On Algebraic Dependence

Abhibhav Garg
Advisor: Prof. Nitin Saxena

Contents

1 Notation

We use capital letters $\mathbb{F}, F, K, L, E$ to represent fields.

In particular, F will always refer to the base field of constants, and $K \setminus F$ to denote that K is an extension with base field F.

Given a field F and a set S, we use $F(S)$ to represent the smallest field containing F and the elements of S.

We work primarily with function fields, and the indeterminants will be denoted by $x_1, \ldots, x_n$ with n denoting the number of indeterminants. In general, we use bold letters, such as $\mathbf{x}$ to denote the set of all indeterminants. We will also use bold letters to indicate vectors of natural numbers, and $\mathbf{x^a}$ will denote the monomial $\pi x_i^{a_i}$.

Polynomials are denoted by $f_1, \ldots, f_m$, with m denoting the number of polynomials. To denote the set of all the polynomials, we use $\mathbf{f}$.

The degree(total) of f_i is denoted by d_i, and $D := \prod f_i$.

The annihilator, will always be denoted by $A(y_1, \ldots, y_m)$ or $A(\mathbf{y})$.

Transcendence degree is shortened to trdeg.

All theorem statements implicitely assume the above notation.

2 Introduction

Given a base field F, and an extension K over F, element $x \in K$ is called *transcendental* over F, if x is not the root of any polynomial with coefficients in F. An element that is not transcendental over F is called *algebraic* over F. A set of elements $S \subset K$ are called algebraically independent if every element $s \in S$ is transcendental over $F(S \setminus \{s\})$.

Any field extension $K \setminus F$ can be decomposed (not necessarily uniquely) into a three length tower of extensions, $K \setminus F(S) \setminus F$ with the following properties:

- The set S is transcendental over F.
- The extension K is algebraic over $F(S)$.

While the set S in a decomposition of the above nature is not necessarily unique, $|S|$ is. This size $|S|$ is called the transcendence degree of the extension $K \setminus F$. Lang (2005) is a good source for learning more about field extensions.

Given the above basic definitons, the algebraic dependence problem is the following:

Problem 1 (Algebraic Independence)**.** Given a base field $\mathbb{F}$, and a set of m polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ in n variables, is the following field extension algebraic:

$$\mathbb{F}\{x_1, \ldots, x_n\} \setminus \mathbb{F}\{f_1, \ldots, f_m\}.$$

Alternatively, the problem can be framed as follows:

Problem 2 (Algebraic Independence)**.** Given a base field $\mathbb{F}$, and a set of m polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ in n variables, does there exist a non-zero polynomial $A(y_1, \ldots, y_m) \in \mathbb{F}[y_1, \ldots, y_m]$ such that

$$A(f_1, \ldots, f_m) \equiv 0.$$

A polynomial A that satisfies the above, if it exists, is called the Annihilator of the polynomials $\mathbf{f}$.

A simple example is as follows: Let $f_1 := x_1^2 + x_2^2$ and $f_2 := x_1 + x_2$. If $\mathbb{F} := \mathbb{F}_2$, then the two polynomials are dependent, with annihilator $f_1^2 + f_2$. If on the other hand, $\mathbb{F} := \mathbb{Q}$, then the polynomials are independent, with $2y^2 - 2yf_1 + f_1^2 - f_2$ the minimal polynomial for both x_1, x_2.

Algebraic depenence can be seen as the natural generalisation of linear dependence. While linear dependence can be checked easily in polynomial time, the same cannot be said of algebraic dependence(yet). The primary reason for this difference is the fact that the algebraic relationship between a set of polynomials can be highly complicated. More formally, the annihilator A can have exponentially high degree.

It is thus not even clear if we can certify algebraic dependence efficiently, let alone solve the problem efficiently. However, recent work (Guo et al. (2018)) puts this problem in AM $\cap$ CoAM, making it unlikely to be NP-hard, under standard assumptions, namely P = BPP and P $\neq$ NP. This is strong evidence that the problem can be solved by a randomised algorithm, or atleast that the problem can be efficiently certified, making the problem "easy".

This report summarises some results that are known about this problem, with a focus on two of them: the above result showing that the problem is easy, and a result that relates algebraic dependence to functional dependence. The reason the second result is important is that currently it is the only known way of getting any semblence of an algorithm for the problem. Finally, it discussed some of the approaches we tried for the case of bounded degree polynomials.

3 Previous Work

3.1 Computability in PSPACE

It it not clear a priori if this problem is even computable - the annihilator of the polynomials $\mathbf{f}$ might have arbitrary degree. Oscar Perron Perron (1927) gave a bound on the degree of the annihilator of $n + 1$

polynomials in n variables in fields of characteristic 0. This was subsequently generalied to arbitrary number of polynomials in Kayal (2009), and to arbitrary characteristic in Mittmann and Bläser (2013). They prove the following:

Theorem 1. Let $\delta := \max(d_i)$, and let r be the trdeg of $\mathbf{f}$, with $r < m$ Then there exists an annihilator A of total degree atmost δ^r.

This gives us a brute force PSPACE algorithm for the problem: Given the polynomials, construct an exponentially big linear system, where the unknowns are the coefficients of A, and check for solutions.

Kayal (2009) also proved that the above degree bound is tight, by constructing a set of dependent polynomials, whose annihilator of smallest degree hits the above exponential bound.

3.2 Jacobian Criterion

The oldest criterion for algebraic dependence was proved by Jacobi in 1851, and subsequently strenghtened by Dvir et al. (2007). Define the Jacobian of the polynomials $\mathbf{f}$ to be the matrix of partial derivatives,

$$J_{\mathbf{x}}(\mathbf{f}) = \left(\frac{\partial f_i}{\partial x_j}\right)_{i,j}$$

They proved the following:

Theorem 2. Let $\mathbb{F}$ have characteristic either 0, or greater than D. Then the trdeg of the polynomials $\mathbf{f}$ is equal to the rank of the Jacobian matrix, over the field $\mathbb{F}(\mathbf{x})$

The above theorem gives us a straightforward randomised polynomial time algorithm for checking algebraic dependence for fields of big enough characteristic: compute the Jacobian, and compute its determinant after randomly fixing the variables x_i. By the DeMillo-Lipton-Schwartz-Zippel lemma (Demillo and Lipton (1978)), if this determinant is zero, so is the determinant of the Jacobian, with high probability. It was also proved that one of the directions in the above, namely that if the Jacobian is full rank then the polynomials are algebraically independent, does not require the condition on the characteristic.

This solves the problem in the large characteristic case. The above fails when the characteristic is small.

3.3 Witt-Jacobian Criterion

The first non-trivial algorithm that was independent of the characteristic of the field was given in Mittmann et al. (2012). Their criterion is based on lifting the Jacobian polynomial to the p-adics, which have characteristic 0. This puts the problem of independence testing in $NP^{\#P}$.

3.4 Algebraic Independence in AM ∩ CoAM

Guo et al. (2018) proved that algebraic independence testing is both in AM and in CoAM, putting it very low on the polynomial heirarchy, in $\Sigma_2 \cap \Pi_2$. This is strong evidence that the problem is not NP-hard. The proof technique employed is algebro-geometric. The idea is to look at the polynomial map induced by the input polynomials, and the size of its image. A gap in the size of this image allows an application of the Goldwasser-Sipser Set Lowerbound protocol Goldwasser and Sipser (1986).

We sketch the proof here. Assume that the problem instance is in field $\mathbb{F}_q$. We will work in an extension $\mathbb{F}_{q'}$. Assume without loss of generality that $m = n$. Let f denote the map $\mathbb{F}_{q'} \mapsto \mathbb{F}_{q'}$ where $f(a_1, \ldots, a_n) = (f_i(a_1, \ldots, a_n))$. Let N_b denote the size of the set $f^{-1}(b)$. Let $\bar{N}_b$ denote the cardinality of the set $f^{-1}(b)$ in the algebraic closure of $\mathbb{F}_{q'}$.

It is clear that if the polynomials $\mathbf{f}$ are algebraically dependent, then every element in the image of the map f must be a root of the annihilator. Since the annihilator has bounded degree, the image cannot be too big. The converse also holds - if the polynomials are independent, then the image of the map is big.

Theorem 3. Testing algebraic dependence of $\mathbf{f}$ is in AM.

Proof sketch. For a random $a \in \mathbb{F}_{q'}^n$, look at the size of $N_{f(a)}$, in case of dependence and independence.

First, consider the case when the polynomials $\mathbf{f}$ are dependent. The claim is that for any $k > 0, N_{f(a)} > 0$ for atmost kD/q' fraction of the $a \in \mathbb{F}_{q'}^n$. By DeMillo-Lipton-Schwartz-Zippel, and the degree bound on the annihilator, we have $|Im(f)| \leq Dq'^{n-1}$. From this, the claim follows by a counting argument.

The case of the independent polynomials is slightly more involved. The claim is that $\bar{N}_{f(a)} \leq D$ for all but atmost nDD'/q' fraction of the $a \in \mathbb{F}_{q'}^n$. Consider the annihilators A_i of $\{x_i, f_1, \ldots, f_n\}$. Let $A_i'(z) := A_i(z, f_1(a), \ldots, f_n(a))$, and assume that none of them are identically zero. It is easy to see that for any b that satisfies $f(a) = f(b)$, the coordinates of b are roots of A_i', which gives us that the number of such b is finite. Now, an application of Bezout's theorem gives the size bound of D that was claimed. To complete the claim, the number of a such that atleast one of the A_i' are identically zero needs to be bounded. This can be done by another application of DeMillo-Lipton-Schwartz-Zippel lemma, by noting that the leading coefficients of all the A_i' are nonzero, since the polynomials are assumed to be independent.

By appropriately picking the parameter q', there is a gap in the size of the set $\left|f^{-1}(f(a))\right|$ for a random a, and by the affore mentioned protocol, this proves the theorem. □

Theorem 4. Testing algebraic dependence of $\mathbf{f}$ is in CoAM.

Proof Sketch. Here, the set in whose size the gap exists is the image of the polynomial map itself.

First consider the dependent case. The claim is that $N_b = 0$ for all but atmost D/q' fraction of $b \in \mathbb{F}_{q'}^n$. This follows directly from the previous discussion on the size of the image of f.

Consider then the independent case. The claim is that $N_b > 0$ for atleast $D^{-1} - nD'q'^{-1}$ fraction of the b. Since for atleast $1 - nDD'q'^{-1}$ fraction of the $a, N_{f(a)} \leq D$, the claim follows by a simple counting argument.

For appropriate values of the parameter q', the above two claims give a gap in the size of the set $Im(f)$, and the proof of the theorem follows from the protocol. □

We reiterate that while the above result is strong evidence that the problem is low in the polynomial heirarchy, the proofs themselves do not hint at any algorithm, or even a certificate for the problem.

3.5 Functional Dependence

Pandey et al. (2018) prove that algebraic dependence is related to functional dependence. In particular, they prove the following theorem:

Theorem 5. Let $t \in \mathbb{N}$. If the trdeg of $\mathbf{f}$ is k, then there exist algebraically independent $\{g_1, \ldots, g_k\} \subset \mathbf{f}$ such that for a random $\mathbf{a} \in \bar{\mathbb{F}}$ and for all i, there are polynomials $h_i \in \bar{\mathbb{F}}[Y_1, \ldots, Y_k]$ satisfying

$$f_i^{=t}(\mathbf{x} + \mathbf{a}) = h_i^{=t}(g_1(\mathbf{x} + \mathbf{a}), \ldots, g_k(\mathbf{x} + \mathbf{a})).$$

Note that for any $f_i \notin \mathbf{g}$, the set $f_i \cup \mathbf{g}$ is algebraically dependent, and thus f_i has a complicated dependence on $\mathbf{g}$. The above result says that upto arbitrary approximation, after applying a shift, f_i is actually a polynomial in $\mathbf{g}$, greatly simplifying what the relationship looks like.

For example, consider the algebraically dependent set $\{x_1, x_2, x_1x_2^2\}$ with field $\bar{\mathbb{F}}_2$. After a random shift, the polynomials look like $x_1 + a_1, x_2 + a_2, (x_1 + a_1)(x_2^2 + a_2^2)$. If we set $t = 1$, then we have

$$x_1 + a_1 \equiv a_2^{-2}(x_1 + a_1)(x_2^2 + a_2^2) \pmod{\langle \mathbf{x} \rangle^2}.$$

While dependent polynomials are also functionally dependent, independent polynomials might also seem functionally dependent if checked for low values of t. This is evident in the previous example: for a very low value of t, x_1 and $x_1x_2^2$, two clearly independent polynomials, seem functionally dependent. The authors proved a upper bound on the t for which independent polynomials can look functionally dependent. Formally, they prove the following:

Theorem 6. Let the base field have characteristic p. Let $\mathbf{f}$ be independent, with inseperable degree p^i. Then,

1. for all $t \geq p^i$, for a random $\bar{a}$, $f_n^{\leq t}(\mathbf{x}+\mathbf{a})$ cannot be written as $h^{\leq t}(f_1(\mathbf{x}+\mathbf{a}), \ldots, f_{n-1}(\mathbf{x}+\mathbf{a}))$, for any $h \in \bar{\mathbb{F}}[\mathbf{Y}]$.
2. for all $1 \leq t < p^i$, there is some j such that for random $\mathbf{a}$, $f_j^{\leq t}(\mathbf{x}+\mathbf{a})$ can be written as $h_{jt}^{\leq t}(f_1(\mathbf{x}+\mathbf{a}), \ldots, f_{j-1}(\mathbf{x}+\mathbf{a}), f_{j+1}(\mathbf{x}+\mathbf{a}), \ldots, f_n(\mathbf{x}+\mathbf{a}))$, for some $h_{jt}[\mathbf{Y}]$.

The above theorem gives a randomised polynomial time algorithm for testing independence, when the inseperable degree is promised to be constant.

4 Bounded Degree Polynomials

In this project, we attempted to study the special case of bounded degree polynomials. In particular, we assume that there is a constant δ, such that for all i, $d_i \leq \delta$. In this setting, all polynomials are vacuously sparse, and we can thus assume that the input consists of the monomials explicitely, as opposed to circuits. In particular, the total number of possible monomials is $\mathcal{O}\left(n^{\delta}\right)$. This allows us to operate on the polynomials arbitrarily, as opposed to allowing only those operations that circuits allow, such as taking standanrd partial derivatives and finding homogeneous parts. While problems such as PIT become trivial in this explicit setting, the problem of algebraic independence testing continues to remain open.

An example that demonstrates the hardness of this setting is the following:

Example 1. Let $\mathbb{F} = \mathbb{F}_p$ for some p. Let $f_1 := x_1^p - x_2, f_2 := x_2^p - x_3$ and in general, for $1 \leq i < n$, $f_i = x_i^p - x_{i+1}$. Finally, let $f_n := x_n$. It is easy to see that the polynomials $\mathbf{f}$ are independent. The minimal polynomial for x_n is just $y = f_n$. The minimal polynomial for x_i, for $i \neq n$ is given by

$$y^{p^{n-i}} = f_n + \sum_{j=1}^{n-i} f_{n-j}^{p^j}.$$

The inseperable degree of $\mathbf{f}$ is p^n, which is far from constant.

It is clear that even for bounded degree polynomials, the annihilator can have exponential degree. This example shows that the inseperable degree can also be exponentially high.

4.1 Reduction to Trinomials

The first thing we tried was checking if the general case of the problem admits reductions to cases with smaller parameters. To this end, a simple reduction is from the general case, to the case of trinomials.

The actual reduction to the trinomials is the obvious one. Here we present the reduction of a single polynomial f. In the general case, all the polynomials f_i are reduced in the same way. The reduction introduces new variables. In the general case, these new variables are also indexed by the index of the polynomial. Essentially, this just ensures that the new variables introduced while reducing distinct polynomials are distinct. Assume that the polynomial f has the form

$$f(\mathbf{x}) = \sum_{\mathbf{a}} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}$$

Assume that $f(\mathbf{x})$ has l many monomials, and that $l > 3$. Fix any ordering for the monomials, say lexicographic, and let $f(\mathbf{x}) = \sum_{i=1}^{l} m_i$, where m_i is the product of the i^{th} monomial in f, with its corresponding coefficient. Introduct $l-3$ new variables, $z_1, \ldots, z_{l-3}$. Define $g_1 := m_1 + m_2 - z_1$. For all $2 \leq i \leq l-3$, define $g_i := m_{i+1} + z_{i-1} - z_i$. Finally, define $g_{l-2} := m_{l-1} + m_l + z_{l-3}$. By definition, each of the g_i are trinomials.

In the general case, we have polynomials $f_1, \ldots, f_m$, with number of monomials $l_1, \ldots, l_m$. We introduce polynomials $g_{i,1}, \ldots, g_{i,l_i-3}$ corresponding to f_i. Each of these $g_{i,j}$ are trinomials, and the total number of new polynomials is $\mathcal{O}\left(n^{\delta+1}\right)$, a polynomial. In order to show that this is a valid reduction, we need to show that dependence is preserved.

Lemma 7. If the polynomials $\mathbf{f}$ are algebraically dependent, then so are the polynomials $\mathbf{g}$.

Proof. Since $\mathbf{f}$ are dependent, they have an annihilator $A(\mathbf{y})$. Define an annihilator $B(\mathbf{w})$ for $\mathbf{g}$ as

$$B(w_{1,1}, w_{1,2}, \ldots, w_{1,l_1-3}, w_{2,1}, \ldots, w_{m,l_m-3} := A(\sum_{i=1}^{l_1-3} w_{1,i}, \ldots, \sum_{i=1}^{l_m-3} w_{m,i}).$$

That B annihilates $\mathbf{g}$ simply follows from the fact that $f_j = \sum_{i=1}^{l_j-3} w_{j,i}$. □

Lemma 8. If the polynomials $\mathbf{f}$ are algebraically independent, then so are the polynomials $\mathbf{g}$.

Proof. Look at the extension $\mathbb{F}(\mathbf{x}, \mathbf{z}) \setminus \mathbb{F}(\mathbf{g})$. Since $\mathbb{F}(\mathbf{f}) \subset \mathbb{F}(\mathbf{g})$, and since each of the x_i are algebraic over $\mathbb{F}(\mathbf{f})$, they are algebraic over $\mathbb{F}(\mathbf{g})$. Thus the extension $\mathbb{F}(\mathbf{g}, \mathbf{x}) \setminus \mathbb{F}(\mathbf{g})$ is algebraic. Let us denote $\mathbb{F}(\mathbf{g}, \mathbf{x})$ by $\mathbb{F}_1$.

Since $g_{i,1}$ are in $\mathbb{F}_1$, and all monomials in $\mathbf{x}$ are also in $\mathbb{F}_1$, so are the elements $z_{i,1}$. Again, since $g_{i,2}$ are in $\mathbb{F}_1$, and all monomials in $\mathbf{x}$ are also in $\mathbb{F}_1$, so are the elements $z_{i,1} - z_{i,2}$. Since $z_{i,1}$ are in $\mathbb{F}_1$, so are $z_{i,2}$. Continuing, we get that all $z_{i,j}$ are in $\mathbb{F}_1$, and hence $\mathbb{F}_1 = \mathbb{F}(\mathbf{x}, \mathbf{z})$. But by definition, $\mathbb{F}_1$ was an algebraic extension of $\mathbb{F}(g)$, and thus $\mathbb{F}(\mathbf{x}, \mathbf{z})$ is algebraic over $\mathbb{F}(\mathbf{g})$, completing the proof of the lemma. □

This reduction begs the following question, which is still open:

Open Question 1. Is there an integer e, such that given an instance of the algebraic independence question for bounded degree polynomials, we can reduce it to an instance of the same problem where all the polynomials have degree atmost e, in a manner that preserves dependence.

The reduction of the degree seems like a harder problem. If we were to achieve this by a reduction similar to above, we would have to come up with some polynomials g_i that are all of bounded degree, but that somehow multiply to give f. Such g_i might not even exist. An action such as substituting x^2 with x' and adding $x^2 - x'$ as a polynomial will also not work, since we cannot recover the original polynomial f via the allowed field actions.

4.2 Towers of Certificates

This is a very high level picture of a potential way this problem can be tackled, and most of the facts in this section are extremely obvious.

Assume that $\mathbf{f}$ are algbraically independent. Consider the field extension $\mathbb{F}(\mathbf{x}) \setminus \mathbb{F}(\mathbf{f})$. This can be decomposed into the following tower of extensions:

$$\mathbb{F}(x_1, \ldots, x_n, \mathbf{f}) \setminus \mathbb{F}(x_2, \ldots, x_n, \mathbf{f}) \setminus \mathbb{F}(x_3, \ldots x_n, \mathbf{f}) \setminus \cdots \setminus \mathbb{F}(\mathbf{f}).$$

Each of these extensions are algebraic. Because of the multiplicative property of the degree of algebraic extensions, a simple averaging argument gives us that not all of these extensions can have very high degree. In particular, atleast one of them will have degree atmost δ. What this tells us is that there is some i such that it is easy to certify the fact that x_i is algebraic over $\mathbb{F}(x_{i+1}, \ldots, x_n, \mathbf{f})$.

This leads to the following question: Is there an i such that x_i is easy to certify over $\mathbb{F}(\mathbf{f})$. In other words, is there a permutation of $\mathbf{x}$, where the small degree step in the tower is the first one? If this were true, then it would give us a way of certifying independence. While this is true of the previous "hard" example, this does not hold in general. The following example, which is a simple modification of example 1 shows this.

Example 2. Let $\mathbb{F} = \mathbb{F}_p$ for some p. Let $f_1 := x_1^p - x_2, f_2 := x_2^p - x_3$ and in general, for $1 \leq i < n$, $f_i = x_i^p - x_{i+1}$. Finally, let $f_n := x_n^p - x_1$.

A simple calculation shows that that the minimal polynomial of any of the x_i has exponential degree over. Every other x_j has very low degree annihilators over $\mathbb{F}(x_i, \mathbf{f})$, but the first one has exponential degree.

In the above example, the inseperable degree becomes 1. However, it is possible to construct examples where the inseperable degree also remains high. The following example works for the case of $n = m = 2$.

Example 3. Let $\mathbb{F} = \mathbb{F}_2$. Let $f_1 := x_1^2 + x_2^2$. Let $f_2 := x_2^2 + x_1 + x_2$. The minimal polynomial for x_1 is $y^4 = f_1^2 + f_2^2 + f_1$, and that for x_2 is $y^4 = f_1 + f_2^2$.

To get the above example, we took polynomials where it was easy to certify the fact that x_1 is algebraic, and then replaced x_1 by $x_1 + x_2$ everywhere. This leads one to believe that maybe it is not one of the x_i that is easy to certify, but some other polynomial a.

The general scheme that we want to try is the following: Find a polynomial a that depends algebraically on $\mathbf{f}$, with the following two additional properties. One, there is a short certificate for a. This can either be done directly via the annihilator of $a, \mathbf{f}$, or via functional dependence. While in general both of the above are exponentially big, since we are picking the polynomial a, we might hope to pick a "good" polynomial where the certificate is not too bad. Also, this certificate should somehow show that a depends non-trivially on one of the polynomials, say f_n. Secondly, a should be simpler than f_n in some appropriate sense. We want a potential function on the set of polynomials, and a should be such that replacing f_n with a reduces this potential function. Examples of possible potential functions include the sum of degrees of all the polynomials. By repeating this replacement technique multiple times, we can potentially convert the problem into an easy instance.

The above ideas are clearly at a very high level, but they currently seem like a good way of tackling the problem. One of the obvious problems in this approach is that certifying the polynomial a itself is an instance of the algebraic dependence problem, with basically the same instance size. This is circular in nature. This is why we must make sure that a is nice enough. The immediate plan is to study the space $\mathcal{H}f_i$ (the non-constant part of $f_i(\mathbf{x} + \mathbf{z})$ with respect to $\mathbf{x}$) more closely. Looking at this space modulo high enough degrees of $\mathbf{x}$ gives the complete functional dependence result, but the space is still not well enough studied to rule out the possibility of it being useful modulo lower powers of $\mathbf{x}$.

Finally, we would like to point out some intuition for the above method from linear algebra. Both linear and algebraic independence satisy matroid properties. In particular, given a set of vectors (polynomials) S, and a vector (polynomial) c, the following holds: if $b \in cl(S \cup \{c\})$ and $b \notin cl(\{c\})$, then $c \in cl(S \cup \{b\})$. In the case of linear independence, the cl operator is just the span, while in the algebraic dependence case, it is the algebraic closure operator. This basically amounts to saying that if we have a basis, and some vector is in its span, we can replace one of the basis vectors with that vector. This is essentially what we want to do in the algebraic case: start with a basis $\mathbf{f}$ and repeatedly replace polynomials with other polynomials that are simpler.

5 Conclusion and Future Work

We studied the problem of algebraic dependence in the special case of bounded degree polynomials, and outlined a potential method of solving the problem. We now plan to try and implement this, by studying the space $\mathcal{H}f_i$ modulo low degree powers of $\mathbf{x}$ and checking what kind of information this yields about the polynomials.

References

Richard A. Demillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193 – 195, 1978. ISSN 0020-0190. doi: https://doi.org/10.1016/0020-0190(78)90067-4. URL http://www.sciencedirect.com/science/article/pii/0020019078900674.

Zeev Dvir, Ariel Gabizon, and Avi Wigderson. Extractors and rank extractors for polynomial sources. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 52–62, Washington, DC, USA, 2007. IEEE Computer Society. ISBN 0-7695-3010-9. doi: 10.1109/FOCS.2007.26. URL http://dx.doi.org/10.1109/FOCS.2007.26.

S Goldwasser and M Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, STOC '86, pages 59–68, New York, NY, USA, 1986. ACM. ISBN 0-89791-193-8. doi: 10.1145/12130.12137. URL http://doi.acm.org/10.1145/12130.12137.

Zeyu Guo, Nitin Saxena, and Amit Sinhababu. Algebraic dependencies and pspace algorithms in approximative complexity. In *Proceedings of the 33rd Computational Complexity Conference*, CCC '18, pages 10:1–10:21, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. ISBN 978-3-95977-069-9. doi: 10.4230/LIPIcs.CCC.2018.10. URL https://doi.org/10.4230/LIPIcs.CCC.2018.10.

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.

S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005. ISBN 9780387953854. URL https://books.google.co.in/books?id=Fge-BwqhqIYC.

Johannes Mittmann and Markus Bläser. Independence in algebraic complexity theory. 2013.

Johannes Mittmann, Nitin Saxena, and Peter Scheiblechner. Algebraic independence in positive characteristic a p-adic calculus. *Trans. Amer. Math. Soc*, page 3450, 2012.

Anurag Pandey, Nitin Saxena, and Amit 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.

O. Perron. *Algebra: Die Grundlagen. I.* Number v. 1 in Göschens Lehrbücherei. Walter de Gruyter & Company, 1927. URL https://books.google.co.in/books?id=S-xauAAACAAJ.