \mathbb{A}^n(K)$ such that the following property holds:*
For every direction $v \in V$, there is a point $x \in E$ such that the affine line $\rho(x,v) := x + K\langle v \rangle$ satisfies

$$\sharp(E \cap \rho(x,v)) \geq q.$$

When $\kappa = \mathbb{F}_q$ is a finite field with q elements, we denote by $\mathbb{F}_q\langle v \rangle$ the $\mathbb{F}_q-$vector space generated by v. Usual Kakeya sets are then defined as follows:

Definition 11 (**Usual Kakeya sets over finite fields**)**.** *Let $\mathbb{F}_q$ be a finite field of cardinal q. A finite subset $E \subseteq \mathbb{A}^n(\mathbb{F}_q)$ is called a Kakeya set if the following property holds:*
For every projective point $v \in \mathbb{P}_{n-1}(\mathbb{F}_q)$, there exists $x \in E$ such that the $\mathbb{F}_q-$rational points of the affine line $\rho(x,v) \subseteq \mathbb{A}^n(\mathbb{F}_q)$ determined by x and v is totally included in E. Namely, such that the following holds:

$$\rho(x,v) := x + \mathbb{F}_q\langle v \rangle := \{x + tv \; : \; t \in \mathbb{F}_q\} \subseteq E.$$

Recall that the Hilbert function of a projective variety $V \subseteq \mathbb{P}_{n-1}(K)$ is a function $\chi_V : \mathbb{N} \longrightarrow \mathbb{N}$ given by the following identity for all $m \in \mathbb{N}$:

$$\chi_V(m) := \dim_K(H_m(X_1,\ldots,X_n)/I_m(V)) = \dim_K(H_m(X_1,\ldots,X_n)) - \dim_K(I_m(V)),$$

where:

- $\dim_K$ means the dimension as $K-$vector spaces,
- $H_m(X_1,\ldots,X_n)$ is the vector space spanned by all homogeneous polynomials of degree m in the set of variables $\{X_1,\ldots,X_n\}$ with coefficients in K and,
- $I_m(V)$ is the vector subspace of polynomials in $H_m(X_1,\ldots,X_n)$ that vanish on the projective points of V.

Hilbert function is known to be a polynomial function of degree equal to the Krull dimension of V as projective variety. Namely, there is a unique polynomial $q \in \mathbb{Z}[T]$ of degree equal to $dim(V)$ and an integer R such that:

$$\chi_V(m) = q(m), \; \forall m \geq R$$

The polynomial q is called Hilbert's polynomial of V and the minimum of those R such that χ_V and q agree is called the *regularity of the Hilbert function of V*.
The next statement proves that $q-$Kakeya sets are correct test sequences and, hence, we have a lower bound for its cardinal based on Proposition 4.12.

Proposition B.1. *With the previous notations and assumptions, given a zero-dimensional projective variety $V \subseteq \mathbb{P}_{n-1}(K)$, for every $q-$Kakeya set E with directions in V we have that:*

$$\sharp(E) \geq \chi_V(d), \; \forall d \in \mathbb{N}, \; d \leq q - 1.$$

Moreover, if R is the regularity of the Hilbert function of V and if $q - 1 \geq R$ we also have:

$$\sharp(E) \geq \sharp(V) = \deg(V).$$

On the other hand, $q-$Kakeya sets with directions in $V \subseteq \mathbb{P}_{n-1}(K)$ with cardinal $(q-1)\deg(V)+1$ do exist.

Proof. Let $\mathbb{A}^N(K)$ be the affine space over K given as the $K-$vector space $P_d := P_d(X_1,\ldots,X_n)$ of all polynomials of degree at most d with coefficients in K, $\mathbb{A}^N(K) := P_d$, where $N := N_d$. For every polynomial $f \in P_d(X_1,\ldots,X_n)$, we consider its decomposition in homogeneous components:

$$f = f_m + \cdots + f_0,$$

where $f_i \in H_i(X_1,\ldots,X_n)$ and $f_m \neq 0$.
Let us denote by $LHC(f) \in P_d$ (leading homogeneous component) the homogeneous component of higher degree of f, i.e. $LHC(f) = f_m$. For every m, $0 \leq m \leq d$, let us define the following constructible subsets of $P_d := P_d(X_1,\ldots,X_n)$:

$$\Omega_m := \{f \in P_d \; : \; \deg(f) = m\},$$

$$\Sigma_m := \{f \in \Omega_m \; : \; LHC(f) \in I_m(V)\},$$

where $I_m(V)$ is the vector space spanned by all homogeneous polynomials of degree m that vanish on V. We finally define:

$$\Omega := \bigcup_{m=0}^{d} \Omega_m = P_d,$$

and

$$\Sigma := \bigcup_{m=0}^{d} \Sigma_m \subseteq \Omega.$$

Claim. *With these notations, the following properties hold:*

    i) *If E is a $q-$Kakeya set with directions in V, then E is a correct test sequence for Ω with respect to Σ.*

    ii) *Let us define $d_0 := \max\{m \in \mathbb{N} \ : \ m \leq d, \ I_m(V) \neq \{0\}\}$. Then, either $d_0 = d$ or $\Sigma_m = \{0\}$ for all $m \leq d$.*

    iii) *The dimension of the constructible sets Ω and Σ are given by the following identities:*

$$\dim(\Omega) := \sum_{i=0}^{d} \dim_K(H_i(X_1, \ldots, X_n)) = \binom{d+n}{n},$$

$$\dim(\Sigma) := \begin{cases} \dim_K(I_d(V)) + \sum_{i=0}^{d-1} \dim_K(H_i(X_1, \ldots, X_n)), & \text{if } I_d(V) \neq \{0\} \\ 0, & \text{otherwise} \end{cases}$$

Proof of the Claim. We prove each part of the claim separately:

    i) Let $f \in \Omega$ be a non-zero polynomial of degree m such that $f|_E = 0$. Then, for every $v \in V$ there is some $x \in E$ such that f vanishes on the intersection $E \cap \rho(x, v)$. Taking the homogeneous components of f:

$$f = f_m + f_{m-1} + \cdots + f_0,$$

where $f_m = LHC(f) \neq 0$, there are polynomials in $2n$ variables h_i such for all $t \in K$ the following identity holds:

$$f(x + tv) = f_m(v)t^m + \sum_{i=1}^{m-1} h_i(x, v)t^i + f_0(x).$$

We consider the univariate polynomial:

$$F(T) := f(x + Tv) = f_m(v)T^m + \sum_{i=1}^{m-1} h_i(x, v)T^i + f_0(x) \in K[T].$$

As E is a $q-$Kakeya set with directions in V, there are at least q different points $t_1, \ldots, t_q \in K$ such that $x + t_i v \in E$, $1 \leq i \leq q$. Therefore, we deduce that $F(t_i) = 0$, $1 \leq i \leq q$, and, by elementary interpolation arguments, we obtain that F is the zero polynomial in $K[T]$. Thus, we conclude that $LHC(f)(v) = f_m(v) = 0$ and, hence, $LHC(f) \in I_m(V)$ and we have proved that:

$$\forall f \in \Omega, \ f|_E = 0 \implies f \in \Sigma,$$

as wanted.

    ii) Note that if $d_0 > 0$, then for every non-zero homogeneous polynomial $f \in I_{d_0}(V)$, the polynomial $X_1^{d-d_0} f \in I_d(V)$. Thus, either $d_0 = d$ or $\Sigma_m = \{0\}$ for all $m \leq d$.

    iii) Let us first observe that for every $m \leq d$ the dimension of the constructible sets Ω_m and Σ_m satisfy the following identities:

$$\dim(\Omega_m) := \sum_{i=0}^{m} \dim_K(H_i(X_1, \ldots, X_n)),$$

whereas

$$\dim(\Sigma_m) := \begin{cases} \dim_K(I_m(V)) + \sum_{i=0}^{m-1} \dim_K(H_i(X_1, \ldots, X_n)), & \text{if } I_m(V) \neq \{0\} \\ 0, & \text{otherwise.} \end{cases}$$

Both identities are immediate from the definitions of Ω_m and Σ_m combined with the definitions of Krull dimension of constructible sets.

Additionally, we also conclude that for $m \leq d$ the following inequalities hold:

$$\dim(\Omega_m) \leq \dim(\Omega_d), \ \dim(\Sigma_m) \leq \dim(\Sigma_d).$$

The first inequality being obvious, for the second one observe that if $m < d$ and $I_m(V) \neq \{0\}$, then $I_d(V) \neq \{0\}$. In this case,

$$\dim_K(I_m(V)) + \sum_{i=0}^{m-1} \dim_K(H_i(X_1, \ldots, X_n)) \leq \sum_{i=0}^{m} \dim_K(H_i(X_1, \ldots, X_n)),$$

and, hence, we have:

$$\dim(\Sigma_m) \leq \dim_K(I_d(V)) + \sum_{i=0}^{d-1} \dim_K(H_i(X_1, \ldots, X_n)).$$

We finally conclude:

$$\dim(\Omega) = \max\{\dim(\Omega_m) \ : \ 0 \leq m \leq d\} = \dim(\Omega_d) = \binom{d+n}{n}.$$

On the other hand, if $I_d(V) \neq \{0\}$, we have:

$$\dim(\Sigma) = \max\{\dim(\Sigma_m) \ : \ 0 \leq m \leq d\} \leq \dim_K(I_d(V)) + \sum_{i=0}^{d-1} \dim_K(H_i(X_1, \ldots, X_n)).$$

Obviously, if $I_d(V) = \{0\}$, then $I_m(V) = \{0\}$ for all $m \leq d$ and, hence, $\Sigma = \{0\}$.

∎

Thus, we just recall Proposition 4.12 to conclude:

$$\sharp(E) \geq \dim(\Omega) - \dim(\Sigma) \geq \dim_K(H_d(X_1, \ldots, X_n)) - \dim_K(I_d(V)) = \chi_V(d).$$

The second Claim of the Proposition follows since V is zero-dimensional. Thus, for every $d \geq R$ we would have that $\chi_V(d) = \deg(V) = \sharp(V)$.

Finally, the last Claim is obvious and not optimal. Just fix a set Λ of q elements in K including 0 and any mapping $\varphi : V \longrightarrow K^n$. Then, the following is a q−Kakeya set with directions in V:

$$E := \bigcup_{v \in V} \{\varphi(v) + \lambda v \ : \ \lambda \in \Lambda\},$$

whose cardinal is at most $q \deg(V) = q\sharp(V)$. Taking φ any constant mapping, we would have a cardinal bounded by $(q-1)\deg(V) + 1$. □

We shall see now that the main outcome of [Dv, 09] is merely a consequence of our Proposition B.1 above:

Corollary B.2 ([Dv, 09]). *Let $\kappa := \mathbb{F}_q$ be a finite field of cardinal q, and $K := \overline{\mathbb{F}_q}$ its algebraic closure. Let $P_d^K = P_d^K(X_1, \ldots, X_n)$ be the constructible set of all polynomials in the set of variables $\{X_1, \ldots, X_n\}$ of degree at most d with coefficients in $K = \overline{\mathbb{F}_q}$.*
Then, if $d \leq q-1$ and if $E \subseteq \mathbb{A}^n(\mathbb{F}_q)$ is a Kakeya set, then E is a correct test sequence for P_d^K (with respect to $\{0\}$). In particular, we conclude:

$$\sharp(E) \geq \dim(P_d^K) = \binom{d+n}{n}, \ \forall d \leq q-1.$$

Proof. First of all, observe that every Kakeya set $E \subseteq \mathbb{A}^n(\mathbb{F}_q)$ is a q−Kakeya set with directions in $V = \mathbb{P}_{n-1}(\mathbb{F}_q)$. Then, it is a correct test sequence for $\Omega := P_d^K$ with respect to Σ, where Σ is the constructible subset of P_d^K defined in the Proof of the previous Proposition. Additionally, by the previous Proposition we conclude that:

$$\sharp(E) \geq \chi_V(d) = \dim_K(H_d(X_1, \ldots, X_n)) - \dim_K(I_d(V)), \ \forall d \leq q-1,$$

where $H_d(X_1, \ldots, X_n)$ is the vector space over $\overline{\mathbb{F}_q}$ spanned by all homogeneous polynomials of degree d with coefficients in $\overline{\mathbb{F}_q}$ and $I_d(V)$ is the vector space spanned by all polynomials

$f \in H_d(X_1, \ldots, X_n)$ that vanish on V. The Corollary follows by proving that $\Sigma = \{0\}$ for every $d \leq q - 1$. This may be achieved if we prove the following statement:

$$\chi_{\mathbb{P}_{n-1}(\mathbb{F}_q)}(d) = \binom{d+n}{n}, \; \forall d \leq q - 1.$$

Equivalently, it will be enough to prove that $I_m(\mathbb{P}_{n-1}(\mathbb{F}_q)) = \{0\}$ for all $m \leq d \leq q - 1$. In order to prove this last claim, let $f \in H_m(X_1, \ldots, X_n)$ a homogeneous non-zero polynomial of degree m. As f is non-zero, at least one of its affine traces must be non-zero. Without loss of generality, we may assume that ${}^a f(X_2, \ldots, X_m) := f(1, X_2, \ldots, X_n) \in \overline{\mathbb{F}_q}[X_2, \ldots, X_n]$ is a non-zero polynomial of degree at most $m \leq q - 1$. As f vanishes in the whole space $\mathbb{P}_{n-1}(\mathbb{F}_q)$, then ${}^a f$ vanishes into the affine points of $\mathbb{A}^{n-1}(\mathbb{F}_q) \subseteq \mathbb{P}_{n-1}(\mathbb{F}_q)$, where:

$$\mathbb{A}^{n-1}(\mathbb{F}_q) := \{(1 : x_2 : \cdots : x_n) \in \mathbb{P}_{n-1}(\mathbb{F}_q) \; : \; x_2, \ldots, x_n \in \mathbb{F}_q\}.$$

If ${}^a f$ vanishes on $\mathbb{F}_q^{n-1}$ we would have:

$$q^{n-1} \leq \sharp \left(V_{\mathbb{F}_q}({}^a f) \right),$$

where $V_{\mathbb{F}_q}({}^a f)$ are the $\mathbb{F}_q$−rational points of the hyper-surface $V_{\mathbb{A}}({}^a f)$. This cannot be true because of Corollary 3.7: Since ${}^a f$ is a non-zero polynomial of degree at most $m \leq d \leq q - 1$, we would have

$$q^{n-1} \leq \sharp \left(V_{\mathbb{F}_q}({}^a f) \right) \leq \deg({}^a f) q^{n-2} \leq (q-1) q^{n-2},$$

which is a contradiction and yields the Corollary. $\qquad\square$

Nevertheless, most correct test sequences are no Kakeya sets.

Corollary B.3. *Let $\mathbb{F}_q$ be a finite field with q elements and let $\overline{\mathbb{F}_q}$ be its algebraic closure. Let $d \in \mathbb{N}$ be a degree and $k \in \mathbb{N}$ a positive integer such that:*

(B.1) $$d < q^{1 - \frac{1}{k}} - 1.$$

Then, for $s := k\binom{d+n}{n}$, the probability that a list of points $\mathbf{Q} \in \mathbb{A}^n(\mathbb{F}_q)^s$ were a correct test sequence for $P_d(X_1, \ldots, X_n)$ with respect to $\{0\}$ is at least:

$$1 - \frac{1}{q^{\dim(\Omega)}}.$$

In particular, given d, k, q and n such that:

(B.2) $$k\binom{d+1}{n} < \frac{q^n}{2^n},$$

and inequality (B.1) holds, there are correct test sequences for $P_d(X_1, \ldots, X_n)$ with respect to $\{0\}$ which are not Kakeya sets.

Proof. With the notations of Subsection B.2, we consider the constructible subset Ω given by the following identity:

$$\Omega := P_d(X_1, \ldots, X_n) := \{f \in \overline{\mathbb{F}_q}[X_1, \ldots, X_n] \; : \; \deg(f) \leq d\}.$$

We reproduce the Proof of Theorem 5.1. Given $s := k \dim(\Omega) \in \mathbb{N}$ a positive integer, let us consider the incidence variety:

$$V(\Omega, s) := \{(f, x_1, \ldots, x_s) \in \Omega \times \left(\mathbb{A}^n(\overline{\mathbb{F}_q}) \right)^s \; : \; f(x_i) = 0, \; 1 \leq i \leq s\}.$$

Let us consider the two canonical projections $\pi_1 : V(\Omega, s) \longrightarrow \Omega$ and $\pi_2 : V(\Omega, s) \longrightarrow \left(\mathbb{A}^n(\overline{\mathbb{F}_q}) \right)^s$ and the class $\mathscr{D}$ formed by all irreducible components C of $V(\Omega, s)$ such that $\pi_1(C) \setminus \{0\} \neq \emptyset$. By the same arguments as in the Proof of Theorem 5.1 we conclude the following properties:

- For every $C \in \mathscr{D}$, its dimension satisfies:

$$\dim(C) \leq (n-1)s + \dim(\Omega) = (n-1)s + \binom{d+n}{n}.$$

- Defining $B(\Omega, s) := \cup_{C \in \mathscr{D}} C$, by Bézout's Inequality we have that:

$$\deg(B(\Omega, s)) \leq \deg(\Omega) (d+1)^s.$$

As Ω is linear in P_d, this yields:

$$\dim(B(\Omega, s)) \leq (n-1)s + \binom{d+n}{n},$$

and

$$\deg(B(\Omega, s)) \leq (d+1)^s.$$

Again, by the same arguments as in Theorem 5.1, taking $C := \mathbb{F}_q^n$, the probability that a list $\mathbf{Q} \in C^s$ is not a correct test sequence for Ω with respect to $\Sigma = \{0\}$ is at most:

$$\frac{\deg(B(\Omega, s))q^{\dim(B(\Omega))}}{\sharp\left(\left(\mathbb{F}_q^n\right)^s\right)} \leq \frac{(d+1)^s q^{(n-1)s+\dim(\Omega)}}{q^{ns}} \leq \frac{(d+1)^s q^{\dim(\Omega)}}{q^s} \leq \frac{1}{q^{\dim(\Omega)\lambda}},$$

where $\lambda := (k-1) - k\log_q(d+1)$. Thus, the probability that a random list of length s in $\mathbb{F}_q^n$ is a correct test sequence for Ω with respect to $\{0\}$ is at least:

$$1 - \frac{1}{q^{\dim(\Omega)\lambda}},$$

where $\lambda := (k-1) - k\log_q(d+1)$. In particular, if $\log_q(d+1) < \frac{k-1}{k} = (1-1/k)$, there are correct test sequences of length $k\dim(\Omega)$.

On the other hand, according to [DKSS, 09], the following lower bound holds for the cardinal of any Kakeya set in $\mathbb{F}_q^n$:

$$\sharp(E) \geq \frac{\sharp(\mathbb{F}_q^n)}{2^n}.$$

Then, if d, k, q and n satisfy Inequalities (B.1) and (B.2), there are correct test sequences for P_d with respect to $\{0\}$ of length $k\binom{d+n}{n}$ which are not Kakeya sets. $\square$

Whereas Inequality (B.2) is natural for asymptotic values of n, Inequality (B.1) implies that our method of proof does not allow to exhibit correct test sequences which were not Kakeya sets for $d = q - 1$.

B.3. **Correct Test Sequences, Alon's Combinatorial Nullstellensatz and duality.** The outcome of [Al, 99], revised in [Tao, 14], is another method that exhibits correct test sequences of exponential length, although it is commonly known as Combinatorial Nullstellensatz. Alon's statement is the following one:

Theorem B.4 (**Combinatorial Nullstellensatz, according to** [Al, 99]). *Let κ be a field and K its algebraic closure. Let $d_1, \ldots, d_n$ be a list of positive integers and let $P \in K[X_1, \ldots, X_n]$ be a polynomial of degree at most $d_1 + \cdots + d_n$ such that the term of the monomial $X_1^{d_1} \cdots X_n^{d_n}$ in P is non-zero. Then, for every family of subsets $E_1, \ldots, E_n \subseteq \kappa$, such that $\sharp(E_i) > d_i$, there is a point ζ in the Cartesian product $E = E_1 \times \cdots \times E_n$ such that $P(\zeta) \neq 0$.*

Here, we revise this statement under a different format. Notations are the same as in previous sections. For each polynomial $f \in P_d(X_1, \ldots, X_n)$ and for every exponent $\underline{\mu} := (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$, such that $|\underline{\mu}| = \mu_1 + \cdots + \mu_n \leq d$, we denote by $f_{\underline{\mu}}$ the coefficient of the monomial $X_1^{\mu_1} \cdots X_n^{\mu_n}$ in the monomial expansion of f. We prove the following statement:

Theorem B.5 (**Combinatorial Nullstellensatz**). *With the same notations as above, let $(d) := (d_1, \ldots, d_n)$ be a degree list, with $d_i \geq 1$. Let $D := d_1 + \cdots + d_n - n$ be a non-negative integer. Let $\Delta_{(d)} \subseteq \mathbb{N}^n$ be the subset given by the following equality:*

$$(\text{B.3}) \qquad \Delta_{(d)} := \{\underline{\mu} \in \mathbb{N}^n \ : \ \underline{\mu} = (\mu_1, \ldots, \mu_n), \ 0 \leq \mu_i \leq d_i - 1\}.$$

Let $\Omega_{(d)} \subseteq P_D^K(X_1, \ldots, X_n)$ be the following constructible subset:

$$\Omega_{(d)} := \{f \in P_D(X_1, \ldots, X_n) \ : \ \exists \underline{\mu} \in \Delta_{(d)}, \ f_{\underline{\mu}} \neq 0, \ |\underline{\mu}| = \deg(f)\} \cup \{0\}.$$

Then, for every finite sequence of subsets $E_1, \ldots, E_n \subseteq K$, such that $\sharp(E_i) = d_i$, the Cartesian product $E := E_1 \times \cdots \times E_n$ is a correct test sequence for $\Omega_{(d)}$ with respect to $\Sigma = \{0\}$. Additionally, if $\sharp(\kappa) \geq \max\{d_i + 1 \ : \ 1 \leq i \leq n\}$, we may choose $E_i \subseteq \kappa$ for every i, $1 \leq i \leq n$.

As $(d_1 - 1, \ldots, d_n - 1) \in \Delta_{(d)}$, this last Theorem includes Alon's Combinatorial Nullstellensatz. We will exhibit a new proof of it, vaguely inspired by the aspects discussed in [Tao, 14], but using as main mathematical ingredient trace and duality on algebras of zero-dimensional varieties. We begin by a classical construction that we recall in order to fix notations. With the same notations and assumptions as above, let κ be a field and K its algebraic closure. For every point $z \in \mathbb{A}^n(K)$ we denote by $\mathfrak{m}_z \subseteq K[X_1, \ldots, X_n]$ the maximal ideal of all polynomials in $K[X_1, \ldots, X_n]$ vanishing at z, i.e.

$$\mathfrak{m}_z := \{f \in K[X_1, \ldots, X_n] \ : \ f(z) = 0\}.$$

Let $E \subseteq \mathbb{A}^n(K)$ be a finite set and let $D = \deg(E) = \sharp(E)$ be its cardinal. Assume $E = \{z_1, \ldots, z_D\} \subseteq \mathbb{A}^n(K)$. Let us denote by $I(E) \subseteq K[X_1, \ldots, X_n]$ the ideal of all polynomials in $K[X_1, \ldots, X_n]$ vanishing at all points in E, i.e.

$$I(E) = \{f \in K[X_1, \ldots, X_n] \ : \ f(z) = 0, \ \forall z \in E\} = \bigcap_{i=1}^{D} \mathfrak{m}_{z_i},$$

Let $K[E] := K[X_1, \ldots, X_n]/I(E)$ be the residual ring, which is a zero-dimensional (Artinian) $K-$algebra and a vector space of dimension equal to $\sharp(E)$.
If $E \subseteq \mathbb{A}^n(\kappa)$ let us also consider the ring $\kappa[E]$ given by:

$$\kappa[X_1, \ldots, X_n]/I(E)^c,$$

where $I(E)^c := I(E) \cap \kappa[X_1, \ldots, X_n]$ is the contraction of $I(E)$. Then, $\kappa[E]$ is also a zero-dimensional (Artinian) ring and we have:

$$K \otimes_\kappa \kappa[E] = K[E].$$

In particular, if $E \subseteq \mathbb{A}^n(\kappa)$, the following dimensions (as vector spaces) agree:

$$\dim_\kappa (\kappa[E]) = \dim_K (K[E]).$$

We now recall a classical identification of residual classes in $K[E]$ (or $\kappa[E]$) with homotheties over the same vector spaces. With the same notations, for every $h \in K[X_1, \ldots, X_n]$, let us denote by $\eta_h : K[E] \longrightarrow K[E]$ the following endomorphism of $K-$vector spaces:

$$\eta_h : \quad \begin{array}{ccc} K[E] & \longrightarrow & K[E] \\ g + I(E) & \longmapsto & (hg) + I(E). \end{array}$$

The trace of these endomorphisms allow us to introduce the next bilinear form on $K[E]$:

$$\langle \cdot, \cdot \rangle_E : \quad \begin{array}{ccc} K[E] \times K[E] & \longrightarrow & K \\ (g_1 + I(E), g_2 + I(E)) & \longmapsto & Tr(\eta_{g_1 g_2}). \end{array}$$

The following are well-known consequences of the Chinese Remainder Theorem applied to $K[E]$: For every $h \in K[X_1, \ldots, X_n]$, η_h is a diagonalizable endomorphism and its Jordan canonical form is the following diagonal matrix:

$$\mathrm{Diag}(h(z_1), \ldots, h(z_D)).$$

In particular, the trace of η_h is given by the following identity:

$$\mathrm{Tr}(\eta_h) = \sum_{i=1}^{D} h(z_i) = \sum_{z \in E} h(z).$$

Moreover, we also have the following statement:

Lemma B.6. *With the same notations as above, for every basis $\mathscr{B} = \{v_1, \ldots, v_D\}$, $v_i = f_i + I(E)$, of $K[E]$ as $K-$vector space there is a basis (called dual with respect to $\langle \cdot, \cdot \rangle_E$) $\mathscr{B}^* = \{w_1, \ldots, w_D\}$, $w_j = g_j + I(E)$, such that for all $i, j \in \{1, \ldots, D\}$ we have:*

$$\langle v_i, w_j \rangle_E = \sum_{z \in E} f_i(z) g_j(z) = \delta_{i,j},$$

where $\delta_{i,j}$ is the Kronecker delta.

Proof. Let $\mathscr{B} := \{v_1, \ldots, v_d\}$ be an ordered basis of $K[E]$ as vector space. By the Chinese Remainder Theorem, we may identify $K[E]$ and K^D by the following isomorphism:

$$\widetilde{\varphi}: \quad \begin{array}{ccc} K[E] & \longrightarrow & K^D \\ g + I(E) & \longrightarrow & (g(z_1), \ldots, g(z_D)). \end{array}$$

Then, $\mathscr{B}$ is a basis of $K[E]$ if and only if the following matrix (vanderMonde's) is a regular matrix:

$$vdM(\mathscr{B}) := \begin{pmatrix} v_1(z_1) & \cdots & v_1(z_D) \\ \vdots & \ddots & \vdots \\ v_D(z_1) & \cdots & v_D(Z_D) \end{pmatrix}.$$

For every i, $1 \leq i \leq D$, let e_k be the $k-$th vector of the "canonical" basis of K^D and let $\omega_i := (\omega_{i,1}, \ldots, \omega_{i,D}) \in K^D$ be the unique solution of the following linear system of equations:

$$vdM(\mathscr{B}) \begin{pmatrix} \omega_{i,1} \\ \vdots \\ \omega_{i,D} \end{pmatrix} = e_i^t,$$

where e_i^t is the transposed matrix of the vector e_i. Then, by the isomorphism $\widetilde{\varphi}$ there exist $g_i \in K[X_1, \ldots, X_n]$ and $w_i = g_i + I(E) \in K[E]$ such that:

$$\widetilde{\varphi}(g_i + I(E)) = (g_i(z_1), \ldots, g_i(z_D)) = (\omega_{i,1}, \cdots, \omega_{i,D}).$$

The family $\mathscr{B}^* := \{w_1, \ldots, w_D\}$ is the "dual" basis of $\mathscr{B}$. $\qquad\square$

Lemma B.7. *Let $h_1, \ldots, h_n \in \kappa[T]$ be univariate polynomials with respective degrees $d_1, \ldots, d_n$. Assume that $h_1, \ldots, h_n$ split completely in κ and that they are square-free (i.e. they do not have multiple roots). We define the ideal $\mathfrak{a} = (h_1(X_1), \ldots, h_n(X_n)) \subseteq K[X_1, \ldots, X_n]$ and, for each i, $1 \leq i \leq n$, let $E_i \subseteq \kappa$ be the set of zeros of h_i in κ. Let us consider also the zero-dimensional variety given by the Cartesian product $E = E_1 \times \cdots \times E_n \subseteq \mathbb{A}^n(K)$. We have:*

  i) *The ideal $\mathfrak{a} = I(E)$ is a radical ideal (i.e. the residual ring $K[X_1, \ldots, X_n]/\mathfrak{a}$ has no non-zero nilpotente element) and, hence, $\mathfrak{a} = I(E) = \{f \in K[X_1, \ldots, X_n] : f|_E = 0\}$.*

  ii) *The family $\{h_1(X_1), \ldots, h_n(X_n)\}$ is a Gröbner basis of $\mathfrak{a} = I(E)$ with respect to the monomial order "degree+lexicographic" with the variable order $X_1 < X_2 < \ldots < X_n$.*

  iii) *The following is a monomial basis of $K[E]$:*

$$\mathscr{B} = \{X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \; : \; 0 \leq \mu_i \leq d_i - 1, 1 \leq i \leq n\}.$$

  iv) *For every i, $1 \leq i \leq n$, let us denote by $\mathscr{B}_i^*$ the dual basis in $K[E_i]$ with respect to the trace $\langle \cdot, \cdot \rangle_{E_i}$ of $\mathscr{B}_i := \{T^{\mu_i} + (h_i) : 0 \leq \mu_i \leq d_i - 1\}$. Let us denote this dual basis by:*

$$\mathscr{B}_i^* := \{g_k^{(i)}(T) + (h_i) : 0 \leq k \leq d_i - 1\} \subseteq K[E_i] := K[T]/(h_i).$$

  Then, the following is a dual basis of $\mathscr{B}$ in $K[E]$ with respect to the bilinear form $\langle \cdot, \cdot \rangle_E$:

$$\mathscr{B}^* = \left\{ \left(\prod_{i=1}^n g_{\mu_i}^{(i)}(X_i) \right) + \mathfrak{a} \; : \; (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n, 0 \leq \mu_i \leq d_i - 1, 1 \leq i \leq n \right\}.$$

Proof. Properties *i*) to *iii*) are well-known and need no additional proof. As for Claim *iv*), let us denote by $(d) = (d_1, \ldots, d_n)$ the degree list and by $\Delta_{(d)}$ the class of monomial exponents introduced in Identity (B.3) of Theorem B.5.

Let us observe that for each i, $1 \leq i \leq n$, we have:

$$\sum_{z_i \in E_i} g_k^{(i)}(z_i) z_i^r := \delta_{k,r},$$

for $0 \leq k, r \leq d_i - 1$.

Given every pair of monomial exponents $\underline{\theta} := (\theta_1, \ldots, \theta_n) \in \Delta_{(d)}$ and $\underline{\mu} := (\mu_1, \ldots, \mu_n) \in \Delta_{(d)}$, let us define the following quantity:

$$D_{\underline{\mu}, \underline{\theta}} := \langle \prod_{i=1}^n g_{\mu_i}^{(i)}(X_i) + \mathfrak{a}, X_1^{\theta_1} \cdots X_n^{\theta_n} + \mathfrak{a} \rangle_E = \sum_{(z_1, \ldots, z_n) \in E} \left(\left(\prod_{i=1}^n g_{\mu_i}^{(i)}(z_i) \right) z_1^{\theta_1} \cdots z_n^{\theta_n} \right).$$

We have:

$$D_{\underline{\mu},\underline{\theta}} = \left(\sum_{z_1 \in E_1} g_{\mu_1}^{(1)}(z_1) z_1^{\theta_1} \right) \left(\sum_{(z_2,\ldots,z_n) \in E_2 \times \cdots \times E_n} \left(\left(\prod_{i=2}^{n} g_{\mu_i}^{(i)}(z_i) \right) z_2^{\theta_2} \cdots z_n^{\theta_n} \right) \right).$$

As $\mathscr{B}_1^*$ is a dual basis of $\mathscr{B}_1$, we conclude that $\left(\sum_{z_1 \in E_1} g_{\mu_1}^{(1)}(z_1) z_1^{\theta_1} \right) = \delta_{\mu_1,\theta_1}$ and we also have:

$$D_{\underline{\mu},\underline{\theta}} = \delta_{\mu_1,\theta_1} \left(\sum_{(z_2,\ldots,z_n) \in E_2 \times \cdots \times E_n} \left(\left(\prod_{i=2}^{n} g_{\mu_i}^{(i)}(z_i) \right) z_2^{\theta_2} \cdots z_n^{\theta_n} \right) \right).$$

By induction on n, we finally conclude:

$$D_{\underline{\mu},\underline{\theta}} = \delta_{\mu_1,\theta_1} \delta_{\mu_2,\theta_2} \cdots \delta_{\mu_n,\theta_n} = \delta_{\underline{\mu},\underline{\theta}},$$

and Claim $iv)$ is proven. $\square$

The following statement is a variation of a Lemma that may be found in [Tao, 14]. We just give a proof based on our duality arguments.

Lemma B.8. *With the same notations as above, let $\underline{\theta} = (\theta_1,\ldots,\theta_n) \in \Delta_{(d)}$ be a monomial exponent in $\Delta_{(d)}$. Let $\underline{\mu} = (\mu_1,\ldots,\mu_n) \in \mathbb{N}^n$ be another monomial exponent such that $|\underline{\mu}| = \mu_1 + \cdots + \mu_n = |\underline{\theta}|$. If there is some index i such that $\mu_i \geq d_i$, then the following holds:*

$$D_{\underline{\theta},\underline{\mu}} = \left\langle \left(\prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = 0.$$

Proof. The proof is similar to that of the preceding Lemma. Without loss of generality, let us assume that $\mu_n \geq d_n$. Since we have:

$$\mu_1 + \cdots + \mu_n = \theta_1 + \cdots + \theta_n, \ 0 \leq \theta_i \leq d_i - 1,$$

then there must exists $j \neq n$ such that $\mu_j \neq \theta_j$ and $0 \leq \mu_j \leq d_i - 1$. In order to prove this, observe that if for all $j \neq n$ either we have $\mu_j = \theta_j$ or $\mu_j \geq d_i$, then we would have:

$$|\underline{\mu}| = \mu_1 + \cdots + \mu_n \geq \theta_1 + \cdots + \theta_{n-1} + \mu_n \geq \theta_1 + \cdots + \theta_{n-1} + \theta_n + 1 > |\underline{\theta}| + 1,$$

which contradicts the hypothesis $|\underline{\mu}| = |\underline{\theta}|$.

Without loss of generality again, we assume that $\mu_1 \neq \theta_1$ and $0 \leq \mu_1 \leq d_1 - 1$. Then, we have:

$$D_{\underline{\mu},\underline{\theta}} := \left\langle \left(\prod_{i=1}^{n} g_{\mu_i}^{(i)}(X_i) \right) + \mathfrak{a}, X_1^{\theta_1} \cdots X_n^{\theta_n} + \mathfrak{a} \right\rangle_E = \sum_{(z_1,\ldots,z_n) \in E} \left(\left(\prod_{i=1}^{n} g_{\mu_i}^{(i)}(z_i) \right) z_1^{\theta_1} \cdots z_n^{\theta_n} \right).$$

Thus, we get:

$$D_{\underline{\mu},\underline{\theta}} = \left(\sum_{z_1 \in E_1} g_{\mu_1}^{(1)}(z_1) z_1^{\theta_1} \right) \left(\sum_{(z_2,\ldots,z_n) \in E_2 \times \cdots \times E_n} \left(\left(\prod_{i=2}^{n} g_{\mu_i}^{(i)}(z_i) \right) z_2^{\theta_2} \cdots z_n^{\theta_n} \right) \right).$$

And, since $\mu_1 \neq \theta_1$, we conclude:

$$D_{\underline{\mu},\underline{\theta}} = 0 \cdot \left(\sum_{(z_2,\ldots,z_n) \in E_2 \times \cdots \times E_n} \left(\left(\prod_{i=2}^{n} g_{\mu_i}^{(i)}(z_i) \right) z_2^{\theta_2} \cdots z_n^{\theta_n} \right) \right) = 0,$$

which finishes the proof of the Lemma. $\square$

Corollary B.9. *With the same notations as above, let $\underline{\theta} \in \Delta_{(d)}$ and $\underline{\mu} \in \mathbb{N}^n$ be two monomial exponents. If $|\underline{\mu}| \leq |\underline{\theta}|$, we have:*

$$D_{\underline{\theta},\underline{\mu}} = \left\langle \left(\prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = \delta_{\underline{\mu},\underline{\theta}},$$

where $\delta_{\underline{\mu},\underline{\theta}}$ is Kronecker delta.

Proof. If $\underline{\mu} \in \Delta_{(d)}$, Lemma B.7 implies the given statement. Otherwise, if $|\underline{\mu}| \leq |\underline{\theta}|$ and $\underline{\mu} \notin \Delta_{(d)}$, the property holds because of Lemma B.8. $\square$

Proof. (OF THEOREM B.5). Let $d_1, \ldots, d_n$ be some degrees, let $(d) = (d_1, \ldots, d_n)$ be the degree list they define and $\Delta_{(d)}$ the class of monomial exponents as in the statement of Theorem B.5. Let $D := d_1 + \cdots + d_n - n$ be the quantity also defined in the statement of this Theorem. Let $\Omega_{(d)} \subseteq P_D(X_1, \ldots, X_n)$ be the following constructible subset made of polynomials of degree at most D:

$$\Omega_{(d)} := \{f \in P_D^K(X_1, \ldots, X_n) \: : \: \exists \underline{\mu} \in \Delta_{(d)}, \: f_{\underline{\mu}} \neq 0, \: |\underline{\mu}| = \deg(f)\} \cup \{0\}.$$

Let $E_1, \ldots, E_n \subseteq K$ be some finite subsets such that $\sharp(E_i) = d_i$. Let $E := E_1 \times \cdots \times E_n$ be the Cartesian product and let $K[E]$ be the residual ring of $K[X_1, \ldots, X_n]$ modulo $I(E)$. Let $\langle \cdot, \cdot \rangle_E$ be the bilinear form associated to the trace on $K[E]$.

For every i, $1 \leq i \leq n$, let $h_i \in K[T]$ be the following univariate polynomial:

$$h_i(T) := \prod_{\zeta \in E_i} (T - \zeta).$$

According to Lemma B.7, let $\mathfrak{a} := (h_1(X_1), \ldots, h_n(X_n))$ be the ideal they generate. Therefore, we have:

$$K[E] = K[X_1, \ldots, X_n]/\mathfrak{a}.$$

Let $\mathscr{B}$ be the monomial basis of $K[E]$ given by the following equality:

$$\mathscr{B} = \{X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \: : \: 0 \leq \mu_i \leq d_i - 1, 1 \leq i \leq n\},$$

and let $\mathscr{B}^*$ be the dual basis of $\mathscr{B}$ exhibited in the Lemma B.7 above:

$$\mathscr{B}^* = \left\{ \left(\prod_{i=1}^n g_{\mu_i}^{(i)}(X_i) \right) + \mathfrak{a} \: : \: (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n, 0 \leq \mu_i \leq d_i - 1, 1 \leq i \leq n \right\}.$$

Let $f \in \Omega_{(d)}$ be a polynomial and suppose $t := \deg(f)$. The monomial expansion of f has the following form:

$$f := \sum_{|\underline{\mu}| \leq t} a_{\underline{\mu}} X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Since $f \in \Omega_{(d)}$, then there exists $\underline{\theta} \in \Delta_{(d)}$ such that $|\underline{\theta}| = \deg(f) = t$ and the coefficient $f_{\underline{\theta}} = a_{\underline{\theta}} \neq 0$ is non-zero.

Let $G_{\underline{\theta}} := \left(\prod_{i=1}^n g_{\theta_i}^{(i)}(X_i) \right) + \mathfrak{a} \in K[E]$. By Corollary B.9 above, we deduce that for all $\underline{\mu} \in \mathbb{N}^n$ such that $\underline{\mu} \neq \underline{\theta}$ the following holds:

$$D_{\underline{\theta}, \underline{\mu}} = \left\langle G_{\underline{\theta}}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = 0.$$

Since

$$D_{\underline{\theta}, \underline{\theta}} = \left\langle G_{\underline{\theta}}, X_1^{\theta_1} \cdots X_n^{\theta_n} + \mathfrak{a} \right\rangle_E = 1,$$

we thus conclude:

$$\left\langle G_{\underline{\theta}}, f + \mathfrak{a} \right\rangle_E = a_{\underline{\theta}} \neq 0.$$

On the other hand, we have:

$$a_\theta = \left\langle G_{\underline{\theta}}, f + \mathfrak{a} \right\rangle_E = \sum_{(z_1, \ldots, z_n) \in E} \left(\prod_{i=1}^n g_{\theta_i}^{(i)}(z_i) \right) f(z_1, \ldots, z_n).$$

Then, we conclude that it is not possible that f vanishes at all points of E since, otherwise, $a_{\underline{\theta}} = 0$, which cannot be possible. $\qquad\square$

REFERENCES

[AK, 06] F. Albiac, N.J. Kalton, *"Topics in Banach Space Theory"*. Graduate Text in Mathematics **233**, 2006.

[Al, 99] N. Alon, *Combinatorial Nullstellensatz*. Combin. Probab. Comput. **8** (1999), 7-29.

[BGHLMPS, 19] B. Bank, M. Giusti, J. Heintz, G. Lecerf, G. Matera, L.M. Pardo, P. Solerno, *"Résolution Géomètrique"*. Book in preparation, 2019.

[BP, 07] C. Beltrán, L.M. Pardo, *Estimates on the Distribution of the Condition Number of Singular Matrices*. Found. Comput. Math. **7** (2007), 87-134.

[BlCuShSm, 98] L. Blum, F. Cucker, M. Shub, and S. Smale, *"Complexity and real computation"*. Springer-Verlag, New York, 1998.

[BuJo, 14] L. Busé, J.P. Jouanolou, *On the discriminant scheme of homogeneous polynomials*. Math. in Comput. Sci. **8** (2014), 175-234.

[CGHMP, 03] D. Castro, M. Giusti, J. Heintz, G. Matera, L. M. Pardo, *The Hardness of Polynomial Equation Solving*. Foundations of Computational Mathematics **3** (2003), 347-420.

[CaDi, 05] E. Cattani, A. Dickenstein, *Introduction to residues and resultants*. In A.Dickenstein, I.Z.Emiris (Eds.): *"Solving Polynomial Equations: Foundations, Algorithms, and Applications"*, Algorithms and Comput. Math., **14**, Springer-Verlag, 2005, 1-61.

[Ch, 64-65] C. Chevalley, *"Introduction à la Théorie des Schémas"*. Cours à l'IHP, Notes de D. Fatiadi, éd. Centre de Physique Théorique de l'École Polytechnique, Pub. N **A75.1268**, 1964-65.

[CKKLW,95] F. Cucker, M. Karpinski, P. Koiran, T. Lickteig, K. Werther, *On real Turing machines that toss coins*. In Proc. of the Twenty-Seventh Ann. ACM Symp. on Theor. of Comput. (F. T. Leighton, A. Borodin eds.), ACM 1995, 335-342.

[DML, 78] R.A. DeMillo, R.J. Lipton, *A probabilistic remark on algebraic program testing*. Information Processing Letters **7** (1978), 193–195.

[Dv, 09] Z. Dvir, *On the size of Kakeya sets on finite fields*. J. of the A.M.S. **22** (2009), 1093-1097.

[DKL, 14] Z. Dvir, J. Kollár, S. Lovett, *Variety evasive sets*. Comput. Complexity **23** (2014), 509–529.

[DKSS, 09] Z. Dvir, S. Kopparty, S. Saraf, M. Sudan, *Extensions to the method of multiplicities, with applications to Kakeya sets and mergers*, 2009 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), 181-190, IEEE Computer Soc., Los Alamitos, CA, 2009.

[FP, 13] M. Fernández, Luis M. Pardo, *An Arithmetic Poisson Formula for the Multi-variate Resultant*. Journal of Complexity **29** (2013), 323-350.

[Fu, 83] W. Fulton, *"Intersection theory"*. New York-Heidelberg-Berlin Tokyo Springer, 1983.

[GHJ, 54] L. Gillman, M. Henriksen, M. Jerison, *On a theorem of Gelfand and Kolmogoroff concerning maximal ideals in rings of continuous functions*. Proc. of the Amer. Math. Soc. **5** (1954), 447-455.

[GHHMMP, 97] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, L. M. Pardo, *Lower bounds for diophantine approximations*. Journal of Pure and Applied Algebra **117** & **118** (1997), 277-317.

[GHMP, 97] M. Giusti, J. Heintz, J.E. Morais, Luis M. Pardo, *Le rôle des structures des données dans les problèmes d'élimination*. Comptes Rendues Acad. Sci. Paris, Sér. I **325** (1997), 1223-1228.

[He, 83] J. Heintz, *Fast Quantifier Elimination for Algebraically Closed Fields*. Theoret. Comput. Sci. **24** (1983), 239-277.

[He, 85] J. Heintz, *Corrigendum: Definability and Fast Quantifier Elimination in Algebraically Closed Fields*. Theoret. Comput. Sci. **39** (1985), 343.

[HeSc, 82] J. Heintz, C. P. Schnorr, *Testing polynomials which are easy to compute*. Logic and algorithmic: An international symposium held in honor of Ernst Specker, Monographie No. **30** de l'Enseignement Mathématique, 1982, 237-254.

[Hew, 48] E. Hewitt, *Rings of real-valued continuous functions. I*. Trans. Amer. Math. Soc. **64** (1948), 45-99.

[Je, 05] Z. Jelonek, *On the effective Nullstellensatz*. Invent. math. **162** (2005), 1–17.

[Jo, 97] J. P. Jouanolou, *Formes d'inertie et résultant: un formulaire*. Advances in Mathematics **126** (1997), 119-250.

[Ko, 99] P. Koiran, *Elimination of Parameters in the Polynomial Hierarchy*. Theor. Comput. Sci. **215** (1999), 289-304.

[Kol, 88] J. Kollár, *Sharp effective Nullstellensatz*. J. Am. Math. Soc. **1** (1988), 963–975.

[KP, 96] T. Krick, Luis M. Pardo, *A computational method for diophantine approximations*. In "Algorithms in Algebraic Geometry" , L. González Vega, T. Recio (eds.), Progress in Mathematics **143** , Birkhauser Verlag, 1996, 193-253.

[LW, 54] S. Lang, A. Weil, *Number of points of varieties in finite fields*. American Journal of Mathematics **76** (1954), 819-827.

[Mu, 87] K. Mulmuley, *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field*. Combinatorica **7** (1987), 101–104.

[Pa, 95] L. M. Pardo, *How lower and upper complexity bounds meet in elimination theory*. In "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes", G. Cohen, M. Giusti & T. Mora, eds., Lecture Notes in Computer Science **948**, Springer Verlag, 1995, 33-69.

[PSM, 04] L. M. Pardo, J. San Martín, *Deformation techniques to solve Generalised Pham Systems*. Theoretical Computer Science **315** (2004), 593-625.

[Ore, 22] Ø. Ore, *Über höhere Kongruenzen*. Norsk Mat. Forenings Skrifter, **8** (1922), 15 pages.

[Sax, 14] N. Saxena, *Progress on Polynomial Identity Testing - II*. In "Perspectives in Computational Complexity: The Somenath Biswas Anniversary Volume, 2014, pages 131–146.

[Sha, 77] I. R. Shafarevich, *"Basic Algebraic Geometry"*. Grundlehren der mathematischen Wissenschaften **213**, Springer, 1977.

[Sch, 80] J. P. Schwarz, *Fast Probabilistic Algorithms for Verification of Polynomial Identities*. J. of the A.C.M. **27** (1980), 701-717.

[So, 99] M. Sombra, *A sparse effective Nullstellensatz*. Adv. Appl. Math. **22** (1999), 271–295.

[St, 69] S. A. Stepanov, *On the number of points of a hyperelliptic curve over a finite prime field*. Mathematics of the USSR-Izvestiya **3** (1969), 1103-1114.

[Tao, 14] T. Tao, *Algebraic Combinatorial geometry: the polynomial method in arithmetic c ombinatorics, incidence combinatorics, and number theory*. EMS Surveys Math. Sci. **1** (2014), 1-46.

[Vo, 84] W. Vogel, *"Lectures on Bézout's Theorem"*. Tata Inst. for Fundamenta Research, Springer-Verlag, 1984.

[We,49] A. Weil, *Numbers of solutions of equations in finite fields*. Bull. Amer. Math. Soc. **55** (1949), 497-508.

[Wo, 99] T. Wolff, *Recent work connected with Kakeya problem*. In *Prospects in mathematics*, Amer. Math. Soc., 1999, 129-162.

[Zp, 79] R. Zippel, *Probabilistic Algorithms for Sparse Polynomials.* In *"Symbolic and Algebraic Computation (EUROSAM'79)"*, Lecture Notes in Computer Science **72**, Springer, 1979, 216-266.

Depto. de Matemáticas, Estadística y Computación. Facultad de Ciencias. Universidad de Cantabria. Avda. Los Castros s/n. E-39071 Santander, Spain.
Email address: luis.m.pardo@gmail.com, luis.pardo@unican.es

Depto. de Matemáticas, Estadística y Computación. Facultad de Ciencias. Universidad de Cantabria. Avda. Los Castros s/n. E-39071 Santander, Spain.
Email address: daniel.sebastian@unican.es