On Algebraic Independence Testing

Abhibhav Garg

Contents

1 Introduction

Given a set of polynomials $f_1, f_2, \ldots, f_m$ in variables $x_1, \ldots, x_n$, we are interested in the problem of testing whether they satisfy an algebraic relationship. While there is an efficient randomised polynomial time algorithms for testing algebraic independence over fields of characteristic zero, the finite characteristic version of this problem is still open.

A recent result put this problem, independent of the characteristic, in coAM $\cap$ AM, making it unlikely to be NP-hard. More interesting than the result (which is already quite interesting) is the perspective used in the proof: look at the polynomials $f_1, \ldots, f_m$ as defining a polynomial map, and study its properties. The goal of this exposition is to understand this perspective better.

To this end, we show that many known results about the algebraic independence problem can be written as properties of the map defined by the input polynomials. We also try and prove these results using standard theorems in algebraic geometry, as opposed to proving everything ourselves. Many of the results we will require only work when the underlying field has characteristic zero. The hope [1] is that writing the proofs this way will allow us to use results from finite characteristic algebraic geometry to patch the holes in the above proofs.

The following subsection will establish some notation that we will use for the rest of this document. In Section 2 we formally define the algebraic independence problem, discuss the general notion of algebraic independence, and also list the results we will subsequently reprove. Finally, in Section 3 we give the proofs of these results. The proofs are algebraic geometric in nature. Atiyah and MacDonald [1994] and Shafarevich [2013] contain all the required background, and will be frequently referred to.

1.1 Notation

We use k to denote the underlying field of constants, which will always be algebraically closed. We use $\operatorname{char} k$ to denote its characteristic. We use $\mathbb{A}^n$ to denote the n-dimensional affine space. Polynomials will be denoted by $f, g, h, \ldots$ and $A, B, \ldots$ with $f_1, \ldots f_m$ reserved for the polynomials whose independence we want to test. Variables will be denoted by $x, y, z, \ldots$ with $x_1, \ldots x_n$ reserved for the variables of the input polynomials. We use m to denote the number of input polynomials, and n to denote the number of input variables. We use vector notation to denote a set of objects, for example $\mathbf{f}$ denotes the set of polynomials $f_1, \ldots, f_m$ while $\mathbf{x}$ denotes the set of variables $x_1, \ldots, x_n$.

We use $k[\mathbf{x}]$ to denote the polynomial ring over k in variables $x_1, \ldots, x_n$, and $k(\mathbf{x})$ to denote its field of fractions. If X is an affine variety, we use $k[X]$ and $k(X)$ to denote its coordinate ring and function field respectively. Given a field K and an extension L, we use $\operatorname{trdeg}_K(L)$ to denote the transcendence degree of L over K. We will always denote ideals by Fraktur letters, for example $\mathfrak{U}, \mathfrak{m}$.

[1] read: My hope

2 Algebraic Independence

2.1 The Decision Problem

We now formally define the algebraic independence problem. The input to the problem is a list of m polynomials $f_1, f_2, \ldots, f_m$ each in variables $x_1, \ldots, x_n$, with constants from field k. Let the polynomials have degree $d_1, \ldots, d_n$ respectively. We assume that these polynomials are given as whiteboxes, via circuits of size at most s.

The polynomials are said to be algebraically independent if and only if for every nonzero polynomial $G \in k[y_1, \ldots, y_m]$, it holds that $G(f_1, \ldots, f_m)$ is not the identically zero polynomial. Equivalently, the polynomials are said to be algebraically dependent if and only if there exists some polynomial $A \in k[y_1, \ldots, y_m]$ such that $A(y_1, \ldots, y_m)$ is the identically zero polynomial. For example, if $f_1 := x_1 + x_2$ and if $f_2 := (x_1 + x_2)^2$, then f_1 and f_2 are algebraically dependent, with $A = y_2 - y_1^2$. On the other hand, if $f_1 := x_1$ and $f_2 := x_1 + x_2$, then no such polynomial A exists, and thus f_1 and f_2 are algebraically independent. [2] When polynomials $f_1, \ldots, f_m$ are dependent, any polynomial A that satisfies $A(f_1, \ldots, f_m) \equiv 0$ will be called an *annihilator* of $f_1, \ldots, f_m$. Note that the dependence/independence of polynomials depends on the underlying field. Consider for example polynomials $f_1 := x_1 + x_2$ and $f_2 := x_1^2 + x_2^2$. If $\operatorname{char} k = 2$, then f_1 and f_2 are dependent, with annihilator $y_2 - y_1^2$. If $\operatorname{char} k \neq 2$, then some more variable chasing will show that f_1 and f_2 are independent.

Algebraic independence of polynomials behaves similar to linear independence in a number of ways. We discuss these in the next subsection.

2.2 Transcendence Degree

Given vectors $v_1, v_2, \ldots, v_n$ from a vector space over some field k, it holds that every maximal linearly independent subset (ordered by inclusion) has the same size. This is the rank of the vector space spanned by the vectors. The proof of this uses the basis exchange property: if S and T are maximal linearly independent subsets of $v_1, \ldots, v_n$, and s is an element of S but not of T, then we can find an element $t \in T$ such that $(S \setminus \{s\}) \cup \{t\}$ is also a maximal and linearly independent.

Similarly, given polynomials $f_1, \ldots, f_m$ from $k[\mathbf{x}]$, it holds that every maximal algebraically independent subset of the polynomials has the same size. This is proved by showing that the same basis exchange property also holds in this setting. Given this, we define the *transcendence degree* of polynomials $f_1, \ldots, f_m$ as the size of the maximal algebraically independent subsets of $f_1, \ldots, f_m$. The name comes from the following. Given polynomials $f_1, \ldots, f_m$, consider the field $k(f_1, \ldots, f_m)$. [3] This is a subfield of

[2] Proving this involves some simple variable chasing.

[3] The ring $k[\mathbf{f}]$ is a subring of $k[\mathbf{x}]$. The latter is a domain, and hence so is the former. Thus the field of fractions is a well defined.

$k(x_1, \ldots, x_n)$, and is an extension of the field k. The transcendence degree of $\mathbf{f}$ as defined above is exactly the transcendence degree of the extension $k(\mathbf{f})/k$. Overloading notation, we use $\operatorname{trdeg}_k(\mathbf{f})$ or $\operatorname{trdeg}(\mathbf{f})$ to denote this. Given that $\operatorname{trdeg}_k k(\mathbf{x}) = n$, and

$$\operatorname{trdeg}_k k(\mathbf{x}) = \operatorname{trdeg}_k k(\mathbf{f}) + \operatorname{trdeg}_{k(\mathbf{f})} k(\mathbf{x}), \tag{1}$$

the decision problem from Subsection 2.1 can equivalently be stated as deciding whether or not the extension $k(\mathbf{x})/k(\mathbf{f})$ is algebraic. From Equation 1 we see that if $m > n$, that is if we have more polynomials than variables, then the polynomials are always dependent. Thus we can always assume that $m \leqslant n$.

Having defined the problem, we now turn to the focus of this document: looking at the polynomials $\mathbf{f}$ as defining a map. The next section motivates and formulates this perspective.

2.3 The Polynomial Map

Given the ring $k[\mathbf{f}]$, a natural object to look at is the affine variety that it corresponds to. [4] Since $k[\mathbf{f}]$ is a finitely generated algebra over k with m generators, it is isomorphic to $k[y_1, \ldots, y_m]/\mathfrak{U}$ for some ideal $\mathfrak{U}$. The isomorphism takes each y_i to f_i. If $\mathbf{f}$ satisfy some algebraic relation, then applying the inverse of the above isomorphism we see that $\mathbf{y}$ also must satisfy the same relation. The converse also holds. Thus the ideal $\mathfrak{U}$ is exactly the ideal of all annihilators of $\mathbf{f}$.

The ring $k[\mathbf{y}]/\mathfrak{U}$ corresponds to the affine variety defined by the equations in $\mathfrak{U}$. We call this affine variety Y. When we want to emphasise the dependence of Y on $\mathbf{f}$, we use $Y_{\mathbf{f}}$. There is a natural map i from $k[\mathbf{y}]/\mathfrak{U}$ to $k[\mathbf{x}]$ that takes each y_i to f_i. As discussed above, this is well defined since elements in $\mathfrak{U}$ are exactly the algebraic relationships in $\mathbf{f}$. Further, this map is an injection, since $\mathfrak{U}$ consists of all algebraic relationships between $\mathbf{f}$. The map i corresponds to a map i^* from the affine variety corresponding to $k[\mathbf{x}]$(namely $\mathbb{A}^n$) to Y. The map i^* has j^{th} coordinate function f_j, and is thus exactly the polynomial map with coordinates $f_1, \ldots, f_m$. We will call this map F. Since i is an injection, the map F is dominant. In other words, Y is exactly the closure of the image of $\mathbb{A}^n$ under F. [5]

The above discussion shows that given $k[\mathbf{f}]$, it is natural to consider the map F with coordinate functions $f_1, \ldots, f_m$. This point is driven home by the fact that the dimension of the affine variety Y is exactly the transcendence degree of $\mathbf{f}$. This follows by (one of) the definition(s) of the dimension of an affine variety. We first make the following simple observation.

Lemma 2.1. *The affine variety Y is irreducible.*

[4] Of course one has to make sure that the ring is a finitely generated algebra over a field with no nilpotent elements, properties that $k[\mathbf{f}]$ satisfies.

[5] The focus of this document is the finite characteristic case, and thus unless stated otherwise, the topology is always the Zariski topology.

Proof of Lemma 2.1. The affine variety $\mathbb{A}^n$ is irreducible, and hence so is its image under the regular map F. The affine variety Y is thus the closure of an irreducible set [6] , and hence is itself irreducible.

Alternatively, an affine variety is irreducible if and only if its coordinate ring is a domain. That $k[\mathbf{f}]$ is a domain follows from the fact that it is a subring of the domain $k[\mathbf{x}]$. $\square$

We can now use the definiton of the dimension.

Definition 1 ([Shafarevich, 2013, p. 67])**.** The dimension of an irreducible affine variety is the transcendence degree of its function field.

Lemma 2.1 allows us to apply the above to Y. In particular, polynomials $f_1, \dots, f_m$ are algebraically independent if and only if $\dim Y_{\mathbf{f}} = m$. Alternatively, the polynomials are independent if and only if the image of the map F is dense in $\mathbb{A}^m$.

We now show that a number of known results about algebraic independence testing can be proved very succinctly, by applying some simple theorems from algebraic geometry to the map F. The following is an informal list of the results we reprove. In the subsequent section we restate them formally before proving them.

Theorem 3.1 Unique annihilator: If $\operatorname{trdeg}(\mathbf{f}) = m - 1$ then the ideal of all annihilators of $\mathbf{f}$ is principal.

Theorem 3.3 Noether normalisation: Suppose $m > n$, and we know that $\operatorname{trdeg}(\mathbf{f}) = r$. Then r random linear combinations of $\mathbf{f}$ form a set of independent polynomials.

Theorem 3.4 Variable reduction: Suppose $m < n$. Then there exists a map ϕ from $k[x_1, \dots, x_n]$ to $k[z_1, \dots, z_m]$ that takes each x_i to a linear combination of the z_j, such that $\operatorname{trdeg}(\mathbf{f}) = \operatorname{trdeg}(\phi(\mathbf{f}))$. Further, a random linear map also works. This allows us to assume $m = n$ without loss of generality when looking for a randomised algorithm.

Theorem 3.5 Jacobian Criterion: The rank of the Jacobian matrix of the polynomials $\mathbf{f}$ treated as a matrix with entries in the field $k(\mathbf{f})$ is equal to the transcendence degree of the $\mathbf{f}$, if char k is zero (or large enough).

Theorem 3.8 The relationship between algebraic and functional dependence.

[6] The image is also a quasi-projective variety, just maybe not affine.

3 Proofs

We start with the easiest of the above results. In all of these cases, the original proofs of the results essentially prove special cases of the theorems we use to give alternative proofs. The hope is that restatement in this form will afford generalisation.

3.1 Unique annihilators

This theorem says that if the transcendence degree is only one less than the number of polynomials, then there is a unique lowest degree annihilator. This is useful when proving hardness results.

Theorem 3.1 ([Kayal, 2009, Lemma 7]). *If $f_1, \ldots, f_m$ are algebraically dependent such that no subset of them are algebraically dependent, then the ideal of annihilators $\mathfrak{U}$ is principal.*

To prove this, we use the following result.

Lemma 3.2 ([Shafarevich, 2013, Theorem 1.21]). *If $X \subset \mathbb{A}^k$ is an irreducible affine variety of dimension $k - 1$, then the coordinate ring $k[X]$ is isomorphic to $k[\mathbf{y}] / \mathfrak{U}_X$ with $\mathfrak{U}_X$ principal.*

We can now prove the theorem.

Proof of Theorem 3.1. By the hypothesis, and Lemma 2.1, the affine variety Y satisfies the premises of Lemma 3.2, and an application of the same gives the desired result. □

3.2 Noether normalisation

We now prove the second result. This is a straigthforward application of the Noether normalisation lemma. This theorem is not directly useful in checking the decision problem of interest, since the setting forces the polynomials to be dependent. It is however useful in some reductions to and from problems related to the decision problem, which will be discussed soon.

Theorem 3.3. *Let $f_1, \ldots, f_m$ be a set of m polynomials in n variables, with $m > n$. Let $\operatorname{trdeg}(\mathbf{f}) = r$. Then there exist polynomials $g_1, \ldots, g_r$ of the form*

$$g_i = \sum_{j=1}^{m} a_{i,j} f_j$$

such that $\operatorname{trdeg}(\mathbf{g}) = r$. Further, a random choice of $a_{i,j}$ also satisfies this property.

The proof will actually give us something stronger.

Proof of Theorem 3.3. Consider the variety $Y \subseteq \mathbb{A}^m$, and consider a normalising map ψ of Y. Since the coordinate ring is infinite, we can pick each ψ_i to be linear in the coordinates of Y. Composing ψ with the map $\mathbf{f}$ gives us the required map, and equivalently the polynomials g_i. The statement about the transcendence degree follows from the fact that normalising maps do not decrease dimensions. □

3.3 Variable reduction

Here we show that we can reduce the number of variables to equal the number of polynomials. Before we state and prove the theorem formally, we sketch the proof strategy. We will assume without loss of generality that **f** are independent. In the general case, we can just replace **f** with a maximal independent set of polynomials for the rest of this argument, or take a random linear combination.

Suppose we have a linear map ϕ that sends each x_i to a linear combination of r variables $z_1, \ldots, z_r$. This corresponds to a linear map from $\mathbb{A}^r$ to $\mathbb{A}^n$. The image will be some r dimensional linear subspace. If we can show that most fibers of the map **f** intersect this linear subspace, then the composed map $\mathbf{f} \circ \phi$ will have image an open subset of Y. The closure of this image will be Y, and thus the dimension of this image will be the same as that of Y.

Let $r = m$. Each fiber of F has dimension atleast $n - m$, and by the theorem on the dimension of intersections, each fiber intersects most m dimensional hyperplanes. But we need a single hyperplane which intersects every hyperplane. For this, we will use the fact that all the fibers are translates of each other, and thus have related intersections with the hyperplane at infinity, after taking projective closures. We now formally state and prove the theorem.

Theorem 3.4 ([Kayal, 2009, Claim 11.1])**.** *Let* $f_1, \ldots, f_m$ *be a set of* m *polynomials in* n *variables, with* $m < n$ *Let* $\operatorname{trdeg}(\mathbf{f}) = r$*. Then there exist a homomorphism* $\phi : k[x_1, \ldots, x_n] \to k[z_1, \ldots, z_m]$ *of the form*

$$\phi(x_i) = a_{i,0} + \sum_{j=1}^{m} a_{i,j} z_j$$

such that $\operatorname{trdeg}(\phi(\mathbf{f})) = \operatorname{trdeg}(\mathbf{f}) = r$.

Proof of Theorem 3.4. Consider a map ϕ of the form above. This induces a map from $\mathbb{A}^m$ to $\mathbb{A}^n$, which is defined as

$$(z_1, \ldots, z_m) \to \left(a_{1,0} + \sum_{j=1}^{m} a_{1,j} z_j, a_{2,0} + \sum_{j=1}^{m} a_{2,j} z_j, \ldots, a_{n,0} + \sum_{j=1}^{m} a_{n,j} z_j \right).$$

This maps $\mathbb{A}^m$ to some affine linear subspace of $\mathbb{A}^n$. We will call this map Φ. The polynomials $\phi(\mathbf{f})$ induce a map from $\mathbb{A}^m$ to $\mathbb{A}^m$, and this map is exactly $F \circ \Phi$. The condition that trdeg $(\phi(\mathbf{f})) = m$ is then equivalent to the condition that $(F \circ \Phi)(\mathbb{A}^m)$ is dense. Therefore in order to prove the theorem, we need to find a dimension m linear subspace of $\mathbb{A}^n$, such that image of this subspace under F is dense in Y. The rest of the proof will show the existance of such a subspace, which will in turn give the existance of ϕ.

Fix a linear subspace L of $\mathbb{A}^n$ of dimension m. Consider the preimage $F^{-1}(y)$ of a point $y \in Y$. The preimage is defined by the equations $f_1 - y_1 = 0, \dots, f_m - y_m = 0$. By the theorem on the dimension of fibres, the preimage dimension atleast $n - m$. [7] Without loss of generality, assume that every fibre has dimension exactly $n-m$, by potentially taking a dense open set of Y. Further, we also assume that the polynomials f_i are homogeneous. In the general case, we will have to replace f_i with the homogeneous component of highest degree of f_i at some points in the argument, which makes it more cumbersome.

If we take the projective closures of L and $F^{-1}(y)$, then their intersection must have dimension atleast 0. Let us study this intersection on the hyperplane at infinity, H. The homegeneous equations for $\overline{F^{-1}(y)}$ are given by $f_i - x_0^{d_i} y_i = 0$ for all i. On H, these are given by $f_i = 0$. [8] We define $Z_y := H \cap \overline{F^{-1}(y)}$. The defining equations of Z_y are independent of y, and thus we have $Z_y = Z_{y'}$ for every y. We can therefore drop the index y. Consider the variety $\overline{L} \cap H$. If we can show that $(\overline{L} \cap H) \cap Z = \emptyset$, then it must be that $\overline{L}$ and $\overline{F^{-1}(y)}$ intersect somewhere on the complement of H, for every y. If this holds, then it must be that the the image of F when restricted to L is dense. We therefore try to find such a subspace L.

The variety Z is defined by the equations $\mathbf{f} = 0$. These are treated as homogeneous polynomials in n variables, defining varieties in $\mathbb{P}^{n-1}$. They define a variety of dimension $n - m - 1$, by the assumption that each fibre $F^{-1}(y)$ has dimension exactly $n - m$. Using [Shafarevich, 2013, Cor 1.6, p.71], the maximum dimension of any linear subspace disjoint from Z is $n - 1 - \dim(Z) - 1 = m - 1$, and also there exists a subspace of this dimension with the required disjointness property. Call this subspace M. Any subspace of the original space $\mathbb{P}^n$ whose intersection with H is M has the properties we require for the restricted image to be dense. This completes the proof of the existance of the required type of subspace. □

We now show that a random linear map of the above type works. In the $n - 1$ dimensional space, if we pick $n - m$ linear polynomials randomly, they will define a $m - 1$ dimensional linear subspace. In order to study the intersection with of this space with Z, we think of the process of picking the subspace as picking linear polynomials one at a time, and replacing Z by its intersection with the zeroset of the linear polynomial. We want to show that the dimension of Z drops by 1 in every step, if this happens then the final variety will have dimension -1, and will thus be empty. The only case when the di-

[7] The theorem says the fibre is either empty, or of dimension atleast $n - m$. The first case is ruled out by the definition of Y.

[8] This is where we use homogenity. In the general case, the intersection is given by $f_i^h = 0$, where f_i^h is the highest degree homogeneous part of f_i.

mension does not decrease when intersecting with the hyperplane is when the hyperplace contains a component of Z. Pick a point from each component of Z. For a hyperplane to contain a particular component of Z, it must contain the picked point. This gives linear constraints that the coefficients of the linear polynomials must satisfy for them to contain components of Z, and thus the set of bad hyperplanes will form a subvariety, proving the required result.

Maps of the above type, which preserve the transcendence degree are called faithful map. We have shown that random linear maps are faithful. It is natural to ask if we can find explicit faithful maps, or atleast small sets of maps atleast one of which is faithful. Explicit faithful maps were found (Agrawal, Saha, Saptharishi, and Saxena [2011]) in the large characteristic setting some years ago, for restricted classes of polynomials, for example sparse polynomials. It would be interesting to see if we can recover those results naturally in the above language.

3.4 Jacobian Criterion

The Jacobian criterion is a classical criterion for algerbaic independence in the case of characteristic zero fields. Given polynomials $\mathbf{f}$, define the Jacobian matrix $\mathcal{J}(\mathbf{f})$ as $\mathcal{J}(\mathbf{f})_{ij} := \partial f_i / \partial x_j$. This is a matrix with entries from the field $k(\mathbf{x})$. The following statement of the Jacobian conjecture is from Pandey, Saxena, and Sinhababu [2018], the references therein point to the places where different cases were first proved.

Theorem 3.5 ([Pandey et al., 2018, Lemma 5])**.** *Let* $f_1, \ldots, f_m$ *be polynomials of degree atmost* d *and transcendence degree* r*. If* $\operatorname{char} k = 0$ *or* $\operatorname{char} k > d^r$ *then* $\operatorname{trdeg}(\mathbf{f}) = \operatorname{rank}_{k(\mathbf{x})} \mathcal{J}(\mathbf{f})$.

To prove this, we will use the notion of tangent spaces. Given a point w on a variety W, we can define ideal $\mathfrak{m}_w$ of $k[W]$ consisting of all polynomials vanishing on w. This ideal is maximal, since the quotient $k[W]/\mathfrak{m}_w$ is k, which is a field. Further, the $k[W]$-module $\mathfrak{m}_w/\mathfrak{m}_w^2$ is annihilated by $\mathfrak{m}_w$, and is thus a k-vector space. The vector space $\mathfrak{m}_W/\mathfrak{m}_w^2$ is called the cotangent space at w, and the dual $(\mathfrak{m}_w/\mathfrak{m}_w^2)^*$ is called the tangent space. This is denoted by $\Theta_{W,w}$. This definition of tangent spaces matches the more classical definition using differentials in the case of complex numbers, but has the advantage of being purely algebraic, and thus being well defined over the closures of finite fields.

Given a regular map $G : W \to Z$, we have an induced map $G^* : k[Z] \mathrm{to} k[W]$. Suppose $G(w) = z$ for some $w \in W, z \in Z$. Then $G^*(\mathfrak{m}_z) \subseteq \mathfrak{m}_w$, and $G^*(\mathfrak{m}_z^2) \subseteq \mathfrak{m}_w^2$. We thus get an induced map $G^* : \mathfrak{m}_z/\mathfrak{m}_z^2 \to \mathfrak{m}_w/\mathfrak{m}_w^2$, which in turn induces a map between $\Theta_{W,w}$ and $\Theta_{Z,z}$. We denote this map $d_w G : \Theta_{W,w} \to \Theta_{Z,z}$.

If W is an irreducible variety, then a point $w \in W$ is called nonsingular if $\dim W = \operatorname{rank} \Theta_{W,w}$. The set of nonsingular points in a variety form a dense open set (a proof can be found in [Shafarevich, 2013, Section 1.4]). Further, we have the following useful lemma.

Lemma 3.6 ([Shafarevich, 2013, Theorem 2.3])**.** *The dimension of the tangent space at a nonsingular point equals the dimension of the variety.*

We now consider our setting. We have a map from $\mathbb{A}^n$ to Y defined by the polynomials F. The tangent space at every point in $\mathbb{A}^n$ is a vector space of dimension n since $\mathbb{A}^n$ is irreducible and nonsingular. The induced map $d_{x_0}F$ at point x_0 is given by the linear map $\mathcal{J}(\mathbf{f})(x_0)$. [9]

Given the above, we can prove one part of Theorem 3.5. Suppose the Jacobian has rank r. If $r < m$, then we can restrict our attention to some r linearly independent rows, and thus we can assume without loss of generality that $r = m$. Let x_0 be a point such that $\mathcal{J}(\mathbf{f})(x_0)$ is rank r. The set of points where this does not hold is a subvariety of $\mathbb{A}^n$ of dimension atmost $n - 1$. The map $d_{x_0}F$ then has image a linear space of rank m, whence the codomain, that is $\Theta_{Y,F(x_0)}$ must have rank atleast m. This shows that in a dense open subset of Y, the tangent space has dimension atleast m, which shows that the dimension of Y is atleast m.

The above proof does not require the characteristic of k to be large, and indeed this requirement is only required for the other direction. For this, we use the following lemma.

Lemma 3.7 ([Shafarevich, 2013, Lemma 2.4])**.** *Suppose* $\operatorname{char} k = 0$*. Then there is a nonempty open subset* $V \subset X$ *such that* d_xF *is surjective for* $x \in V$.

While the above lemma assumes that the characteristic is zero, the proof works as long as the characteristic is large enough, that is bigger than d^r. The above lemma immediately gives us the other direction of the Jacobian criterion: since the map on the tangent spaces is surjective, it must be that for a dense open subset of Y we have $\operatorname{rank} \Theta_{Y,y} \leqslant m$. This implies that $\dim Y \leqslant m$, as required.

3.5 Functional Dependence

Suppose we have dependent polynomials $g_1, \dots, g_r$. In general, the dependency of any g_i on the rest will is nonlinear, and we cannot write say $g_1 = H(g_2, \dots, g_r)$ for some polynomial H. Pandey et al. [2018] showed that while the above is not possible, if we randomly shift the polynomials and allow power series, then we can write a power of g_1 as a function of $g_2, \dots, g_r$. Formally, they proved the following theorem.

Theorem 3.8 ([Pandey et al., 2018, Theorem 10])**.** *Let* $\mathbf{f}$ *be a set of polynomials of transcendence degree* r*. Then there exist an algebraically independent subset* $\{g_1, \dots, g_r\} \subset \mathbf{f}$ *of polynomials such that for a random* $\mathbf{a} \in k^n$ *and every* f_j*, there is a power series* $h_j \in k[[y_1, \dots, y_r]]$ *such that* $f_j(\mathbf{x} + \mathbf{a}) = h_j(g_1(\mathbf{x} + \mathbf{a}) - g_1(\mathbf{a}), \dots, g_r(\mathbf{x} + \mathbf{a}) - g_r(\mathbf{a}))$.

We now prove the result. Define the polynomial map F with coordinate functions $(f_1, \dots, f_m)$. Given polynomials $\mathbf{f}$, the shifted polynomials $\mathbf{f}(\mathbf{x}+\mathbf{a}) - \mathbf{f}(\mathbf{a})$ have the property

[9] I will put down the proofs of these soon.

that $\mathbf{0}$ is mapped to $\mathbf{0}$. Further, the variety corresponding to the shifted polynomials, which we call $Y_{\mathbf{a}}$, is such that the origin of $Y_{\mathbf{a}}$ is the image of $\mathbf{a}$ in Y. If $\mathbf{a}$ is picked randomly, then $F(\mathbf{a})$ is a general point, and thus by shifting we have made the origin of $Y_{\mathbf{a}}$ a general point. In particular, in $Y_{\mathbf{a}}$, we can assume that the origin is a nonsingular point.

The ideal $\mathfrak{m} := \mathfrak{m}_{\mathbf{0}}$ in $k[Y]$ is generated by $y_1, \ldots, y_m$. A subset of these elements also then generate the vector space $\mathfrak{m}/\mathfrak{m}^2$. Since the origin is nonsingular, this vector space has dimension r. Let $y'_1, \ldots, y'_r$ be the y_j whose images generate this vector space. The y'_i form a system of local parameters at the origin. [10] Since the point is nonsingular, the local ring $\mathcal{O}_{\mathbf{0}}$ has an isomorphic inclusion into the power series ring generated by the y'_i. Each y_j can thus be written as a power series in the y'_i on $Y_{\mathbf{a}}$. Finally, given the power series for y_j in terms of y'_i, we can substitute $f_i(\mathbf{x}+\mathbf{a}) - f_i(\mathbf{a})$ for y_i everywhere to get a power series for $f_j(\mathbf{x}+\mathbf{a}) - f_j(\mathbf{a})$. This completes the proof. [11]

[10] The definition of systems of local parameters can be found in Shafarevich [2013], in Chapter 2.

[11] This proof essentially uses newton iteration to find the power series. The result can also be proved directly using newton iteration, by picking a separable transcendence basis as the g_i, and applying netwon iteration on the annihilators of f_j and g_i to get the required power series. A minimality assumption on the annihilator along with the fact that the f_j depends separably on the g_i will allow the application of NI.

4 Bibliography

M. Agrawal, C. Saha, R. Saptharishi, and N. Saxena. Jacobian hits circuits: hitting-sets, lower bounds for depth-d occur-k formulas & depth-3 transcendence degree-k circuits. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:143, 2011.

M. Atiyah and I. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Avalon Publishing, 1994. ISBN 9780813345444. URL `https://books.google.co.in/books?id=HOASFid4x18C`.

N. Kayal. The complexity of the annihilating polynomial. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 184–193, July 2009. doi: 10.1109/CCC.2009.37.

A. Pandey, N. Saxena, and A. Sinhababu. Algebraic independence over positive characteristic: New criterion and applications to locally low-algebraic-rank circuits. *computational complexity*, 27(4):617–670, Dec 2018. ISSN 1420-8954. doi: 10.1007/s00037-018-0167-5. URL `https://doi.org/10.1007/s00037-018-0167-5`.

I. Shafarevich. *Basic Algebraic Geometry 1: Varieties in Projective Space*. SpringerLink : Bücher. Springer Berlin Heidelberg, 2013. ISBN 9783642379567. URL `https://books.google.co.in/books?id=tyK4BAAAQBAJ`.