Regression for sets of polynomial equations

Franz J. Király*, Paul von Bünau, Jan S. Müller, Duncan A. J. Blythe, Frank C. Meinecke, Klaus-Robert Müller
Berlin Institute of Technology (TU Berlin), Machine Learning dept., Franklinstr. 28/29, 10587 Berlin

APPENDIX – SUPPLEMENTARY MATERIAL

This Supplementary Material contains the theoretical background for a treatment of the ideal regression problem. In Section A we explain why ideal regression is the correct framework to estimate parametric systems of equations. In Section B, we present the concept of genericity, which is essential for formulating a generative model of ideal regression. Moreover, we prove some theoretical results related to genericity. These results are then applied in Section C to obtain identifiability results and an estimator for ideal regression, and - as a special application - for the common marginals problem.

A From estimating sets of equations to ideal regression

In this section, we will explain why ideal regression is the natural formulation for estimating sets of equations. We will provide some examples leading to the conclusion that ideals in rings are the canonical objects which capture the ambiguities of sets of polynomial equations. The reader may find some knowledge on ring theory, in particular on ideals and Hilbert's Nullstellensatz helpful, as presented for example in [1], but not necessary to understand the phenomena presented in this section.

As already stated in the main corpus of the paper, we want to estimate a system of polynomial equations with specific structure, given some arbitrary system of polynomial equations:

Problem A.1 *Given input polynomials $q_1, \ldots, q_n$, estimate a regression parameter θ such that the parametric system $p_\theta^{(1)}, \ldots, p_\theta^{(m)}$, is "close" to the inputs $q_1, \ldots, q_n$.*

Of course, Problem A.1 is still an informal problem description: it remains to state how θ parameterizes the system of equations, and it has yet to be stated what "close" should mean. Intuitively, "close" should mean that the set of solutions defined by the $p_\theta^{(1)}, \ldots, p_\theta^{(m)}$ is close to the set or sets of solutions defined by the $q_1, \ldots, q_n$, i.e. formally

$$\begin{aligned} V_\theta &= \mathrm{V}(p_\theta^{(1)}, \ldots, p_\theta^{(m)}) \\ &= \{x \in \mathbb{C}^D \,;\, p_\theta^{(1)}(x) = \cdots = p_\theta^{(m)}(x) = 0\}. \end{aligned}$$

Before we continue, we first show a basic example for ideal regression:

Example A.2 In ordinary regression, we are given points $(x^{(1)}, y^{(1)}), \ldots, (x^{(N)}, y^{(N)}) \in \mathbb{R}^k \times \mathbb{R}$. We want to estimate a linear polynomial

$$p_\theta(X_1, \ldots, X_k, Y) = \beta_1 X_1 + \cdots + \beta_k X_k + \alpha - Y$$

with parameter $\theta = (\beta_1, \ldots, \beta_k, \alpha) \in \mathbb{R}^{k+1}$ such that $p_\theta(x^{(i)}, y^{(i)})$ is small for all i. For example, in least squares regression, the optimal θ is obtained by minimizing the sum of the squares of the $p_\theta(x^{(i)}, y^{(i)})$.

Now each point $(x^{(i)}, y^{(i)})$ is the unique solution to the set of $k+1$ equations

$$\begin{aligned} q_{i0}(X_1, \ldots, X_k, Y) &= Y - y^{(i)} = 0 \\ q_{i1}(X_1, \ldots, X_k, Y) &= X_1 - x_1^{(i)} = 0 \\ q_{i2}(X_1, \ldots, X_k, Y) &= X_2 - x_2^{(i)} = 0 \\ &\vdots \\ q_{ik}(X_1, \ldots, X_k, Y) &= X_k - x_k^{(i)} = 0 \end{aligned}$$

For one point $(x^{(i)}, y^{(i)})$, being close to the regression hyperplane $\mathrm{V}(p_\theta)$ means that p_θ is a principal vector of the q_{ij} with i fixed (w.r.t certain error measures) considered as elements in the vector space of linear polynomials. So, being a good approximation to all points means that p_θ is a principal vector for the data given by all q_{ij}.

The following examples will show the central ambiguities which occur when considering more than one equation:

* Franz J. Király is also at Discrete Geometry Group (FU Berlin), Arnimallee 2, 14195 Berlin

Example A.3 Let us imagine we want to regress two equations instead of a single one, i.e. we want to determine two regressor polynomials

$$p_\theta^{(1)}(X_1,\dots,X_k,Y) = \beta_1^{(1)}X_1 + \cdots + \beta_k^{(1)}X_k + \alpha^{(1)} - Y$$
$$p_\theta^{(2)}(X_1,\dots,X_k,Y) = \beta_1^{(2)}X_1 + \cdots + \beta_k^{(2)}X_k + \alpha^{(2)} - Y$$

where θ includes the information on the regression coefficients $\beta_j^{(i)}$ and the $\alpha^{(i)}$. Now it is essential to note that the set of solutions

$$\begin{aligned} V_\theta &= \mathrm{V}(p_\theta^{(1)}, p_\theta^{(2)}) \\ &= \{(x,y) \in \mathbb{R}^k \times \mathbb{R}\,;\; p_\theta^{(1)}(x,y) = p_\theta^{(2)}(x,y) = 0\} \end{aligned}$$

is already uniquely determined by the linear span of the two polynomials $p_\theta^{(1)}(X_1,\dots,X_k,Y)$ and $p_\theta^{(2)}(X_1,\dots,X_k,Y)$, seen as elements in the vector space of linear polynomials. For example, two polynomials $p_\theta^{(1)}$ and $p_\theta^{(2)}$ give rise to the same set of solutions V_θ as the two polynomials $p_\theta^{(1)} + p_\theta^{(2)}$ and $p_\theta^{(1)} - p_\theta^{(2)}$. One can also prove that these are the only ambiguities in the solution. Thus for V_θ, the parameter θ has not $2k+2$ degrees of freedom, but only $2k+1$. The parameter space for θ is the space of all 2-dimensional affine linear spaces in $(k+1)$-space. In general, similar additive ambiguities occur, and it makes sense to speak about the set of solutions only uniquely with respect to these additive symmetries.

Example A.4 Similarly, consider the case where we want to regress a conic section, i.e. we want to regress a linear polynomial ℓ_θ and a quadratic polynomial q_θ; the parameter θ determining all coefficients of the two polynomials. Again, different choices of coefficients can lead to the set of solutions

$$V_\theta = \mathrm{V}(\ell_\theta, q_\theta);$$

For example, if ℓ_θ, q_θ are some choices for the polynomials, ℓ_θ and $q_\theta + \ell'\ell_\theta$ give rise to the same set of solutions, where ℓ' is an arbitrary linear polynomial. Similar multiplicative ambiguities also occur in the general case.

The correct algebraic structure to remove these ambiguities is the ideal in ring theory:

Definition A.5 *Let R be a commutative ring, e.g. the ring of polynomials in D variables $R = \mathbb{C}[X_1,\dots,X_D]$ with addition and multiplication. An ideal of R is a proper subset $\mathcal{I} \subsetneq R$ such that:*

1. *(i) $\mathcal{I}$ is additively closed, i.e. $f+g \in \mathcal{I}$ for all $f,g \in \mathcal{I}$*
2. *(ii) $\mathcal{I}$ is closed under multiplication with R, i.e. $f \cdot g \in \mathcal{I}$ for all $f \in \mathcal{I}$ and $g \in R$*

A radical ideal additionally fulfills:

1. *(iii) $\mathcal{I}$ is closed under taking roots, i.e. $f \in \mathcal{I}$ if $f^n \in \mathcal{I}$ for some $n \in \mathbb{N}$.*

Hilbert's Nullstellensatz states that in the ring $\mathbb{C}[X_1,\dots,X_D]$, the radical ideals uniquely parameterize the different solution sets of polynomial equations. Thus we can remove the ambiguities in the parametric model by replacing sets of equations by ideals. Problem A.1 then becomes

Problem A.6 *Let $\mathcal{F}_\theta$ be a parametric family of radical ideals in $\mathbb{C}[X_1,\dots,X_D]$. Given input polynomials $q_1,\dots,q_n$, estimate a regression parameter θ such that $\mathcal{F}_\theta$ is "close" to the inputs $q_1,\dots,q_n$.*

The radical ideals themselves are uniquely parameterized by parts of a certain manifold, the so-called Hilbert scheme; this automatically implies unique parametrization for the parametric family $\mathcal{F}_\theta$ if θ is a parameter of the Hilbert scheme. For example, the d-dimensional sub-vector spaces of D-space are equally parameterized by the possible row-spans of maximal rank $(d \times D)$-matrices. Algebraically, this corresponds to the non-singular part of the Grassmann manifold $\mathrm{Gr}(d,D)$.

Also note that we in general cannot remove all the ambiguities in the input polynomials by putting them into a single ideal, since the measurements of the q_i may be noisy, and the noise is on the coefficients of particular elements in the ideal. However, one could group for example some of them into classes of ideals, depending on the setting (for example the ideals of points in ordinary regression).

It remains to say what it means for input polynomials and regressor ideal $\mathcal{F}_\theta$ to be "close". As in ordinary regressions, there are different ways in which one can choose to penalize differences. For example, one can explicitly or numerically optimize a regularized loss function. On the other hand, a pragmatical approach is to measure the differences in terms of squared errors on the graded vector space structure of the ideal; e.g. if the input polynomials are all degree 2, one would sum the squared distances to the vector space consisting of degree two and less polynomials in $\mathcal{F}_\theta$; or, if $\mathcal{F}_\theta$ is generated in degree 3 and higher, then the least square error in the higher degree parts.

In the algorithm we present in section C, we try to minimize squared errors in the graded parts, since quadratic optimization provides explicit and efficient solutions and thus deterministic algorithms.

B Algebraic Geometry of Genericity

In the paper, we have introduced the framework of ideal regression, where we estimate ideals from noisy input polynomials. In its algebraic formulation as Problem A.6, we want to find a good regression parameter θ for the ideal $\mathcal{F}_\theta$. In ordinary regression, the generative assumption is, slightly reformulated, that the data points are points on the regression hyperplane, plus some independent noise, often even assumed i.i.d. Moreover, the sample points are assumed to be "generic" in the sense that the points are not the same and sufficiently distinct so that one can regress a hyperplane to them.

Thus, for ideal regression it is analogous and natural to postulate as generative model that the input polynomials are "generic" polynomials from the ideal $\mathcal{F}_\theta$ which are then disturbed by additional sampling noise. In the following section, we explain our probabilistic model for genericity, its relation to known types of genericity, and its theoretical implications for the ideal regression problem. The additional noise will be treated in the next section.

Since ideal regression is an algebraic procedure, knowledge about basic algebraic geometry will be required for an understanding of the following sections. In particular, the reader should be at least familiar with the following concepts before reading this section: polynomial rings, ideals, radicals, factor rings, algebraic sets, algebra-geometry correspondence (including Hilbert's Nullstellensatz), primary decomposition, height and dimension theory in rings. A good introduction into the necessary framework can be found in [1].

B.1 Definition of genericity

In the algebraic setting of the paper, we would like to calculate the radical and homogenous saturation of an ideal

$$\mathcal{I} = \langle f_1, \ldots, f_n \rangle.$$

This ideal $\mathcal{I}$ is of a special kind: its generators f_i are random, and are only subject to the constraints that they vanish on the linear subspace S which we want to identify, and that they are homogenous of fixed degree. In order to derive meaningful results on how $\mathcal{I}$ relates to S, or on the solvability of the problem, we need to model this kind of randomness.

In this section, we present a concept called genericity. Informally speaking, a generic situation is a situation without pathological degeneracies. In our case, it is reasonable to believe that apart from the conditions of homogeneity and the vanishing on S, there are no additional degeneracies in the choice of the generators. So, informally spoken, the ideal $\mathcal{I}$ is generated by generic homogenous elements vanishing on S. This section is devoted to developing a formal theory for addressing genericity, as it occurs for example in conditioned sampling as a generative assumption.

The concept of genericity is already widely used in theoretical computer science, combinatorics or discrete mathematics; there, it is however often defined inexactly or not at all, or it is only given as an ad-hoc definition for the particular problem. On the other hand, genericity is a classical concept in algebraic geometry, in particular in the theory of moduli. The interpretation of generic properties as probability-one-properties is also a known concept in applied algebraic geometry, e.g. algebraic statistics. However, the application of probability distributions and genericity to the setting of generic ideals, in particular in the context of conditional probabilities, are original to the best of our knowledge, though not being the first one to involve generic resp. general polynomials, see [4]. Generic polynomials and ideals have been also studied in [3]. A collection of results on generic polynomials and ideals which partly overlap with ours may also be found in the recent paper [5].

Before continuing to the definitions, let us explain what genericity should mean. Intuitively, generic objects are objects without unexpected pathologies or degeneracies. For example, if one studies say n lines in the real plane, one wants to exclude pathological cases where lines lie on each other or where many lines intersect in one point. Having those cases excluded means examining the "generic" case, i.e. the case where there are $n(n+1)/2$ intersections, $n(n+1)$ line segments and so forth. Or when one has n points in the plane, one wants to exclude the pathological cases where for example there are three affinely dependent points, or where there are more sophisticated algebraic dependencies between the points which one wants to exclude, depending on the problem.

In the points example, it is straightforward how one can define genericity in terms of sampling from a probability distribution: one could draw the points under a suitable continuous probability distribution from real two-space. Then, saying that the points are "generic" just amounts to examine properties which are true with probability one for the n points. Affine dependencies for example would then occur with probability zero and are automatically excluded from our interest. One can generalize this idea to the lines example: one can parameterize the lines by a parameter space, which in this case is two-dimensional (slope and ordinate), and then sample lines uniformly distributed in this space (one has of course to make clear what this means). For example, lines lying on each other or more than two lines intersecting at a point would

occur with probability zero, since the part of parameter space for this situation would have measure zero under the given probability distribution.

When we work with polynomials and ideals, the situation gets a bit more complicated, but the idea is the same. Polynomials are uniquely determined by their coefficients, so they can naturally be considered as objects in the vector space of their coefficients. Similarly, an ideal can be specified by giving the coefficients of some set of generators. Let us make this more explicit: suppose first we have given a single polynomial $f \in \mathbb{C}[X_1, \dots X_D]$ of degree k.

In multi-index notation, we can write this polynomial as a finite sum

$$f = \sum_{\alpha \in \mathbb{N}^D} c_\alpha X^\alpha \quad \text{with } c_\alpha \in \mathbb{C}.$$

This means that the possible choices for f can be parameterized by the $\binom{D+k}{k}$ coefficients c_I with $\|I\|_1 \leq k$. Thus polynomials of degree k with complex coefficients can be parameterized by complex $\binom{D+k}{k}$-space.

Algebraic sets can be similarly parameterized by parameterizing the generators of the corresponding ideal. However, this correspondence is not one-to-one, as different generators may give rise to the same zero set. While the parameter space can be made unique by dividing out redundancies, which gives rise to the Hilbert scheme, we will instead use the redundant, though pragmatic characterization in terms of a finite dimensional vector space over $\mathbb{C}$ of the correct dimension.

We will now fix notation for the parameter space of polynomials and endow it with algebraic structure. The extension to ideals will then be derived later. Let us write $\mathcal{M}_k$ for complex $\binom{D+k}{k}$-space (we assume D as fixed), interpreting it as a parameter space for the polynomials of degree k as shown above. Since the parameter space $\mathcal{M}_k$ is isomorphic to complex $\binom{D+k}{k}$-space, we may speak about algebraic sets in $\mathcal{M}_k$. Also, $\mathcal{M}_k$ carries the complex topology induced by the topology on $\mathbb{R}^{2k}$ and by topological isomorphy the Lebesgue measure; thus it also makes sense to speak about probability distributions and random variables on $\mathcal{M}_k$. This dual interpretation will be the main ingredient in our definition of genericity, and will allow us to relate algebraic results on genericity to the probabilistic setting in the applications. As $\mathcal{M}_k$ is a topological space, we may view any algebraic set in $\mathcal{M}_k$ as an event if we randomly choose a polynomial in $\mathcal{M}_k$:

Definition B.1 *Let X be a random variable with values in $\mathcal{M}_k$. Then an event for X is called algebraic event or algebraic property if the corresponding event set in $\mathcal{M}_k$ is an algebraic set. It is called irreducible if the corresponding event set in $\mathcal{M}_k$ is an irreducible algebraic set.*

If an event A is irreducible, this means that if we write A as the event "A_1 and A_2", for algebraic events A_1, A_2, then $A = A_1$, or $A = A_2$. We now give some examples for algebraic properties.

Example B.2 The following events on $\mathcal{M}_k$ are algebraic:

1. The sure event.
2. The empty event.
3. The polynomial is of degree n or less.
4. The polynomial vanishes on a prescribed algebraic set.
5. The polynomial is contained in a prescribed ideal.
6. The polynomial is homogenous of degree n or zero.
7. The polynomial is homogenous.
8. The polynomial is a square.
9. The polynomial is reducible.

Properties 1-6 are additionally irreducible.

We now show how to prove these claims: 1-2 are clear, we first prove that properties 3-6 are algebraic and irreducible. By definition, it suffices to prove that the subset of $\mathcal{M}_k$ corresponding to those polynomials is an irreducible algebraic set. We claim: in any of those cases, the subset in question is moreover a linear subspace, and thus algebraic and irreducible. This can be easily verified by checking directly that if f_1, f_2 fulfill the property in question, then $f_1 + \alpha f_2$ also fulfills the property.

Property 7 is algebraic, since it can be described as the disjunction of the properties "The polynomial is homogenous of degree n or zero" for all $n \leq k$, for some fixed k. Those single properties can be described by linear subspaces of $\mathcal{M}_k$ as above, thus property 7 is parameterized by the union of those linear subspaces. In general, these are not contained in each other, so property 6 is not irreducible.

Property 8 is algebraic, as we can check it through the vanishing of a system of generalized discriminant polynomials. One can show that it is also irreducible since the subset of $\mathcal{M}_k$ in question corresponds to the image of a Veronese map (homogenization to degree k is a strategy); however, since we will not need such a result, we do not prove it here.

Property 9 is algebraic, since factorization can also be checked by sets of equations. One has to be careful here though, since those equations depend on the degrees of the factors. For example, a polynomial of degree 4 may factor into two polynomials of degree 1 and 3, or in two polynomials of degree 2 each. Since in general each possible combination defines different sets of equations and thus different algebraic subsets of $\mathcal{M}_k$, property 8 is in general not irreducible (for $k \leq 3$ it is).

The idea defining a choice of polynomial as generic follows the intuition of the affirmed non-sequitur: a generic, resp. generically chosen polynomial should not fulfill any algebraic property. A generic polynomial, having a particular simple (i.e. irreducible) algebraic property, should not fulfill any other algebraic property which is not logically implied by the first one. Here, algebraic properties are regarded as the natural model for restrictive and degenerate conditions, while their logical negations are consequently interpreted as generic, as we have seen in Example B.2. These considerations naturally lead to the following definition of genericity in a probabilistic context:

Definition B.3 *Let X be a random variable with values in $\mathcal{M}_k$. Then X is called generic, if for any irreducible algebraic events A, B, the following holds:*

The conditional probability $P_X(A|B)$ vanishes if and only if B does not imply A.

In particular, B may also be the sure event.

Note that without giving a further explication, the conditional probability $P_X(A|B)$ is not well-defined, since we condition on the event B which has probability zero. There is also no unique way of remedying this, as for example the Borel-Kolmogorov paradox shows. In section B.2, we will discuss the technical notion which we adopt to ensure well-definedness.

Intuitively, our definition means that an event has probability zero to occur unless it is logically implied by the assumptions. That is, degenerate dependencies between events do not occur.

For example, non-degenerate multivariate Gaussian distributions or Gaussian mixture distributions on $\mathcal{M}_k$ are generic distributions. More general, any positive continuous probability distribution which can be approximated by Gaussian mixtures is generic (see Example B.9). Thus we argue that non-generic random variables are very pathological cases. Note however, that our intention is primarily not to analyze the behavior of particular fixed generic random variables (this is part of classical statistics). Instead, we want to infer statements which follow not from the particular structure of the probability function, but solely from the fact that it is generic, as these statements are intrinsically implied by the conditional postulate in Definition B.3 alone. We will discuss the definition of genericity and its implications in more detail in section B.2.

With this definition, we can introduce the terminology of a generic object: it is a generic random variable which is object-valued.

Definition B.4 *We call a generic random variable with values in $\mathcal{M}_k$ a generic polynomial of degree k. When the degree k is arbitrary, but fixed (and still ≥ 1), we will say that f is a generic polynomial, or that f is generic, if it is clear from the context that f is a polynomial. If the degree k is zero, we will analogously say that f is a generic constant.*

We call a set of constants or polynomials $f_1, \ldots, f_m$ generic if they are generic and independent.

We call an ideal generic if it is generated by a set of m generic polynomials.

We call an algebraic set generic if it is the vanishing set of a generic ideal.

Let $\mathcal{P}$ be an algebraic property on a polynomial, a set of polynomials, an ideal, or an algebraic set (e.g. homogenous, contained in an ideal et.). We will call a polynomial, a set of polynomials, or an ideal, a generic $\mathcal{P}$ polynomial, set, or ideal, if it the conditional of a generic random variable with respect to $\mathcal{P}$.

If $\mathcal{A}$ is a statement about an object (polynomial, ideal etc), and $\mathcal{P}$ an algebraic property, we will say briefly "A generic $\mathcal{P}$ object is $\mathcal{A}$" instead of saying "A generic $\mathcal{P}$ object is $\mathcal{A}$ with probability one".

Note that formally, these objects are all polynomial, ideal, algebraic set etc -valued random variables. By convention, when we state something about a generic object, this will be an implicit probability-one statement. For example, when we say

"A generic green ideal is blue",

this is an abbreviation for the by definition equivalent but more lengthy statement

"Let $f_1, \ldots, f_m$ be independent generic random

variables with values in $\mathcal{M}_{k_1}, \ldots, \mathcal{M}_{k_m}$. If the ideal $\langle f_1, \ldots, f_m \rangle$ is green, then with probability one, it is also blue - this statement is independent of the choice of the k_i and the choice of which particular generic random variables we use to sample.

On the other hand, we will use the verb "generic" also as a qualifier for "constituting generic distribution". So for example, when we say

"The Z of a generic red polynomial is a generic yellow polynomial",

this is an abbreviation of the statement

"Let X be a generic random variable on $\mathcal{M}_k$, let X' be the yellow conditional of X. Then the Z of X' is the red conditional of some generic random variable - in particular this statement is independent of the choice of k and the choice of X."

It is important to note that the respective random variables will not be made explicit in the following subsections, since the statements will rely only on its property of being generic, and not on its particular structure which goes beyond being generic.

As an exemplary application of these concepts, we can formulate the noise-free version of the common marginals problem in terms of generic algebra:

Problem B.5 *Let $\mathfrak{s} = \mathrm{I}(S)$, where S is an unknown d-dimensional subspace of $\mathbb{C}^D$. Let*

$$\mathcal{I} = \langle f_1, \ldots, f_m \rangle$$

with $f_i \in \mathfrak{s}$ generic of fixed degree each (in our case, one and two), such that $\sqrt{\mathcal{I}} = \mathfrak{s}$.

Then determine a reduced H-basis (or another simple generating system) for $\mathfrak{s}$.

We will derive a noisy version for the more general setting of ideal regression in section C.

B.2 Zero-measure conditionals, and relation to other types of genericity

In this section, se will discuss the definition of genericity in Definition B.3 and ensure its well-definedness. Then we will invoke alternative definitions for genericity and show their relation to our probabilistic intuitive approach from section B.1. As this section contains technical details and is not necessary for understanding the rest of the appendix, the reader may opt to skip it.

An important concept in our definition of genericity in Definition B.3 is the conditional probability $P_X(A|B)$. As B is an algebraic set, its probability $P_X(B)$ is zero, so the Bayesian definition of conditional cannot apply. There are several ways to make it well-defined; in the following, we explain the Definition of conditional we use in Definition B.3. The definition of conditional we use is one which is also often applied in this context.

Remark B.6 Let X be a real random variable (e.g. with values in $\mathcal{M}_k$) with probability measure μ. If μ is absolutely continuous, then by the theorem of Radon-Nikodym, there is a unique continuous density p such that

$$\mu(U) = \int_U p \, d\lambda$$

for any Borel-measurable set U and the Lebesgue measure λ. If we assume that p is a continuous function, it is unique, so we may define a restricted measure μ_B on the event set of B by setting

$$\nu(U) = \int_U p \, dH,$$

for Borel subsets of U and the Hausdorff measure H on B. If $\nu(B)$ is finite and non-zero, i.e. ν is absolutely continuous with respect to H, then it can be renormalized to yield a conditional probability measure $\mu(.)|_B = \nu(.)/\nu(B)$. The conditional probability $P_X(A|B)$ has then to be understood as

$$P_X(A|B) = \int_B \mathbb{1}(A \cap B) \, d\mu \mid_B,$$

whose existence in particular implies that the Lebesgue integrals $\nu(B)$ are all finite and non-zero.

As stated, we adopt this as the definition of conditional probability for algebraic sets A and B. It is important to note that we have made implicit assumptions on the random variable X by using the conditionals $P_X(A|B)$ in Remark B.6 (and especially by assuming that they exist): namely, the existence of a continuous density function and existence, finiteness, and non-vanishing of the Lebesgue integrals. Similarly, by stating Definition B.3 for genericity, we have made similar assumptions on the generic random variable X, which can be summarized as follows:

Assumption B.7 *X is an absolutely continuous random variable with continuous density function p, and for every algebraic event B, the Lebesgue integrals*

$$\int_B p \, dH,$$

where H is the Hausdorff measure on B, are non-zero and finite.

This assumption implies the existence of all conditional probabilities $P_X(A|B)$ in Definition B.3, and are also necessary in the sense that they are needed for the conditionals to be well-defined. On the other hand, if those assumptions are fulfilled for a random variable, it is automatically generic:

Remark B.8 Let X be a $\mathcal{M}_k$-valued random variable, fulfilling the Assumptions in B.7. Then, the probability density function of X is strictly positive. Moreover, X is a generic random variable.

proof 1 Let X be a $\mathcal{M}_k$-valued random variable fulfilling the Assumptions in B.7. Let p be its continuous probability density function.

We first show positivity: If X would not be strictly positive, then p would have a zero, say x. Taking $B = \{x\}$, the integral $\int_B p\, dH$ vanishes, contradicting the assumption.

Now we prove genericity, i.e. that for arbitrary irreducible algebraic properties A, B such that B does not imply A, the conditional probability $P_X(A|B)$ vanishes. Since B does not imply A, the algebraic set defined by B is not contained in A. Moreover, as B and A are irreducible and algebraic, $A \cap B$ is also of positive codimension in B. Now by assumption, X has a positive continuous probability density function f which by assumption restricts to a probability density on B, being also positive and continuous. Thus the integral

$$P_X(A|B) = \int_B \mathbb{1}_A f(x)\, dH,$$

where H is the Hausdorff measure on B, exists. Moreover, it is zero, as we have derived that A has positive codimension in B.

This means that already under mild assumptions, which merely ensure well-definedness of the statement in the Definition B.3 of genericity, random variables are generic. The strongest of the comparably mild assumptions are the convergence of the conditional integrals, which allow us to renormalize the conditionals for all algebraic events. In the following example, a generic and a non-generic probability distribution are presented.

Example B.9 Gaussian distributions and Gaussian mixture distributions are generic, since for any algebraic set B, we have

$$\int_B \mathbb{1}_{\mathcal{B}(t)}\, dH = O(t^{\dim B}),$$

where $\mathcal{B}(t) = \{x \in \mathbb{R}^n \,;\, \|x\| < t\}$ is the open disc with radius t. Note that this particular bound is false in general and may grow arbitrarily large when we omit B being algebraic, even if B is a smooth manifold. Thus $P_X(A|B)$ is bounded from above by an integral (or a sum) of the type

$$\int_0^\infty \exp(-t^2) t^a\, dt \quad \text{with } a \in \mathbb{N}$$

which is known to be finite.

Furthermore, sums of generic distributions are again generic; also, one can infer that any continuous probability density dominated by the distribution of a generic density defines again a generic distribution.

An example of a non-generic but smooth distribution is given by the density function

$$p(x, y) = \frac{1}{\mathcal{N}} e^{-x^4 y^4}$$

where $\mathcal{N}$ is some normalizing factor. While p is integrable on $\mathbb{R}^2$, its restriction to the coordinate axes $x = 0$ and $y = 0$ is constant and thus not integrable.

Now we will examine different known concepts of genericity and relate them briefly to the one we have adopted.

A definition of genericity in combinatorics and geometry which can be encountered in different variations is that there exist no degenerate interpolating functions between the objects:

Definition B.10 *Let $P_1, \ldots, P_m$ be points in the vector space $\mathbb{C}^n$. Then $P_1, \ldots, P_m$ are general position (or generic, general) if no $n+1$ points lie on a hyperplane. Or, in a stronger version: for any $d \in \mathbb{N}$, no (possibly inhomogenous) polynomial of degree d vanishes on $\binom{n+d}{d} + 1$ different P_i.*

As $\mathcal{M}_k$ is a finite dimensional $\mathbb{C}$-vector space, this definition is in principle applicable to our situation. However, this definition is deterministic, as the P_i are fixed and no random variables, and thus preferable when making deterministic statements. Note that the stronger definition is equivalent to postulating general position for the points $P_1, \ldots, P_m$ in any polynomial kernel feature space.

Since not lying on a hyperplane (or on a hypersurface of degree d) in $\mathbb{C}^n$ is a non-trivial algebraic property for any point which is added beyond the n-th (resp. the $\binom{n+d}{d}$-th) point P_i (interpreted as polynomial in $\mathcal{M}_k$), our definition of genericity implies general position. This means that generic polynomials $f_1, \ldots, f_m \in \mathcal{M}_k$ (almost surely) have the deterministic property of being in general position as stated in Definition B.11. A

converse is not true for two reasons: first, the P_i are fixed and no random variables. Second, even if one would define genericity in terms of random variables such that the hyperplane (resp. hypersurface) conditions are never fulfilled, there are no statements made on conditionals or algebraic properties other than containment in a hyperplane, also Lebesgue zero sets are not excluded from occuring with positive probability.

Another example where genericity classically occurs is algebraic geometry, where it is defined rather general for moduli spaces. While the exact definition may depend on the situation or the particular moduli space in question, and is also not completely consistent, in most cases, genericity is defined as follows: general, or generic, properties are properties which hold on a Zariski-open subset of an (irreducible) variety, while very generic properties hold on a countable intersection of Zariski-open subsets (which are thus paradoxically "less" generic than general resp. generic properties in the algebraic sense, as any general resp. generic property is very generic, but the converse is not necessarily true). In our special situation, which is the affine parameter space of tuples of polynomials, these definitions can be rephrased as follows:

Definition B.11 *Let $B \subseteq \mathbb{C}^k$ be an irreducible algebraic set, let $P = (f_1, \ldots, f_m)$ be a tuple of polynomials, viewed as a point in the parameter space B. Then a statement resp. property A of P is called very generic if it holds on the complement of some countable union of algebraic sets in B. A statement resp. property A of P is called general (or generic) if it holds on the complement of some finite union of algebraic sets in B.*

This definition is more or less equivalent to our own; however, our definition adds the practical interpretation of generic/very generic/general properties being true with probability one, while their negations are subsequently true with probability zero. In more detail, the correspondence is as follows: If we restrict ourselves only to algebraic properties A, it is equivalent to say that the property A is very generic, or general for the P in B, and to say with our original definition that a generic P fulfilling B is also A; since if A is by assumption an algebraic property, it is both an algebraic set and a complement of a finite (countable) union of algebraic sets in an irreducible algebraic set, so A must be equal to an irreducible component of B; since B is irreducible, this implies equality of A and B. On the other hand, if A is an algebraic property, it is equivalent to say that the property not-A is very generic, or general for the P in B, and to say with our original definition that a generic P fulfilling B is not A - this corresponds intuitively to the probability-zero condition $P(A|B) = 0$ which states that non-generic cases do not occur. Note that by assumption, not-A is then always the complement of a finite union of algebraic sets.

B.3 Arithmetic of generic polynomials

In this subsection, we study how generic polynomials behave under classical operations in rings and ideals. This will become important later when we study generic polynomials and ideals.

To introduce the reader to our notation of genericity, and since we will use the presented facts and similar notations implicitly later, we prove the following:

Lemma B.12 *Let $f \in \mathbb{C}[X_1, \ldots, X_D]$ be generic of degrees k. Then:*
(i) *The product αf is generic of degree k for any fixed $\alpha \in \mathbb{C} \setminus \{0\}$.*
(ii) *The sum $f + g$ is generic of degree k for any $g \in \mathbb{C}[X_1, \ldots, X_D]$ of degree k or smaller.*
(iii) *The sum $f + g$ is generic of degree k for any generic $g \in \mathbb{C}[X_1, \ldots, X_D]$ of degree k or smaller.*

proof 2 (i) is clear since the coefficients of g_1 are multiplied only by a constant. (ii) follows directly from the definitions since adding a constant g only shifts the coefficients without changing genericity. (iii) follows since f, g are independently sampled: if there were algebraic dependencies between the coefficients of $f+g$, then either f or g was not generic, or the f, g are not independent, which both would be a contradiction to the assumption.

Recall again what this Lemma means: for example, Lemma B.12 (i) does not say, as one could think:

"Let X be a generic random variable with values in the vector space of degree k polynomials. Then $X = \alpha X$ for any $\alpha \in \mathbb{C} \setminus \{0\}$."

The correct translation of Lemma B.12 (i) is:

"Let X be a generic random variable with values in the vector space of degree k polynomials. Then $X' = \alpha X$ for any fixed $\alpha \in \mathbb{C} \setminus \{0\}$ is a generic random variable with values in the vector space of degree k polynomials"

The other statements in Lemma B.12 have to be interpreted similarly.

The following remark states how genericity translates

through dehomogenization:

Lemma B.13 *Let $f \in \mathbb{C}[X_1, \ldots, X_D]$ be a generic homogenous polynomial of degree d.*
Then the dehomogenization $f(X_1, \ldots, X_{D-1}, 1)$ is a generic polynomial of degree d in the polynomial ring $\mathbb{C}[X_1, \ldots, X_{D-1}]$.

Similarly, let $\mathfrak{s} \subseteq \mathbb{C}[X_1, \ldots, X_D]$ be a generic homogenous ideal. Let $f \in \mathfrak{s}$ be a generic homogenous polynomial of degree d.
Then the dehomogenization $f(X_1, \ldots, X_{D-1}, 1)$ is a generic polynomial of degree d in the dehomogenization of $\mathfrak{s}$.

proof 3 For the first statement, it suffices to note that the coefficients of a homogenous polynomial of degree d in the variables $X_1, \ldots, X_D$ are in bijection with the coefficients of a polynomial of degree d in the variables $X_1, \ldots, X_{D-1}$ by dehomogenization. For the second part, recall that the dehomogenization of $\mathfrak{s}$ consists exactly of the dehomogenizations of elements in $\mathfrak{s}$. In particular, note that the homogenous elements of $\mathfrak{s}$ of degree d are in bijection to the elements of degree d in the dehomogenization of $\mathfrak{s}$. The claims then follows from the definition of genericity.

B.4 Dimension of generic spans and ideals

In this subsection, we will derive the first results on generic ideals. We will derive an statement about spans of generic polynomials, and generic versions of Krull's principal ideal and height theorems which will be the main tool in controlling the structure of generic ideals. This has immediate applications for the cumulant comparison problem.

We begin with a probably commonly known result, formulated in terms of genericity:

Proposition B.14 *Let P be an algebraic property such that the polynomials with property P form a vector space V. Let $f_1, \ldots, f_m \in \mathbb{C}[X_1, \ldots X_D]$ be generic polynomials satisfying P. Then*

$$\operatorname{rank} \operatorname{span}(f_1, \ldots, f_m) = \min(m, \dim V).$$

proof 4 It suffices to prove: if $i \leq M$, then f_i is linearly independent from $f_1, \ldots f_{i-1}$ with probability one. Assuming the contrary would mean that for some i, we have

$$f_i = \sum_{k=0}^{i-1} f_k c_k \quad \text{for some } c_k \in \mathbb{C},$$

thus giving several equations on the coefficients of f_i. But these are fulfilled with probability zero by the genericity assumption, so the claim follows.

This may be seen as a straightforward generalization of the statement: the span of n generic points in $\mathbb{C}^D$ has dimension $\min(n, D)$.

We now proceed to another nontrivial result which will now allow us to formulate a generic version of Krull's principal ideal theorem:

Proposition B.15 *Let $Z \subseteq \mathbb{C}^D$ be a non-empty algebraic set, let $f \in \mathbb{C}[X_1, \ldots X_D]$ generic. Then f is a non-zero divisor in $\mathcal{O}(Z) = \mathbb{C}[X_1, \ldots X_D]/\operatorname{I}(Z)$.*

proof 5 We claim: being a zero divisor in $\mathcal{O}(Z)$ is an irreducible algebraic property. We will prove that the zero divisors in $\mathcal{O}(Z)$ form a linear subspace of $\mathcal{M}_k$, and linear spaces are irreducible.

For this, one checks that sums and scalar multiples of zero divisors are also zero divisors: if g_1, g_2 are zero divisors, there must exist h_1, h_2 such that $g_1 h_1 = g_2 h_2 = 0$. Now for any $\alpha \in \mathbb{C}$, we have that

$$(g_1 + \alpha g_2)(h_1 h_2) = (g_1 h_1) h_2 + (g_2 h_2) \alpha h_1 = 0.$$

This proves that $(g_1 + \alpha g_2)$ is also a zero divisor, proving that the zero divisors form a linear subspace and thus an irreducible algebraic property.

To apply the genericity assumption to argue that this event occurs with probability zero, we must exclude the possibility that being a zero divisor is trivial, i.e. always the case. This is equivalent to proving that the linear subspace has positive codimension, which is true if and only if there exists a non-zero divisor in $\mathcal{O}(Z)$. But a non-zero divisor always exists since we have assumed Z is non-empty: thus $\operatorname{I}(Z)$ is a proper ideal, and $\mathcal{O}(Z)$ contains $\mathbb{C}$, which contains a non-zero divisor, e.g. the one.

So by the genericity assumption, the event that f is a zero divisor occurs with probability zero, i.e. a generic f is not a zero divisor. Note that this does not depend on the degree of f.

This result is already known, compare Conjecture B in [5].

A straightforward generalization using the same proof technique is given by the following

Corollary B.16 *Let $\mathcal{I} \subseteq \mathbb{C}[X_1, \ldots, X_D]$, let P be a non-trivial algebraic property. Let $f \in \mathbb{C}[X_1, \ldots X_D]$ be a generic polynomial with property P. If one can*

write $f = f' + c$, where f' is a generic polynomial subject to some property P', and c is a generic constant, then f is non-zero divisor in $\mathbb{C}[X_1, \ldots, X_D]/\mathcal{I}$.

proof 6 First note that f is a zero divisor in $\mathbb{C}[X_1, \ldots, X_D]/\mathcal{I}$ if and only if f is a zero divisor in $\mathbb{C}[X_1, \ldots, X_D]/\sqrt{\mathcal{I}}$. This allows us to reduce to the case that $\mathcal{I} = \mathrm{I}(Z)$ for some algebraic set $Z \subseteq \mathbb{C}^D$.

Now, as in the proof of Proposition B.15, we see that being a zero divisor in $\mathcal{O}(Z)$ is an irreducible algebraic property and corresponds to a linear subspace of $\mathcal{M}_k$, where $k = \deg f$. The zero divisors with property P are thus contained in this linear subspace. Now let f be generic with property P as above. By assumption, we may write $f = f' + c$. But c is (generically) a non-zero divisor, so f is also not a zero divisor, since the zero divisors form a linear subspace of $\mathcal{M}_k$. Thus f is non-zero divisor. This proves the claim.

Note that Proposition B.15 is actually a special case of Corollary B.16, since we can write any generic polynomial f as $f' + c$, where f' is generic of the same degree, and c is a generic constant.

The major tool to deal with the dimension of generic intersections is Krull's principal ideal theorem:

Theorem B.17 (Krull's principal ideal theorem) *Let R be a commutative ring with unit, let $f \in R$ be non-zero and non-invertible. Then*

$$\mathrm{ht}\langle f \rangle \leq 1,$$

with equality if and only if f is not a zero divisor in R.

The reader unfamiliar with height theory may take

$$\mathrm{ht}\,\mathcal{I} = \mathrm{codim}\,\mathrm{V}(\mathcal{I})$$

as the definition for the height of an ideal (cave: codimension has to be taken in R).

Reformulated geometrically for our situation, Krull's principal ideal theorem implies:

Corollary B.18 *Let Z be a non-empty algebraic set in $\mathbb{C}^D$. Then*

$$\mathrm{codim}(Z \cap \mathrm{V}(f)) \leq \mathrm{codim}\, Z + 1.$$

proof 7 Apply Krull's principal ideal theorem to the ring $R = \mathcal{O}(Z) = \mathbb{C}[X_1, \ldots, X_D]/\,\mathrm{I}(Z)$.

Together with Proposition B.15, one gets a generic version of Krull's principal ideal theorem:

Theorem B.19 (Generic principal ideal theorem) *Let Z be a non-empty algebraic set in $\mathbb{C}^D$, let $R = \mathcal{O}(Z)$, and let $f \in \mathbb{C}[X_1, \ldots, X_D]$ be generic. Then we have*

$$\mathrm{ht}\langle f \rangle = 1.$$

In its geometric formulation, we obtain the following result.

Corollary B.20 *Consider an algebraic set $Z \subseteq \mathbb{C}^D$, and the algebraic set $\mathrm{V}(f)$ for some generic $f \in \mathbb{C}[X_1, \ldots, X_D]$. Then*

$$\mathrm{codim}(Z \cap \mathrm{V}(f)) = \min(\mathrm{codim}\, Z + 1,\ D + 1).$$

proof 8 This is just a direct reformulation of Theorem B.19 in the vein of Corollary B.18. The only additional thing that has to be checked is the case where $\mathrm{codim}\, Z = D + 1$, which means that Z is the empty set. In this case, the equality is straightforward.

The generic version of the principal ideal theorem straightforwardly generalizes to a generic version of Krull's height theorem. We first mention the original version:

Theorem B.21 (Krull's height theorem) *Let R be a commutative ring with unit, let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subseteq R$ be an ideal. Then*

$$\mathrm{ht}\,\mathcal{I} \leq m,$$

with equality if and only if $f_1, \ldots, f_m$ is an R-regular sequence, i.e. f_i is not invertible and not a zero divisor in the ring $R/\langle f_1, \ldots, f_{i-1} \rangle$ for all i.

The generic version can be derived directly from the generic principal ideal theorem:

Theorem B.22 (Generic height theorem) *Let Z be an algebraic set in $\mathbb{C}^D$, let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ be a generic ideal in $\mathbb{C}[X_1, \ldots, X_D]$. Then*

$$\mathrm{ht}(\mathrm{I}(Z) + \mathcal{I}) = \min(\mathrm{codim}\, Z + m,\ D + 1).$$

proof 9 We will write $R = \mathcal{O}(Z)$ for abbreviation.

First assume $m \leq D + 1 - \mathrm{codim}\, Z$. It suffices to show that $f_1, \ldots, f_m$ forms an R-regular sequence, then apply Krull's height theorem. In Proposition B.15, we have proved that f_i is not a zero divisor in the ring $\mathcal{O}(Z \cap \mathrm{V}(f_1, \ldots, f_{i-1}))$ (note that the latter ring is nonzero by Krull's height theorem). By Hilbert's Nullstellensatz, this is the same as the ring $R/\sqrt{\langle f_1, \ldots, f_{i-1} \rangle}$. But by the definition of radical, this implies that f_i is a non-zero divisor in the ring $R/\langle f_1, \ldots, f_{i-1} \rangle$, since if $f_i \cdot h = 0$ in the first ring, we have

$$(f_i \cdot h)^N = f_i \cdot (f_i^{N-1} h^N) = 0$$

in the second. Thus the f_i form an R-regular sequence, proving the theorem for the case $m \leq D+1-\operatorname{codim} Z$.

If now $m > k := D + 1 - \operatorname{codim} Z$, the above reasoning shows that the radical of $\mathrm{I}(Z) + \langle f_1, \ldots, f_k \rangle$ is the module $\langle 1 \rangle$, which means that those are equal. Thus

$$\mathrm{I}(Z) + \langle f_1, \ldots, f_k \rangle = \mathrm{I}(Z) + \langle f_1, \ldots, f_m \rangle = \langle 1 \rangle,$$

proving the theorem.

Note that we could have proved the generic height theorem also directly from the generic principal ideal theorem by induction.

Again, we give the geometric interpretation of Krull's height theorem:

Corollary B.23 *Let Z_1 be an algebraic set in $\mathbb{C}^D$, let Z_2 be a generic algebraic set in $\mathbb{C}^D$. Then one has*

$$\operatorname{codim}(Z_1 \cap Z_2) = \min(\operatorname{codim} Z_1 + \operatorname{codim} Z_2,\ D+1).$$

proof 10 This follows directly from two applications of the generic height theorem B.22: first for $Z = \mathbb{C}^D$ and $Z_2 = \mathrm{V}(\mathcal{I})$, showing that $\operatorname{codim} Z_2$ is equal to the number m of generators of $\mathcal{I}$; then, for $Z = Z_1$ and $Z_2 = \mathrm{V}(\mathcal{I})$, and substituting $m = \operatorname{codim} Z_2$.

We can now immediately formulate a homogenous version of Proposition B.23:

Corollary B.24 *Let Z_1 be a homogenous algebraic set in $\mathbb{C}^D$, let Z_2 be a generic homogenous algebraic set in $\mathbb{C}^D$. Then one has*

$$\operatorname{codim}(Z_1 \cap Z_2) = \min(\operatorname{codim} Z_1 + \operatorname{codim} Z_2,\ D).$$

proof 11 Note that homogenization and dehomogenization of a non-empty algebraic set do not change its codimension, and homogenous algebraic sets always contain the origin. Also, one has to note that by Lemma B.13, the dehomogenization of Z_2 is a generic algebraic set in $\mathbb{C}^{D-1}$.

Finally, using Corollary B.16, we want to give a more technical variant of the generic height theorem, which will be of use in later proofs. First, we introduce some abbreviating notations:

Definition B.25 *Let $f \in \mathbb{C}[X_1, \ldots X_D]$ be a generic polynomial with property P. If one can write $f = f' + c$, where f' is a generic polynomial subject to some property P', and c is a generic constant, we say that f has independent constant term. If c is generic and independent with respect to some collection of generic objects, we say that f has independent constant term with respect to that collection.*

In this terminology, Corollary B.16 rephrases as: a generic polynomial with independent constant term is a non-zero divisor. Using this, we can now formulate the corresponding variant of the generic height theorem:

Lemma B.26 *Let Z be an algebraic set in $\mathbb{C}^D$. Let $f_1, \ldots, f_m \in \mathbb{C}[X_1, \ldots, X_D]$ be generic, possibly subject to some algebraic properties, such that f_i has independent constant term with respect to Z and $f_1, \ldots, f_{i-1}$. Then*

$$\operatorname{ht}(\mathrm{I}(Z) + \mathcal{I}) = \min(\operatorname{codim} Z + m,\ D+1).$$

proof 12 Using Corollary B.16, one obtains that f_i is non-zero divisor modulo $\mathrm{I}(Z) + \langle f_1, \ldots, f_{i+1} \rangle$. Using Krull's height theorem yields the claim.

B.5 Dimension of conditioned generic ideals

The generic height theorem B.22 has allowed us to make statements about the structure of ideals generated by generic elements without constraints. However, the ideal $\mathcal{I}$ in our the cumulant comparison problem is generic subject to constraints: namely, its generators are contained in a prescribed ideal, and they are homogenous. In this subsection, we will use the theory developed so far to study generic ideals and generic ideals subject to some algebraic properties, e.g. generic ideals contained in other ideals. We will use these results to derive an identifiability result on the marginalization problem which has been derived already less rigourously in the supplementary material of [6] for the special case of Stationary Subspace Analysis.

Proposition B.27 *Let $\mathfrak{s} \subseteq \mathbb{C}[X_1, \ldots, X_D]$ be an ideal, having an H-basis $g_1, \ldots, g_n$. Let*

$$\mathcal{I} = \langle f_1, \ldots, f_m \rangle, \quad m \geq \max(D+1, n)$$

with generic $f_i \in \mathfrak{s}$ such that

$$\deg f_i \geq \max_j (\deg g_j) \quad \textit{for all } 1 \leq i \leq m.$$

Then $\mathcal{I} = \mathfrak{s}$.

proof 13 First note that since the g_i form a degree-first Groebner basis, a generic $f \in \mathfrak{s}$ is of the form

$$f = \sum_{k=1}^{n} g_k h_k \quad \text{with generic } h_k,$$

where the degrees of the h_k are appropriately chosen, i.e. $\deg h_k \leq \deg f - \deg g_k$.

So we may write

$$f_i = \sum_{k=1}^{n} g_k h_{ki} \quad \text{with generic } h_{ki},$$

where the h_{ki} are generic with appropriate degrees, and independently chosen. We may also assume that the f_i are ordered increasingly by degree.

To prove the statement, it suffices to show that $g_j \in \mathcal{I}$ for all j. Now the height theorem B.22 implies that

$$\langle h_{11}, \dots h_{1m} \rangle = \langle 1 \rangle,$$

since the h_{ki} were independently generic, and $m \geq D+1$. In particular, there exist polynomials $s_1, \dots, s_m$ such that

$$\sum_{i=1}^{m} s_i h_{1i} = 1.$$

Thus we have that

$$\begin{aligned}\sum_{i=1}^{m} s_i f_i &= \sum_{i=1}^{m} s_i \sum_{k=1}^{n} g_k h_{ki} = \sum_{k=1}^{n} g_k \sum_{i=1}^{m} s_i h_{ki} \\ &= g_1 + \sum_{k=2}^{n} g_k \sum_{i=1}^{m} s_i h_{ki} =: g_1 + \sum_{k=2}^{n} g_k h'_k.\end{aligned}$$

Subtracting a suitable multiple of this element from the $f_1, \dots, f_m$, we obtain

$$f'_i = \sum_{k=2}^{n} g_k (h_{ki} - h_{1i} h'_k) =: \sum_{k=2}^{n} g_k h'_{ki}.$$

We may now consider $h_{1i} h'_k$ as fixed, while the h_{ki} are generic. In particular, the h'_{ki} have independent constant term, and using Lemma B.26, we may conclude that

$$\langle h'_{21}, \dots, h'_{2m} \rangle = \langle 1 \rangle,$$

allowing us to find an element of the form

$$g_2 + \sum_{k=3}^{n} g_k \cdot \dots$$

in $\mathcal{I}$. Iterating this strategy by repeatedly applying Lemma B.26, we see that g_k is contained in $\mathcal{I}$, because the ideals $\mathcal{I}$ and $\mathfrak{s}$ have same height. Since the numbering for the g_j was arbitrary, we have proved that $g_j \in \mathcal{I}$, and thus the proposition.

The following example shows that in general, we may not take the degrees of the f_i lower than the maximal degree of the g_j in the proposition, i.e. the condition on the degrees is necessary:

Example B.28 Keep the notations of Proposition B.27. Let $\mathfrak{s} = \langle X_2 - X_1^2, X_3 \rangle$, and $f_i \in \mathfrak{s}$ generic of degree one. Then

$$\langle f_1, \dots, f_m \rangle = \langle X_3 \rangle.$$

This example can be generalized to yield arbitrarily bad results if the condition on the degrees is not fulfilled.

However note that when $\mathfrak{s}$ is generated by linear forms, as in the marginalization problem, the condition on the degrees vanishes.

We may use Proposition B.27 also in another way to derive a more detailed version of the generic height theorem for constrained ideals:

Proposition B.29 *Let V be a fixed d-codimensional algebraic set in $\mathbb{C}^D$. Assume that there exist d generators $g_1, \dots, g_d$ for $\mathrm{I}(V)$. Let $f_1, \dots, f_m$ be generic forms in $\mathrm{I}(V)$ such that $\deg f_i \geq \deg g_i$ for $1 \leq i \leq \min(m, d)$. Then we can write $\mathrm{V}(f_1, \dots, f_m) = V \cup U$ with U an algebraic set of*

$$\operatorname{codim} U \geq \min(m,\ D+1),$$

the equality being strict for $m < \operatorname{codim} V$.

proof 14 If $m \geq D+1$, this is just a direct consequence of Proposition B.27.

First assume $m = d$. Consider the image of the situation modulo $X_m, \dots, X_D$. This corresponds to looking at the situation

$$\mathrm{V}(f_1, \dots, f_m) \cap H \subseteq H \cong \mathbb{C}^{m-1},$$

where H is the linear subspace given by $X_m = \dots = X_D = 0$. Since the coordinate system was generic, the images of the f_i will be generic, and we have by Proposition B.27 that $\mathrm{V}(f_1, \dots, f_m) \cap H = V \cap H$. Also, the H can be regarded as a generic linear subspace, thus by Corollary B.23, we see that $\mathrm{V}(f_1, \dots, f_m)$ consists of V and possibly components of equal or higher codimension. This proves the claim for $m = \operatorname{codim} V$.

Now we prove the case $m \geq d$. We may assume that $m = D+1$ and then prove the statement for the sets $\mathrm{V}(f_1, \dots, f_i), d \leq i \leq m$. By the Lasker-Noether-Theorem, we may write

$$\mathrm{V}(f_1, \dots, f_d) = V \cup Z_1 \cup \dots \cup Z_N$$

for finitely many irreducible components Z_j with $\operatorname{codim} Z_j \geq \operatorname{codim} V$. Proposition B.27 now states that

$$\mathrm{V}(f_1, \dots, f_m) = V.$$

For $i \geq d$, write now

$$Z_{ji} = Z_j \cap \mathrm{V}(f_1, \dots, f_i) = Z_j \cap \mathrm{V}(f_{d+1}, \dots, f_i).$$

With this, we have the equalities

$$\begin{aligned}\mathrm{V}(f_1,\ldots,f_i) &= \mathrm{V}(f_1,\ldots,f_d)\cap\mathrm{V}(f_{d+1},\ldots,f_i)\\ &= V\cup(Z_1\cap\mathrm{V}(f_{d+1},\ldots,f_i))\cup\ldots\\ &\qquad\cup(Z_N\cap\mathrm{V}(f_{d+1},\ldots,f_i))\\ &= V\cup Z_{1i}\cup\cdots\cup Z_{Ni}.\end{aligned}$$

for $i\geq d$. Thus, reformulated, Proposition B.27 states that $Z_{jm}=\varnothing$ for any j. We can now infer by Krull's principal ideal theorem B.17 that

$$\operatorname{codim} Z_{ji}\leq\operatorname{codim} Z_{j,i-1}+1$$

for any i,j. But since $\operatorname{codim} Z_{jm}=D+1$, and $\operatorname{codim} Z_{jd}\geq d$, we thus may infer that $\operatorname{codim} Z_{ji}\geq i$ for any $d\leq i\leq m$. Thus we may write

$$\mathrm{V}(f_1,\ldots,f_i)=V\cup U\quad\text{with } U=Z_{1i}\cup\cdots\cup Z_{Ni}$$

with $\operatorname{codim} U\geq i$, which proves the claim for $m\geq\operatorname{codim} V$.

The case $m<\operatorname{codim} V$ can be proved again similarly by Krull's principal ideal theorem B.17: it states that the codimension of $\mathrm{V}(f_1,\ldots,f_i)$ increases at most by one with each i, and we have seen above that it is equal to $\operatorname{codim} V$ for $i=\operatorname{codim} V$. Thus the codimension of $\mathrm{V}(f_1,\ldots,f_i)$ must have been i for every $i\leq\operatorname{codim} V$. This yields the claim.

Note that depending on V and the degrees of the f_i, it may happen that even in the generic case, the equality in Proposition B.29 is not strict for $m\geq\operatorname{codim} V$:

Example B.30 Let V be a generic linear subspace of dimension d in $\mathbb{C}^D$, let $f_1,\ldots,f_m\in\mathrm{I}(V)$ be generic with degree one. Then $\mathrm{V}(f_1,\ldots,f_m)$ is a generic linear subspace of dimension $\max(D-m,d)$ containing V. In particular, if $m\geq D-d$, then $\mathrm{V}(f_1,\ldots,f_m)=V$. In this example, $U=\mathrm{V}(f_1,\ldots,f_m)$, if $m<\operatorname{codim} V$, with codimension m, and $U=\varnothing$, if $m\geq\operatorname{codim} V$, with codimension $D+1$.

Similarly, one may construct generic examples with arbitrary behavior for $\operatorname{codim} U$ when $m\geq\operatorname{codim} V$, by choosing V and the degrees of f_i appropriately.

As in the geometric version for the height theorem, we may derive the following geometric interpretation of this result:

Corollary B.31 *Let $V\subseteq Z_1$ be fixed algebraic sets in $\mathbb{C}^D$. Let Z_2 be a generic algebraic set in $\mathbb{C}^D$ containing V. Then*

$$\begin{aligned}&\operatorname{codim}(Z_1\cap Z_2\setminus V)\geq\\ &\qquad\min(\operatorname{codim}(Z_1\setminus V)+\operatorname{codim}(Z_2\setminus V),\ D+1).\end{aligned}$$

Informally, we have derived a height theorem type result for algebraic sets under the constraint that they contain another prescribed algebraic set V.

We also want to give a homogenous version of Proposition B.29, since the ideals in the paper are generated by homogenous forms:

Corollary B.32 *Let V be a fixed homogenous algebraic set in $\mathbb{C}^D$. Let $f_1,\ldots,f_m$ be generic homogenous forms in $\mathrm{I}(V)$, satisfying the degree condition as in Proposition B.29. Then $\mathrm{V}(f_1,\ldots,f_m)=V+U$ with U an algebraic set fulfilling*

$$\operatorname{codim} U\geq\min(m,\ D).$$

In particular, if $m>D$, then $\mathrm{V}(f_1,\ldots,f_m)=V$. Also, the maximal dimensional part of $\mathrm{V}(f_1,\ldots,f_m)$ equals V if and only if $m>D-\dim V$.

proof 15 This follows immediately by dehomogenizing, applying Proposition B.29, and homogenizing again.

B.6 Hilbert series of generic ideals

In this section we will study the dimension of the vector spaces of homogenous polynomials of fixed degrees. A classical tool to do this in commutative algebra are Hilbert series; let us introduce some notations first.

Notation B.33 *We will write $R=\mathbb{C}[X_1,\ldots,X_D]$. Let $\mathcal{I}$ be some ideal of R, or R itself. We will denote the $\mathbb{C}$-vector space of homogenous polynomials of degree k in $\mathcal{I}$ by $\mathcal{I}_k$.*

The Hilbert series links the dimensions of those vector spaces to the graded structure of the whole ideal:

Definition B.34 *Let $\mathcal{I}$ be some ideal of R. Then the Hilbert series of $\mathcal{I}$ is the power series*

$$H(\mathcal{I})(t)=\sum_{k=0}^{\infty}t^k\left(\dim(R_k)-\dim(\mathcal{I}_k)\right).$$

It is classically known that the a_k satisfy a polynomial relation for $k\geq M$ with a big enough M. However, we will be mainly interested in the exact coefficients a_k below $k\leq M$ when the ideal $\mathcal{I}$ is conditioned generic. I.e. we are interested in the situation where we have some ideal $\mathfrak{s}$, and an ideal $\mathcal{I}$ generated by generic homogenous polynomials $f_1,\ldots,f_m$ in $\mathfrak{s}$. Since in this situation, we have $\mathcal{I}\subseteq\mathfrak{s}$, we will consider the Hilbert series of the difference

$$\begin{aligned}H(\mathcal{I}/\mathfrak{s})(t) &= H(\mathcal{I})(t)-H(\mathfrak{s})(t)\\ &=\sum_{k=0}^{\infty}t^k\left(\dim(\mathfrak{s}_k)-\dim(\mathcal{I}_k)\right).\end{aligned}$$

The following homogenous version of Proposition B.27 will allow us to study this further:

Proposition B.35 *Let $\mathfrak{s} \subseteq R$ be a homogenously saturated ideal generated by n homogenous elements of degree at most δ. Let*

$$\mathcal{I} = \langle f_1, \ldots, f_m \rangle, \quad m \geq \max(D+1, n)$$

with generic $f_i \in \mathfrak{s}$ such that

$$\deg f_i \geq \delta \quad \textit{for all } 1 \leq i \leq m.$$

For any $1 \leq j \leq D$, we then have

$$\begin{aligned} \mathfrak{s} &= (\mathcal{I} : X_j) \\ &= \{g \in R \ : \ gX_D^n \in \mathcal{I} \textit{ for some } n \in \mathbb{N}\}. \end{aligned}$$

proof 16 Since the f_i are generic, we may make a permutation of variables without altering the statement; i.e. we may assume that $j = D$. The proof strategy will be to derive a homogenous version of Proposition B.27. In order to do this, we first dehomogenize every object with respect to X_D, i.e. we substitute 1 for X_D. Then, we will be in the situation of Proposition B.27 for the dehomogenized objects, and from that, we can conclude the statement for our homogenous version.

Let us first fix some notation: Let $g_1, \ldots, g_n$ be some generators for $\mathfrak{s}$. Let $\mathfrak{s}'$ be the dehomogenization of $\mathfrak{s}$. The ideal $\mathfrak{s}'$ is generated by $g_1', \ldots, g_n'$ in the $D-1$ variables $X_1, \ldots, X_{D-1}$, where g_i' is the dehomogenization of g_i. The dehomogenization of $\mathcal{I}$ is also an ideal in $D-1$ variables, generated by the dehomogenizations f_i' of f_i. By Lemma B.13, the f_i' are generic polynomials in $\mathfrak{s}'$, of same degrees as the f_i.

Now we are in the situation of Proposition B.27: $\mathcal{I}'$ is an ideal generated by the generic polynomials f_i' in $\mathfrak{s}'$. We also have $\deg f_i' \geq \max_i \deg g_i'$. Thus we may conclude that $\mathcal{I}' = \mathfrak{s}'$.

To prove the main statement from this, it now suffices to prove that $g_1 \in (\mathcal{I} : X_D)$, since the numbering of the g_i is arbitrary, and thus it will then follow that $g_i \in (\mathcal{I} : X_D)$ for any i, which implies $(\mathcal{I} : X_D) \supseteq \mathfrak{s}$. On the other hand, as $\mathfrak{s}$ is saturated, we have that $(\mathcal{I} : X_D) \subseteq (\mathfrak{s} : X_D) = \mathfrak{s}$, and thus have proved both inclusions, when seeing that $g_1 \in (\mathcal{I} : X_D)$.

By our above reasoning, we have $\mathcal{I}' = \mathfrak{s}'$, so there exist polynomials $P_i \in \mathbb{C}[X_1, \ldots, X_{D-1}]$ such that

$$g_1' = f_1' P_1 + \cdots + f_m' P_m.$$

Let $a = \deg g_1'$, let $d_i = \deg(f_1' P_1)$, and let $d' = \max_i d_i$. By polynomial arithmetic, we have $a \leq d'$. Let Q_i be the homogenization of the P_i. We then have

$$g_1 X_D^{d'-a} = f_1 Q_1 X_D^{d'-d_1} + \cdots + f_m Q_m X_D^{d'-d_m}.$$

The right hand side is an element of the ideal $\mathcal{I}$, thus the left hand side must be also in $\mathcal{I}$. In particular, this implies that $g_1 \in (\mathcal{I} : X_D)$, what had to be proven.

(Note that we have implicitly re-proved that the homogenization of the dehomogenization of an ideal is its homogenous saturation).

Readers familiar with algebra may note that Proposition B.35 is only a description of the homogenization of the ideal $\mathfrak{s}'$, respectively the homogenous saturation of the ideal $\mathfrak{s}$. This is no surprise, since it is merely the homogenous reformulation of Proposition B.27.

This Proposition directly implies that the coefficients of $H(\mathcal{I}/\mathfrak{s})(t)$ stabilize to zero if $\mathcal{I}$ has enough generators:

Proposition B.36 *Let $f_i, \mathcal{I}, \mathfrak{s}$ be as in Proposition B.35. Then there exists an $N \in \mathbb{N}$ such that*

$$\mathcal{I}_N = \mathfrak{s}_N.$$

proof 17 Let us fix a homogenous generating set $g_1, \ldots, g_n$ for $\mathfrak{s}$, let $\delta = \max_j \deg g_j$. The set consisting of all elements $g_i M$ where $1 \leq i \leq n$ and $\deg g_i \leq k$ and M a monomial in $X_1, \ldots, X_D$ of degree $k - \deg g_i$ is a generating set for $\mathfrak{s}_k$. By Corollary B.35 we know that for each i and each j, there exists a number q_{ij} such that $g_i X_j^{q_{ij}} \in \mathcal{I}$. Let q be the maximum of the $q_{ij}, 1 \leq i \leq n, 1 \leq j \leq D$. Then $g_i X_j^q \in \mathcal{I}$ for every i, j. Now by the pigeonhole principle, every monomial M in $X_1, \ldots, X_D$ of degree $D(q-1)+1$ will be divisible by X_j^q for some j. In particular, $g_i M \in \mathcal{I}$ for every i and every monomial M of degree $D(q-1)+1$. In particular,

$$\mathfrak{s}_N \subseteq \mathcal{I}_N$$

for $N = \delta + D(q-1) + 1$, which proves the claim.

For the case where instead of $\mathfrak{s}$ we take the whole ring $\mathbb{C}[X_1, \ldots, X_D]$, Fröberg's famous conjecture [3] states what the Hilbert function would be expected to be:

Conjecture B.37 *Let $f_1, \ldots, f_m$ be generic homogenous polynomials in R of fixed degrees $d_1, \ldots, d_m$, let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$. Then*

$$H(\mathcal{I})(t) = \left| \frac{\prod_{i=1}^m (1-t)^{d_i}}{(1-t)^D} \right|,$$

where for a power series, $\left|\sum_{k=0}^\infty a_k t^k\right|$ denotes setting all coefficients a_ℓ to zero for which there exists k such that $k < \ell$ and $a_k < 0$.

The Conjecture is known to be true for several cases, Fröberg has proved the following [2, 3]:

Theorem B.38 *Let $f_1, \ldots, f_m$ be any homogenous polynomials in R of fixed degrees $d_1, \ldots, d_m$, let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$. Let*

$$H(\mathcal{I})(t) = \sum_{k=0}^{\infty} b_k t^k$$

be the true Hilbert series of $\mathcal{I}$, and

$$\sum_{k=0}^{\infty} a_k t^k = \left| \frac{\prod_{i=1}^{m} (1-t)^{d_i}}{(1-t)^D} \right|$$

the Hilbert series from Conjecture B.37. Then one has

$$b_k \geq a_k.$$

Equality holds if the f_i are generic and $m \leq D$.

In view of the evidence we have gathered in numerical computer experiments, we formulate the following generalization of Fröberg's conjecture B.37 for the conditioned case:

Conjecture B.39 *Let $\mathfrak{s} \subseteq R$ be a homogenous ideal, having a generating set in degree $\leq \delta$. Let $f_1, \ldots, f_m$ be generic homogenous polynomials in $\mathfrak{s}$ of fixed degrees $d_1, \ldots, d_m \geq \delta$. Let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$. Then*

$$H(\mathcal{I}/\mathfrak{s})(t) = \left| \frac{\prod_{i=1}^{m} (1-t)^{d_i}}{(1-t)^D} - H(\mathfrak{s})(t) \right|.$$

One can generalize Fröberg's theorem B.38 to the conditioned case:

Theorem B.40 *Let $\mathfrak{s} \subseteq R$ be a homogenous ideal, having a generating set in degree $\leq \delta$. Let $f_1, \ldots, f_m$ be any homogenous polynomials in R of fixed degrees $d_1, \ldots, d_m \geq \delta$, let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$. Let*

$$H(\mathcal{I}/\mathfrak{s})(t) = \sum_{k=0}^{\infty} b_k t^k$$

be the true Hilbert series of $\mathcal{I}/\mathfrak{s}$, and

$$\sum_{k=0}^{\infty} a_k t^k = \left| \frac{\prod_{i=1}^{m} (1-t)^{d_i}}{(1-t)^D} - H(\mathfrak{s})(t) \right|$$

the Hilbert series from Conjecture B.39. Then one has

$$b_k \geq a_k.$$

Equality holds for $m \leq d$, where d is the Krull dimension of $R/\mathfrak{s}$.

proof 18 For the first part, we use Fröberg's original theorem B.38. Let us denote

$$\sum_{k=0}^{\infty} c_k t^k = \left| \frac{\prod_{i=1}^{m} (1-t)^{d_i}}{(1-t)^D} \right|.$$

The theorem then implies that

$$\dim \mathcal{I}_k \leq \dim R_k - c_k.$$

Also, since $\mathcal{I} \subseteq \mathfrak{s}$, we have

$$\dim \mathcal{I}_k \leq \dim \mathfrak{s}_k.$$

Translating this into differences to $\mathfrak{s}$, we obtain

$$b_k = \dim \mathfrak{s}_k - \dim \mathcal{I}_k \geq \dim \mathfrak{s}_k - \dim R_k + c_k$$

and

$$b_k = \dim \mathfrak{s}_k - \dim \mathcal{I}_k \geq 0.$$

On the other hand,

$$a_k = \dim \mathfrak{s}_k - \dim R_k + c_k$$

for all k until the right hand side would become negative, from where it is zero. Together with the above, this implies $b_k \geq a_k$.

Now we will prove Conjecture B.39 for $m \leq d$. We can assume that $\mathcal{I}$ and $\mathfrak{s}$ are in Noether position, i.e. the chosen coordinate system $X_1, \ldots, X_D$ is generic (with respect to unitary linear transformations). Since d is the Krull dimension of $\mathfrak{s}$, we may assume that $X_1, \ldots, X_d$ are transcendental variables in $R/\mathfrak{s}$. Let $\tilde{f}_1, \ldots, \tilde{f}_m$ be the polynomials in $\mathbb{C}[X_1, \ldots, X_D]$, obtained from setting all terms in $f_1, \ldots, f_m$ to zero which are not divisible by one of the variables $X_1, \ldots, X_d$. These generate an ideal $\tilde{\mathcal{I}} \subseteq \mathbb{C}[X_1, \ldots, X_D]$. Since the $X_1, \ldots, X_d$ are transcendental in $R/\mathfrak{s}$, and $\mathcal{I}$ and $\mathfrak{s}$ are in Noether position, the remaining monomials are linearly independent. Thus we have that $\dim \tilde{\mathcal{I}}_k \leq \dim \mathcal{I}_k = \dim \mathfrak{s}_k - b_k$. But the $\tilde{f}_1, \ldots, \tilde{f}_m$ form a regular sequence, since the coefficients are generic, so we may use Fröberg's original theorem B.38, obtaining the correct dimension.

These considerations give us important bounds on the N from Proposition B.36:

Corollary B.41 *Let $\mathfrak{s} \subseteq R$ be an ideal generated by n homogenous elements of degree at most δ. Let $f_1, \ldots, f_m \in \mathfrak{s}$ be generic with degrees $d_1, \ldots, d_m \geq \delta$ and $m \geq \max(D+1, n)$. Let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$. Let N' be the smallest number such that the coefficient $a_{N'}$ in the power series*

$$\sum_{k=0}^{\infty} a_k t^k = \frac{\prod_{i=1}^{m} (1-t)^{d_i}}{(1-t)^D} - H(\mathfrak{s})(t)$$

is non-positive. Then

$$\mathcal{I}_N = \mathfrak{s}_N$$

only if $N \geq N'$. If Conjecture B.39 holds, the converse is also true.

B.7 An Algorithm to prove the generalized Fröberg conjecture

In this subsection, we will present an algorithm with which one can use in a computer assisted proof of Conjecture B.39 for fixed d_i, D and $\mathfrak{s}$.

The basic observation is that given polynomials $f_1, \ldots, f_m \in \mathfrak{s}$ of fixed degrees $d_1, \ldots, d_m$ and the ideal $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$, the assertion $A(c) = [\dim \mathcal{I}_k \leq c]$ is an algebraic property for every c, since it corresponds to the vanishing of (sub-)minors of a matrix whose coefficients can be expressed in those of f_i. Note that $A(c)$ depends on the f_i resp. d_i, but for reading convenience we do not write that explicitly out. By Theorem B.40, $A(\dim \mathfrak{s}_k - a_k)$ (with a_k as in the theorem) is the sure event resp. the true property, which is also irreducible.

If we can now find a single set of polynomials $\tilde{f}_1, \ldots, \tilde{f}_m \in \mathfrak{s}$ of degrees $d_1, \ldots, d_m$ for which $A(\dim \mathfrak{s}_k - a_k)$ holds but not $A(\dim \mathfrak{s}_k - a_k - 1)$, this implies that $A(\dim \mathfrak{s}_k - a_k)$ does not imply $A(\dim \mathfrak{s}_k - a_k - 1)$ or any of its irreducible sub-properties. Thus, by the definition of genericity, we would have proved that generic polynomials $f_1, \ldots, f_m$ fulfill $A(\dim \mathfrak{s}_k - a_k)$, but not $A(\dim \mathfrak{s}_k - a_k - 1)$. Checking this for all k up to the N for which $\mathcal{I}_N = \mathfrak{s}_N$ then proves Conjecture B.39 for the fixed set of d_i, D and $\mathfrak{s}$.

These considerations give rise to Algorithm 1, which can be used to prove Conjecture B.39 for specific subcases.

In order to check Conjecture B.39 for fixed $d_1, \ldots, d_m$ and $\mathfrak{s}$, one executes Algorithm 1 for $k = 1, 2, \ldots$ and stops when $\mathcal{I}_N = \mathfrak{s}_N$. This terminates if Conjecture B.39 is true. It is important to note that the computations in Algorithm 1 only constitute a proof if they are carried out exactly, or with floating point arithmetic where one additionally has to ensure that the initial numerical error cannot increase the rank r. This can be for example ensured by computing r as the approximate rank of Q with respect to a high enough threshold, depending on the machine precision and the propagation of initial errors.

We have checked Conjecture B.39 in the case where $\mathfrak{s}$ is an ideal of dimension d generated by $D - d$ linear forms, and the f_i are quadrics - the simplest case relevant for the statistical marginalization problem. As the coordinate system can be regarded as generic, it suffices to check Conjecture B.39 for a specific choice of $\mathfrak{s}$ where d is fixed, as the genericity phenomena stay invariant under linear transformations.

Algorithm 1 Checking Conjecture B.39.
Input: Degrees $d_1, \ldots, d_m$, number of variables D; the ideal $\mathfrak{s}$.
Output: Terminates if $b_k = a_k$ in Theorem B.40.

1: Randomly sample polynomials $f_1, \ldots, f_m$ of degrees $d_1, \ldots, d_m$ from $\mathfrak{s}$
2: Initialize $Q \leftarrow [\,]$ with the empty matrix.
3: **for** $i = 1 \ldots n$ **do**
4: **for** all monomials M of degree $k - \deg f_i$ **do**
5: Add a row vector of coefficients, $Q \leftarrow \begin{bmatrix} Q \\ f_i M \end{bmatrix}$
6: **end for**
7: **end for**
8: Calculate $r = \operatorname{rank} Q$.
9: **if** $r = \dim \mathfrak{s}_k - a_k$ **then**
10: Terminate
11: **else**
12: Goto step 1
13: **end if**

Theorem B.42 *Conjecture B.39 is true for linear $\mathfrak{s}$, $d_1, \ldots, d_m \leq 2$ and $D \leq 11$.*

proof 19 This follows from the above considerations and executing Algorithm 1 for any of the finitely many possible cases. As the algorithm is correct and we have found that it terminates, Conjecture B.39 is true.

Of course, Algorithm 1 as it is cannot be used to prove Conjecture B.39 in total, as this would require to check a countably infinite number of cases for every $\mathfrak{s}$. On the other hand, even if Conjecture B.39 does not hold, it can be slightly modified to Algorithm 2 which may be used for computing the N in Proposition B.36.

If the calculations are performed exactly, then the algorithm yields the smallest N from Proposition B.36. If the calculations are performed in floating point arithmetic, it is not guaranteed that it finds the smallest N, but it terminates with probability one.

C Applications to ideal regression

In this section, we present some fundamental properties for the ideal regression problem which can be derived from the results on genericity in section B. Recall our formulation for ideal regression, which was derived e.g. as Problem A.6:

Problem C.1 *Let $\mathcal{F}_\theta$ be a parametric family of radical ideals in $\mathbb{C}[X_1, \ldots, X_D]$. Given input polynomials*

Algorithm 2 Compute N in Proposition B.36.
Input: Degrees $d_1, \ldots, d_m$, number of variables D; the ideal $\mathfrak{s}$.
Output: An N such that $\mathfrak{s}_N = \mathcal{I}_N$.

1: Calculate N' as in Corollary B.41, $k \leftarrow N'$.
2: Randomly sample polynomials $f_1, \ldots, f_m$ of degrees $d_1, \ldots, d_m$ from $\mathfrak{s}$
3: Initialize $Q \leftarrow [\,]$ with the empty matrix.
4: **for** $i = 1 \ldots n$ **do**
5: **for** all monomials M of degree $k - \deg f_i$ **do**
6: Add a row vector of coefficients, $Q \leftarrow \begin{bmatrix} Q \\ f_i M \end{bmatrix}$
7: **end for**
8: **end for**
9: Calculate $r = \operatorname{rank} Q$.
10: **if** $r = \dim \mathfrak{s}_k$ **then**
11: Terminate
12: **else**
13: $k \leftarrow k + 1$, goto step 2
14: **end if**

$q_1, \ldots, q_m$, *estimate a regression parameter* θ *such that* $\mathcal{F}_\theta$ *is "close" to the inputs* $q_1, \ldots, q_m$.

Before continuing, will give a generative version of the problem. In ordinary regression, it is a common assumption that there exists a true regressor hyperplane, and the data are generatively sampled from this regressor hyperplane, with some centered noise added. This naturally generalizes to the following assumption on the inputs q_i in ideal regression:

Assumption C.2 *There is a true regressor parameter* θ *and a true regressor ideal* $\mathcal{F}_\theta$. *Moreover, for every polynomial* q_i, *we have that*

$$q_i = f_i + \varepsilon_i,$$

where f_i *is a generic polynomial of some fixed degree* d_i *in* $\mathcal{F}_\theta$, *and* ε_i *is some generic polynomial.*

This formulation models the classical splitting of sampling randomness and error randomness: the randomness in f_i models the sampling process, while the randomness in ε_i represents the noise.

Also note that while this assumption is natural for the common marginals problem, it may be too narrow for the general case; a broader assumption would be that f_i is a generic polynomial from an ideal or a class of ideals (e.g. ideals with fixed Hilbert function or Krull dimension) contained in $\mathcal{F}_\theta$. However, due to brevity, we restrict to this class of ideal regression problems for the rest of the exposition.

In the following, we will restrict to the homogenous case, which is basically equivalent to the inhomogenous case. Finding a generating set for a homogenously generated $\mathcal{F}_\theta$ corresponds to finding a H-basis for an inhomogenous $\mathcal{F}_\theta$. Thus, in all what follows, the parametric family $\mathcal{F}_\theta$ will be homogenously generated, and the q_i, f_i, ε_i will homogenous polynomial-valued. Note that since the f_i and ε_i are generic, the f_i, q_i and the ε_i are in fact polynomial-valued random variables.

Under these assumptions, the ideal regression problem can be expressed as follows:

Problem C.3 *Let* $\mathcal{F}_\theta$ *be a parametric family of homogenously generated, radical ideals in* $\mathbb{C}[X_1, \ldots, X_D]$. *For* $1 \leq i \leq m$, *let* f_i *be generic polynomials in* $\mathcal{F}_\theta$ *for some fixed ground truth* θ, *let* ε_i *be generic polynomials. Let*

$$q_i = f_i + \varepsilon_i$$

the noisy inputs. Given $q_1, \ldots, q_m$, *estimate* θ.

Having well-definedness, the immediate question is about identifiability: is there a consistent estimator for θ in the $q_1, \ldots, q_m$? That means, is there an estimator, which converges to the true value θ, when the number of i.i.d. samples for each q_i (simultaneously) goes to infinity, or alternatively, the variance of the noise terms ε_i (simultaneously) go to zero? In particular, considering their number m and the degrees $d_1, \ldots, d_m$. One necessary condition is that θ can be uniquely calculated from the noise-free sample $f_1, \ldots, f_m$. In the following subsections, we will give a necessary condition for the latter and a general estimation algorithm for the noisy case.

C.1 Identifiability

In this section, we study the identifiability of the ideal regression problem, in the formulation of Problem C.3. By definition, identifiability is given if and only if there exists a consistent estimator for θ. Equivalently, identifiability holds if and only if there is a consistent estimator for a system of generators of $\mathcal{F}_\theta$. As stated above, a necessary condition for identifiability is that $\mathcal{F}_\theta$ is uniquely identifiable from $f_1, \ldots, f_m$. We conjecture that this condition is also sufficient. What we can say about identifiability is the following weaker, but provable sufficient condition:

Proposition C.4 *Let* $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$. *If* $\mathcal{F}_\theta = (\mathcal{I} : X_D)$, *then the (noisy) ideal regression Problem C.3 is identifiable.*

proof 20 The assumption $\mathcal{F}_\theta = (\mathcal{I} : X_D)$ gives a rule of calculation to obtain $\mathcal{F}_\theta\theta$ for the noise-free case, and thus θ due to unique parameterization. It remains to show that this rule can be adapted to deal with noise. But this can be algorithmically done, as we will show in

the next chapter by stating the approximate saturation algorithm 3.

Thus, to get a sufficient condition on identifiability of ideal regression, we can now check when we can obtain $\mathcal{F}_\theta$ from saturating the ideal generated by the f_i. Since the f_i are generic, we can apply Proposition B.35 to directly obtain an identifiability criterion:

Theorem C.5 *Keep the notations for ideal regression as stated in Problem C.3. Then, the true parameter θ is identifiable if*

$$m \geq \max(D+1, n) \text{ and}$$
$$\deg f_i \geq \delta \quad \text{for all } 1 \leq i \leq m,$$

where n is the cardinality of an arbitrary H-basis of $\mathcal{F}_\theta$, and $\delta = \max_i \deg f_i$.

For the common marginals problem, Theorem C.5 can be used to obtain a more sharp identifiability criterion, by noticing that any linearly generated homogenous ideal has an H-basis of at most D elements in degree one:

Corollary C.6 *Keep the notations of Problem C.3. Consider the ideal regression problem, where $\mathcal{F}_S = \mathrm{I}(S)$, for a d-dimensional sub-vector space S of $\mathbb{C}^D$. If $m \geq D+1$, then S is identifiable, independent of the degrees of the f_i.*

In particular, this corollary also implies identifiability for the noise-free version stated in Problem B.5. For sake of clarity, we state the particular situation for the noise-free case resp. the $f_1, \ldots, f_m$:

Corollary C.7 *Let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ be an ideal generated by $m \geq D+1$ generic homogenous polynomials vanishing on a linear d-dimensional subspace $S \subseteq \mathbb{C}^D$, let ℓ be any linear homogenous polynomial. Then*

$$\sqrt{\mathcal{I}} = \mathrm{I}(S) = (\mathcal{I} : \ell).$$

proof 21 The rightmost equality is a direct consequence of Proposition B.35 and the fact that the coordinate system in Proposition B.35 is arbitrary. The leftmost equality follows from Proposition B.36 and the fact that $h^N \in \mathrm{I}(S)_N$ for any linear homogenous element h of $\mathrm{I}(S)$.

C.2 Calculating approximate saturations

In this section, we will present an algorithm which is able to estimate the parametric ideal $\mathcal{F}_\theta$ consistently when the conditions of the identifiability Theorem C.5 are fulfilled, thus completing the proof of the theorem. If the conditions of the theorem are fulfilled, then from Proposition B.35, we know that $\mathcal{F}_\theta$ can be obtained as the homogenous saturation of $\mathcal{I} = \langle f_1, \ldots, f_n \rangle$. While this is a classical task in Computational Algebraic Geometry, we do not know the f_i, but only the q_i which are endowed with noise. Thus, we will have to calculate the saturation approximately.

For this, we the following Algorithm 3 to compute homogenous saturations approximately. In step 1, Algorithm 3 first needs to find an N where the saturation coincides with the ideal. Such an N exists, however to find it is not a trivial task. Here, one needs either knowledge on $\mathcal{I}$ or genericity assumptions as a simple criterion. Then, it builds with Q an approximate representation of $(\mathcal{I} : X_D)_N$. From this, the method ReduceDegreeHom, which can be found as Algorithm 4, constructs an approximate representation of $(\mathcal{I} : X_D)_{N-1}$. This can be repeated until reaching a k for which $(\mathcal{I} : X_D)_k$ is empty. The calculations have to be performed approximately in the sense that the principal components of the row-spans have to be considered with a suitable singular value threshold.

Algorithm 3 Approximate homogenous saturation.
Input: A homogenous ideal $\mathcal{I} = \langle f_1, \ldots, f_n \rangle$.
Output: Homogenous generator set G for the approximate saturation $(\mathcal{I} : X_D)$.

1: Determine N such that $\mathcal{I}_N = (\mathcal{I} : X_D)_N$.
2: Initialize $Q \leftarrow [\,]$ with the empty matrix, $G \leftarrow \{\}$.
3: **for** $i = 1 \ldots n$ **do**
4: **for** all monomials M of degree $N - \deg f_i$ **do**
5: Add a row vector of coefficients, $Q \leftarrow \begin{bmatrix} Q \\ f_i M \end{bmatrix}$
6: **end for**
7: **end for**
8: **for** $k = N \ldots 2$ **do**
9: Set $G \leftarrow G \cup$ an approximate row basis for Q
10: Set $Q \leftarrow \mathrm{ReduceDegreeHom}(Q)$
11: **end for**
12: Return G (or reduce it first)

Algorithm 4 estimates $((\mathcal{I} : X_D) \cap \langle X_D \rangle)_N$ approximately and then divides out X_D from the approximate basis representation. Again, one has to consider principal components of a suitable approximation threshold. A more detailed description for the special case of the marginalization problem can be found in the main body along the algorithms presented there.

A similar strategy can be applied when computing saturations $(\mathcal{J} : f)$ for arbitrary ideals.

However, we refrain from further explanations, as the given version is already sufficient to prove the identifiability Theorem C.5.

Algorithm 4 ReduceDegreeHom (Q).
Input: Approximate basis for $(\mathcal{I} : X_D)_k$ given as the rows of the matrix Q
Output: Approximate basis for $(\mathcal{I} : X_D)_{k-1}$, given as the rows of the matrix A

1: Let $Q' \leftarrow$ the submatrix of Q obtained by removing all columns corresponding to monomials divisible by X_D
2: Compute $L \leftarrow$ an approximate left null space matrix of Q'
3: Compute $L' \leftarrow$ an approximate row span matrix of $L_i Q$
4: Let $L'' \leftarrow$ the matrix obtained from L' by removing all columns corresponding to monomials not divisible by X_D
5: Compute $A \leftarrow$ an approximate row span matrix of L''

Using Corollary C.7, we can even obtain the saturation $\mathfrak{s} = \sqrt{\mathcal{I}} = (\mathcal{I} : \ell)$ more efficiently and stably under genericity conditions which we have for example in the ideal regression problem C.3. Namely, Corollary B.41 allows us to obtain $\mathfrak{s}_N$ for some N from $\mathcal{I}$. Then it suffices to saturate the ideal $\langle \mathfrak{s}_N \rangle$ by any linear polynomial ℓ. As any polynomial ℓ will yield the same saturation, so one can additionally simultaneously saturate with respect to multiple linear polynomials and then compare or average.

Finally, if we know $\mathfrak{s}$ to be linear, or if we know the Hilbert function of $\mathfrak{s}$, we know the exact dimensions of the approximate spans and kernels (e.g. from Theorem B.38). Algorithms 1 and 2 (found in the paper) additionally use this specific knowledge in order to compute the saturation more accurately.

Moreover, Corollaries **??** and B.41 guarantee correctness and termination of the algorithm under genericity conditions if the inputs are exact; if they are subject to noise, the output of the algorithm approaches the true solution with decreasing noise, or, alternatively, increasing number of i.i.d. samples, equal in distribution to the f_i.

References

[1] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[2] Ralf Fröberg. An inequality for hilbert series of graded algebras. *Math. Scand.*, 56:117 – 144, 1985.

[3] Ralf Fröberg and Joachim Hollman. Hilbert series for ideals generated by generic forms. *Journal of Symbolic Computation*, 17(2):149 – 157, 1994.

[4] Anthony Iarrobino. Compressed algebras: Artin algebras having given socle degrees and maximal length. *Transactions of the American Mathematical Society*, 285(1):337 – 378, 1984.

[5] Keith Pardue. Generic sequences of polynomials. *Journal of Algebra*, 324(4):579 – 590, 2010.

[6] Paul von Bünau, Frank C. Meinecke, Franz J. Király, and Klaus-Robert Müller. Finding stationary subspaces in multivariate time series. *Phys. Rev. Lett.*, 103(21):214101, Nov 2009.