# Constructing Faithful Homomorphisms over Fields of Finite Characteristic

**Prerona Chatterjee**
Tata Institute of Fundamental Research, Mumbai, India
prerona.chatterjee@tifr.res.in

**Ramprasad Saptharishi**
Tata Institute of Fundamental Research, Mumbai, India
ramprasad@tifr.res.in

## Abstract

We study the question of algebraic rank or transcendence degree preserving homomorphisms over finite fields. This concept was first introduced by Beecken et al. [3] and exploited by them and Agrawal et al. [2] to design algebraic independence based identity tests using the Jacobian criterion over characteristic zero fields. An analogue of such constructions over finite characteristic fields were unknown due to the failure of the Jacobian criterion over finite characteristic fields.

Building on a recent criterion of Pandey, Saxena and Sinhababu [14], we construct explicit faithful maps for some natural classes of polynomials in fields of positive characteristic, when a certain parameter called the *inseparable degree* of the underlying polynomials is bounded (this parameter is always 1 in fields of characteristic zero). This presents the first generalisation of some of the results of Beecken, Mittmann and Saxena [3] and Agrawal, Saha, Saptharishi, Saxena [2] in the positive characteristic setting.

**2012 ACM Subject Classification** Theory of computation → Algebraic complexity theory; Computing methodologies → Symbolic and algebraic manipulation

**Keywords and phrases** Faithful Homomorphisms, Identity Testing, Algebraic Independence, Finite characteristic fields

**Digital Object Identifier** 10.4230/LIPIcs.FSTTCS.2019.11

**Related Version** `https://eccc.weizmann.ac.il/report/2018/212/`

**Funding** *Prerona Chatterjee*: Supported by a fellowship of the DAE.
*Ramprasad Saptharishi*: Research supported by Ramanujan Fellowship of DST.

## 1 Introduction

Multivariate polynomials are fundamental objects in mathematics. These are the primary objects of study in algebraic complexity with regard to classifying their hardness as well as algorithmic tasks involving them. The standard computational model for computing multivariate polynomials is *algebraic circuits*. They are directed acyclic graphs with internal nodes labelled by "+" and "×" gates having the obvious operational semantics, and leaves are labelled by the input variables or field constants.

An important concept about relationships between polynomials is the notion of *algebraic dependence*. A set of polynomials $\mathbf{f} = \{f_1, \ldots, f_m\} \subset \mathbb{F}[\mathbf{x}]$ is said to be *algebraically dependent* if there is some nonzero polynomial combination of them that is zero. Such a nonzero polynomial $A(z_1, \ldots, z_m) \in \mathbb{F}[\mathbf{z}]$, if one exists, for which $A(f_1, \ldots, f_m) = 0$ is called the *annihilating polynomial* for the set $\{f_1, \ldots, f_m\}$. For instance, if $f_1 = x$, $f_2 = y$ and $f_3 = x^2 + y^2$, then $A = z_1^2 + z_2^2 - z_3$ is an annihilator. Note that the underlying field is very important. For example, the polynomials $x + y$ and $x^p + y^p$ are algebraically dependent over $\mathbb{F}_p$, but algebraically independent over a characteristic zero field.

39th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2019).
Editors: Arkadev Chattopadhyay and Paul Gastin; Article No. 11; pp. 11:1–11:14
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Algebraic independence is very well-studied and it is known that algebraically independent subsets of a given set of polynomials form a *matroid* ([13]). Hence, the size of the maximum algebraically independent subset of $\mathbf{f}$ is well-defined and is called the *algebraic rank* or *transcendence degree* of $\mathbf{f}$. We denote it by $\mathsf{algrank}(\mathbf{f}) = \mathsf{algrank}(f_1, \ldots, f_m)$.

Several computational questions arise from the above definition. For instance, given a set of polynomials $\mathbf{f} = \{f_1, \ldots, f_m\}$, each $f_i$ given in its dense representation, can we compute the algebraic rank of this set efficiently? What if the $f_i$'s are provided as algebraic circuits?

Furthermore, in instances when $\mathsf{algrank}(\mathbf{f}) = m - 1$, the smallest degree annihilating polynomial is unique ([9]). There could be various questions about the minimal degree annihilator in this case. For instance, can we compute it efficiently? Kayal [9] showed that even checking if the constant term of the annihilator is zero is NP-hard, and evaluating the annihilator at a given point is #P-hard. In fact, recently Guo, Saxena, Sinhababu [7] showed that even in the general case, checking if the constant term of every annihilator is zero is NP-hard. This effectively means that computing the algebraic rank via properties of the annihilating polynomials would be hard.

Despite this, over fields of characteristic zero, algebraic rank has an alternate characterisation via the Jacobian criterion. Jacobi [8] showed that the algebraic rank of a set of polynomials $\mathbf{f}(\subseteq \mathbb{F}[\mathbf{x}])$ is given by the linear rank (over the rational function field $\mathbb{F}(\mathbf{x})$) of the Jacobian of these polynomials. This immediately yields a randomized polynomial time algorithm to compute the algebraic rank of a given set of polynomials by computing the rank of the Jacobian matrix evaluated at a random point [12, 15, 16, 5].

## Faithful homomorphisms and PIT

Algebraic independence shares a lot of similarities with linear independence due to the matroid structure. One natural task is to find a *rank-preserving transformation* in this setting. This is defined by what are called *faithful homomorphisms.*

▶ **Definition 1.1** (Faithful homomorphisms [3]). *Let $\mathbf{f} = \{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ be a set of polynomials. If $\mathbb{K}$ is an extension field of $\mathbb{F}$, a homomorphism $\Phi : \mathbb{F}[\mathbf{x}] \to \mathbb{K}[\mathbf{y}]$ is said to be an* $\mathbb{F}$-faithful *homomorphism for $\{f_1, \ldots, f_m\}$ if*

$$\mathsf{algrank}_{\mathbb{F}}\{f_1, \ldots, f_m\} = \mathsf{algrank}_{\mathbb{F}}\{\Phi(f_1), \ldots, \Phi(f_m)\}.$$

Ideally, we would like a faithful homomorphism with $|\mathbf{y}| \approx \mathsf{algrank}\{\mathbf{f}\}$ and $\mathbb{K} = \mathbb{F}$. Beecken, Mittmann and Saxena [3] showed that a *generic* $\mathbb{F}$-linear homomorphism to $\mathsf{algrank}(\mathbf{f})$ many variables would be an $\mathbb{F}$-faithful homomorphism with high probability.

One important consequence of faithful homomorphisms is that they preserve nonzeroness of any polynomial composition of $f_1, \ldots, f_m$.

▶ **Lemma 1.2** ([3, 2]). *Suppose $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ and $\Phi$ is an $\mathbb{F}$-faithful homomorphism for $\{f_1, \ldots, f_m\}$. Then, for any circuit $C(z_1, \ldots, z_m) \in \mathbb{F}[z_1, \ldots, z_m]$, we have* $C(f_1, \ldots, f_m) = 0 \Leftrightarrow C(\Phi(f_1), \ldots, \Phi(f_m)) = 0$.

Thus, constructing explicit faithful homomorphisms can also be used for polynomial identity testing (PIT), which is the task of checking if a given algebraic circuit $C$ computes the identically zero polynomial. For PIT, the goal is to design a deterministic algorithm that runs in time polynomial in the size of the circuit. There are two types of PIT algorithms, *whitebox* and *blackbox* – in the blackbox setting, we are only provided evaluation access to the circuit and some of its parameters (such as degree, number of variables, size etc.). Thus blackbox PIT algorithms for a class $\mathcal{C}$ is equivalent to constructing a *hitting set*, which is a small list of points in $S \subset \mathbb{F}^n$ such that any nonzero polynomial $f \in \mathcal{C}$ is guaranteed to evaluate to a nonzero value on some $\mathbf{a} \in S$.

It follows from Lemma 1.2 that if we can construct explicit $\mathbb{F}$-faithful homomorphisms for a set $\{f_1, \ldots, f_m\}$ whose algebraic rank is $k \ll n$, then we have a *variable reduction* that preserves the nonzeroness of any composition $C(f_1, \ldots, f_m)$. This approach was used by Beecken, Mittmann and Saxena [3] and Agrawal, Saha, Saptharishi, Saxena [2], in the characteristic zero setting, to design identity tests for several subclasses by constructing faithful maps for $\{f_1, \ldots, f_m\}$ with algebraic rank at most $k = O(1)$, when

- each $f_i$ is a sparse polynomial,
- each $f_i$ is a product of multilinear, variable disjoint, sparse polynomials,
- each $f_i$ is a product of linear polynomials,

and further generalisations.

All the above constructions crucially depend on the fact that the rank of the Jacobian captures algebraic independence. However, this fact is true only over fields of characteristic zero and hence the above results are not known to hold over fields of positive characteristic.

## Algebraic independence over finite characteristic

A standard example to exhibit the failure of the Jacobian criterion over fields of finite characteristic, is $\left\{x^{p-1}y, y^{p-1}x\right\}$ – these polynomials are algebraically independent over $\mathbb{F}_p$ but the Jacobian is *not* full-rank over $\mathbb{F}_p$. Pandey, Saxena and Sinhababu [14] characterised the extent of failure of the Jacobian criterion for $\{f_1, \ldots, f_m\}$ by a notion called the *inseparable degree* associated with this set (formally defined in the full version [4]). Over characteristic zero, this is always 1 but over characteristic $p$ this is a power of $p$. In their work, Pandey et al. presented a Jacobian-like criterion to capture algebraic independence. Informally, each row of the *generalized Jacobian matrix* is obtained by taking the Taylor expansion of $f_i(\mathbf{x} + \mathbf{z})$ about a generic point, and truncating to just the terms of degree up to the *inseparable degree*[1] (formally defined in the full version [4]). The exact characterisation is more involved and is presented in Subsection 2.2 but we just state their theorem here.

▶ **Theorem 1.3.** [14] *Let $\{f_1, \ldots, f_k\}$ be a set of $n$-variate polynomials over a field $\mathbb{F}$ with inseparable degree $t$. Then, they are algebraically dependent if and only if*

$$\exists(\alpha_1, \ldots, \alpha_k)(\neq \mathbf{0}) \in \mathbb{F}(\mathbf{z})^k \ \textit{s.t.} \ \sum_{i=1}^{k} \alpha_i \cdot \boldsymbol{\mathcal{H}}_t(f_i) = 0 \mod \langle \boldsymbol{\mathcal{H}}_t(f_1), \ldots, \boldsymbol{\mathcal{H}}_t(f_k)\rangle_{\mathbb{F}(\mathbf{z})}^{\geq 2} + \langle \mathbf{x} \rangle^{t+1}.$$

Although the above statement seems slightly different from the one in [14], it is not too hard to see that they are actually equivalent. In their paper, Pandey et al. have stated their criterion in terms of functional dependence. However, stated this way, it clearly generalises the traditional Jacobian criterion.

In the setting when the *inseparable degree* is constant, this characterisation yields a randomized polynomial time algorithm to compute the algebraic rank. Thus, a natural question is whether this criterion can be used to construct faithful homomorphisms for similar classes of polynomials as studied by Beecken et al. [3] and Agrawal et al. [2].

▶ Remark 1.4. Recently, Guo et al. [7] showed that the task of testing algebraic independence is in $\mathsf{AM} \cap \mathsf{coAM}$ via a very different approach. However, it is unclear if their algorithm also yields constructions of faithful homomorphisms or applications to PIT in restricted settings.

[1] Over characteristic zero, the inseparable degree is 1 and this is just the vector of first order partial derivatives.

## 1.1 Our Results

Following up on the criterion of Pandey, Saxena and Sinhababu [14] for algebraic independence over finite characteristic, we extend the results of Beecken et al. [3] and Agrawal et al. [2] to construct faithful homomorphisms for some restricted settings. We note that we have not formally defined the term *inseparable degree* yet. Although the definition would be required to precisely understand the criterion of Pandey, Saxena and Sinhababu [14], it is not essential for the proofs in this paper. The interested reader may find these field theoretic preliminaries and formal definitions in the full version of the paper [4].

▶ **Theorem 1.5.** *Let $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that* algrank $\{f_1, \ldots, f_m\} = k$ *and the inseparable degree is $t$. If $t$ and $k$ are bounded by a constant, then we can construct a polynomial (in the input length) sized list of homomorphisms of the form $\Phi : \mathbb{F}[\mathbf{x}] \to \mathbb{F}(s)[y_0, y_1, \ldots, y_k]$ such that at least one of them is guaranteed to be to $\mathbb{F}$-faithful for the set $\{f_1, \ldots, f_m\}$, in the following two settings:*

- *When each of the $f_i$'s are sparse polynomials,*
- *When each of the $f_i$'s are products of variable disjoint, multilinear, sparse polynomials.*

Prior to this, construction of faithful homomorphisms over finite fields was known only in the setting when each $f_i$ has small individual degree [3]. Over characteristic zero fields, the inseparable degree is always 1 and hence the faithful maps constructed in [3], [2] over such fields can be viewed as special cases of our constructions.

The above theorem also holds for a few other models studied by Agrawal et al. [2] (for instance, occur-$k$ products of sparse polynomials). We mention the above two models just as an illustration of lifting the recipe for faithful maps from [3, 2] to the finite characteristic setting.

▶ **Corollary 1.6.** *If $\{f_1, \ldots, f_m\} \in \mathbb{F}[x_1, \ldots, x_n]$ is a set of $s$-sparse polynomials with algebraic rank $k$ and inseparable degree $t$ where $k, t = O(1)$. Then, for the class of polynomials of the form $C(f_1, \ldots, f_m)$ for any polynomial $C(z_1, \ldots, z_m) \in \mathbb{F}[\mathbf{z}]$, there is an explicit hitting set of size $(s \cdot \deg(C))^{O(1)}$.*

▶ **Corollary 1.7.** *Let $\mathcal{C} = \sum_{i=1}^{m} T_i$ be a depth-4 multilinear circuit of size $s$, where each $T_i$ is a product of variable-disjoint, $s$-sparse polynomials. Suppose $\{T_1, \ldots, T_m\} \in \mathbb{F}[x_1, \ldots, x_n]$ is a set of polynomials with algebraic rank $k$ and inseparable degree $t$ where $k, t = O(1)$. Then, for the class of polynomials of the form $C(T_1, \ldots, T_m)$ for any polynomial $C(z_1, \ldots, z_m) \in \mathbb{F}[\mathbf{z}]$, there is an explicit hitting set of size $(s \cdot \deg(C))^{O(1)}$.*

### Comparison with the PIT of [14]

Pandey et al. [14] also gives a PIT result for circuits of the form $\sum_i (f_{i,1} \cdots f_{i,m})$ where algrank $\{f_{i,1}, \ldots, f_{i,m}\} \le k$ for every $i$ and each $f_{i,j}$ is a degree $d$ polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. They extend the result of Kumar and Saraf [11] to arbitrary fields by giving quasi-polynomial time hitting sets if $kd$ is at most poly-logarithmically large.

Corollary 1.7 however is incomparable to the PIT of Pandey et al. [14] for the following reasons:

- The algebraic rank bound in the case of [14, 11] is a gate-wise bound rather than a global bound. Thus, in principle, it could be the case that algrank $\{f_{i,1}, \ldots, f_{i,m}\}$ is bounded by $k$ for each $i$ but this would not necessarily translate to a bound on algrank $\left\{\prod_j f_{i,j} \ : \ i\right\}$ as demanded in Corollary 1.7. Hence, in this regard, the PIT of [14, 11] is stronger.

- In the regime when we have $\mathsf{algrank}\left\{\prod_j f_{i,j} \ : \ i\right\}$ and the inseparable degree of this set to be bounded by a constant, Corollary 1.7 presents an explicit hitting set of polynomial size, whereas it is unclear if [14, 11] provide any non-trivial upper bound as this does not translate to any bound on $\mathsf{algrank}\left\{f_{i,1}, \ldots, f_{i,m}\right\}$.

### On other models studied by Agrawal et al. [2]

Our results, in its current form, do not extend directly some of the other models studied by Agrawal et al. [2], most notably larger depth multilinear formulas. The primary hurdle appears to be the *recursive* use of explicit faithful homomorphisms for larger depth formulas. In the characteristic $p$ setting, unfortunately, it is unclear if a bound on the inseparable degree of the original gates can be used to obtain a bound on the inseparable degree of other sets of polynomials considered in the recursive construction of Agrawal et al. [2].

## 1.2 Proof overview

The general structure of the proof follows the outline of Agrawal et al. [2]'s construction of faithful homomorphisms in the characteristic zero setting. Roughly speaking, this can be described in the following steps:

**Step 1** : For a *generic linear map* $\Phi : \mathbf{x} \to \mathbb{F}(s)[y_1, \ldots, y_k]$, write the Jacobian of the set $\{f_1 \circ \Phi, \cdots, f_k \circ \Phi\}$ in terms of the Jacobian of the set $\{f_1, \cdots, f_k\}$. This can be described succinctly as a matrix product of the form

$$J_{\mathbf{y}}(f \circ \Phi) = \Phi(J_{\mathbf{x}}(\mathbf{f})) \cdot J_{\mathbf{y}}(\Phi(\mathbf{x})).$$

**Step 2** : We know that $J_{\mathbf{x}}(\mathbf{f})$ is full rank. Ensure that $\Phi(J_{\mathbf{x}}(\mathbf{f}))$ (where $\Phi$ is applied to every entry of the matrix $J_{\mathbf{x}}(\mathbf{f})$) remains full rank. This can be done if $\mathbf{f}$'s are some structured polynomials such as sparse polynomials, or variable-disjoint products of sparse polynomials etc.

**Step 3** : Choose the map $\Phi$ so as to ensure that

$$\operatorname{rank}(\Phi(J_{\mathbf{x}}(\mathbf{f})) \cdot J_{\mathbf{y}}(\Phi(\mathbf{x}))) = \operatorname{rank}(\Phi(J_{\mathbf{x}}(\mathbf{f}))).$$

This is typically achieved by choosing $\Phi$ so as to make $J_{\mathbf{y}}(\Phi(\mathbf{x}))$ a *rank-extractor*. It was shown by Gabizon and Raz [6] that a parametrized Vandermonde matrix has this property, and this allows one to work with a homomorphism of the form (loosely speaking)

$$\Phi : x_i \mapsto \sum_{j=1}^{k} s^{ij} y_j.$$

We would like to execute essentially the same sketch over fields of finite characteristic but we encounter some immediate difficulties. The criterion of Pandey et al. [14] over finite characteristic is more involved but it is reasonably straightforward to execute Steps 1 and 2 in the above sketch using the chain rule of (Hasse) derivatives. The primary issue is in executing Step 3 and this is for two very different reasons.

The first is that, unlike in the characteristic zero setting, the analogue of the matrix $J_{\mathbf{y}}(\Phi(\mathbf{x}))$ have many correlated entries. In the characteristic zero setting, we have complete freedom to choose $\Phi$ so that $J_{\mathbf{y}}(\Phi(\mathbf{x}))$ can be any matrix that we want. Roughly speaking, we only have $n \cdot k$ parameters to define $\Phi$ but the analogue of $J_{\mathbf{y}}(\Phi(\mathbf{x}))$ is much larger in the finite characteristic setting. Fortunately, there is just about enough structure in the matrix that we can show that it continues to have some rank-preserving properties. This is done in Section 3.

The second hurdle comes from the subspace that we need to work with in the modified criterion. The *rank-extractor* is essentially parametrized by the variable $s$. In order to show that it preserves the rank of $\Phi(J_{\mathbf{x}}(\mathbf{f}))$ under right multiplication, we would like ensure that the variable $s$ effectively does not appear in this matrix. In the characteristic zero setting, this is done by suitable restriction on other variables to remove any dependencies on $s$ in $\Phi(J_{\mathbf{x}}(\mathbf{f}))$. Unfortunately, in the criterion of Pandey et al. [14], we have to work modulo some suitable subspace and these elements introduce other dependencies on $s$ that appear to be hard to remove. Due to this hurdle, we are unable to construct $\mathbb{F}(s)$-faithful homomorphisms even in restricted settings.

However, we observe that for the PIT applications, we are merely required to ensure that $\{f_1 \circ \Phi, \ldots, f_k \circ \Phi\}$ remain $\mathbb{F}$-algebraically independent instead of $\mathbb{F}(s)$-algebraically independent. With this weaker requirement, we can obtain a little more structure in the subspace involved and that lets us effectively execute Step 3.

### Structure of the paper

We begin by describing some preliminaries that are necessary to understand the criterion of Pandey, Saxena and Sinhababu [14] in the next section. Following that, in Section 3, we show that certain Vandermonde-like matrices have *rank-preserving properties.* We use these matrices to give a recipe of constructing faithful maps, in Section 4, and execute this for the settings of Theorem 1.5 in Section 5.

## 2 Preliminaries

### 2.1 Notations

- For a positive integer $m$, we will use $[m]$ to denote set $\{1, 2, \ldots, m\}$.
- We will use bold face letters such as $\mathbf{x}$ to denote a set of indexed variables $\{x_1, \ldots, x_n\}$. In most cases the size of this set would be clear from context. Extending this notation, we will use $\mathbf{x}^{\mathbf{e}}$ to denote the monomial $x_1^{e_1} \cdots x_n^{e_n}$.
- For a set of polynomials $f_1, \ldots, f_m$, we will denote by $\langle f_1, \ldots, f_m \rangle_{\mathbb{K}}$ the set of all $\mathbb{K}$-linear combinations of $f_1, \ldots, f_m$. Extending this notation, we will use $\langle f_1, \ldots, f_m \rangle_{\mathbb{K}}^{r}$ to denote the set of all $\mathbb{K}$-linear combinations of $r$-products $f_{i_1} \cdots f_{i_r}$ (with $i_1, \ldots, i_r \in [m]$) and $\langle f_1, \ldots, f_m \rangle_{\mathbb{K}}^{\geq r}$ similarly. In instances when we just use $\langle f_1, \ldots, f_m \rangle$, we will denote the *ideal* generated by $f_1, \ldots, f_m$.

### Hitting set generators

▶ **Definition 2.1** (Hitting set generators (HSG)). *Let $\mathcal{C}$ be a class of $n$-variate polynomials. A tuple of polynomials $\mathcal{G} = (G_1(\alpha), \ldots, G_n(\alpha))$ is a* hitting set generator *for $\mathcal{C}$ if for every nonzero polynomial $P(\mathbf{x}) \in \mathcal{C}$ we have $P(G_1(\alpha), \ldots, G_n(\alpha))$ is a nonzero polynomial in $\alpha$.*

*The degree of this generator is defined to be* $\max \deg(G_i)$*.*

Intuitively, such a tuple can be used to *generate* a hitting set for $\mathcal{C}$ by running over several instantiations of $\alpha$. Also, it is well known that any hitting set can be transformed into to HSG via interpolation.

### Isolating weight assignments

Suppose $\mathsf{wt} : \{x_i\} \to \mathbb{N}$ is a weight assignment for the variables $\{x_1, \ldots, x_n\}$. We can extend it to define the weight of a monomial as follows.

$$\mathsf{wt}(\mathbf{x}^{\mathbf{e}}) = \sum_{i=1}^{n} e_i \cdot \mathsf{wt}(x_i)$$

▶ **Definition 2.2.** *A weight assignment* $\mathsf{wt} : \{x_i\} \to \mathbb{N}$ *is said to be isolating for a set $S$ of monomials if every pair of distinct monomials in $S$ receives distinct weights.*

With this background, we are now ready to state the criterion for algebraic independence over fields of finite characteristic. Similar to the Jacobian Criterion, Pandey, Saxena and Sinhababu [14] reduce the problem of checking algebraic independence to that of checking linear independence. However, their criterion is slightly more subtle in the sense that we will have to check the linear independence of a set of vectors modulo a large subspace.

A formal statement of the Jacobian criterion along with some field theoretic preliminaries are present in the full version [4]. These include the formal definition of terms such as *inseparable degree* etc. to precisely understand the criterion of Pandey, Saxena and Sinhababu [14] but are not essential for the proof in this paper.

## 2.2 The PSS Criterion over fields of finite characteristic

In this section we present a slightly different perspective on the criterion of Pandey et al. [14]. A more elaborate discussion of their criterion is deferred to the full version [4].

Define the following operator $\boldsymbol{\mathcal{H}}_t(f) := \deg_{\leq t}(f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z}))$, where $\deg_{\leq t}$ restricts to just those monomials in $\mathbf{x}$ of degree at most $t$. It is also worth noting that $\boldsymbol{\mathcal{H}}_t(f)$ does not have a constant term and this would become useful in the criterion.

The operator $\boldsymbol{\mathcal{H}}_t$ however, as defined above, is indexed by $t$. Pandey et al. [14] show that the correct value of $t$ to work with is the *inseparable degree* of the given set of polynomials (see full version [4] for details).

Let $\mathcal{U}_t(\mathbf{f}) = \mathcal{U}_t(f_1, \ldots, f_k)$ denote the subspace $\langle \boldsymbol{\mathcal{H}}_t(f_1), \ldots, \boldsymbol{\mathcal{H}}_t(f_k) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}$. Then, for any $h \in \mathcal{U}_t(\mathbf{f})$, we define the modified Jacobian matrix as follows.

$$\mathsf{PSSJac}_t(\mathbf{f}, h) = \begin{bmatrix} \boldsymbol{\mathcal{H}}_t(f_1) + h \\ \boldsymbol{\mathcal{H}}_t(f_2) \\ \vdots \\ \boldsymbol{\mathcal{H}}_t(f_k) \end{bmatrix}.$$

The columns of this matrix are indexed by monomials in $\mathbf{x}$ and entries in the column indexed by $\mathbf{x}^{\mathbf{e}}$ are the coefficient of $\mathbf{x}^{\mathbf{e}}$ in the corresponding rows.

▶ **Theorem 2.3** (Alternate Statement for the PSS-criterion)**.** *Let $\{f_1, \ldots, f_k\}$ be a set of $n$-variate polynomials over a field $\mathbb{F}$ with inseparable degree $t$. Then, they are algebraically independent if and only if for every $h \in \mathcal{U}_t(\mathbf{f})$,* $\mathsf{PSSJac}_t(\mathbf{f}, h)$ *is full rank.*

Let $\mathcal{V}_t(g_1, \ldots, g_k)$ denote the subspace $\langle \boldsymbol{\mathcal{H}}_t(g_1), \ldots, \boldsymbol{\mathcal{H}}_t(g_k) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{g}(\mathbf{v}))} \bmod \langle \mathbf{y} \rangle^{t+1}$. The following lemma can be inferred in the dependent case.

▶ **Lemma 2.4.** *Let $\mathbb{F}$ any field and $\mathbb{K}$ be an extension field of $\mathbb{F}$. If $\{g_1, \ldots, g_k\}$ is a set of $n$-variate polynomials in $\mathbb{K}[\mathbf{y}]$ that are $\mathbb{F}$-algebraically dependent, then for any positive integer $t$, there exists $h' \in \mathcal{V}_t(g_1, \ldots, g_k)$ such that* $\mathsf{PSSJac}_t(\mathbf{g}, h')$ *is not full rank.*

A proof is given in the full version [4] for the sake of completeness, but we note that the steps are almost identical to those in [14].

## 3 Rank Condensers from Isolating Weight Assignments

In this section, we focus on *rank-preserving* properties of certain types of matrices. These are slight generalisations of similar properties of Vandermonde matrices that were proved by Gabizon and Raz [6] that would be necessary for the application to constructing faithful homomorphisms.

▶ **Lemma 3.1.** *Suppose we have an $n \times n$ matrix $V$ given by*

$$V = \left(\left(s^{j \cdot w_i}\right)\right)_{i,j}$$

*where $w_i < w_j$ whenever $i < j$. If $V'$ is a matrix obtained from $V$ by replacing some of the non-diagonal entries by zero, then $\det(V') \neq 0$ and furthermore $\deg(\det(V')) = \sum_{i=1}^{n} i \cdot w_i$.*

The proof of this lemma is not too hard, and can be found in the full version [4]. The following lemma extends this to *rank-preserving* properties of a related matrix.

▶ **Lemma 3.2.** *Let $A$ be a matrix over a field $\mathbb{F}$ with $k$ rows and columns indexed by monomials in $\mathbf{x}$ of degree at most $D$ that is full-rank. Further, let $w = (w_1, \ldots, w_n)$ be an isolating weight assignment for the set of degree $D$ monomials, and let $\mathsf{wt}(\mathbf{x}^{\mathbf{e}}) = \sum_{i=1}^{n} w_i e_i$.*

*Suppose $M_\Phi$ is a matrix whose rows are indexed by monomials in $\mathbf{x}$ of degree at most $D$, and columns indexed by* pure monomials $\left\{y_i^d \;:\; i \in \{1, \ldots, k\}\;,\; d \leq D\right\}$ *given by*

$$M_\Phi(\mathbf{x}^{\mathbf{e}}, y_i^d) = \begin{cases} s^{i \cdot \mathsf{wt}(\mathbf{x}^{\mathbf{e}})} & \text{if } \deg(\mathbf{x}^{\mathbf{e}}) = d \\ 0 & \text{otherwise} \end{cases}.$$

*where $s$ is a formal variable. Then, $\operatorname{rank}_{\mathbb{F}(s)}(A \cdot M_\Phi) = \operatorname{rank}_{\mathbb{F}}(A)$.*

**Proof.** By the Cauchy-Binet formula, if we restrict $M'_\Phi$ to a set $T$ of $k$-columns, then

$$\det(A \cdot M'_\Phi[T]) = \sum_{\substack{S \subseteq \text{Columns}(A) \\ |S| = k}} \det(A[S]) \cdot \det(M'_\Phi[S, T])$$

We wish to show that the above sum is nonzero for some choice of columns $T$. We do that by first defining a weight function on minors of $A$, then proving that there is a unique nonzero minor of $A$ of largest weight, and then choosing a set of columns $T$ such that the degree of $\det(M'_\Phi[S,T])$ coincides with this chosen weight function. Define the *weight* of a minor of $A$ as follows:

> Suppose the columns of the minor is indexed by $S = \{\mathbf{x}^{\mathbf{e_1}}, \ldots, \mathbf{x}^{\mathbf{e_k}}\}$ with the property that $\mathsf{wt}(\mathbf{x}^{\mathbf{e_1}}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e_2}}) < \cdots < \mathsf{wt}(\mathbf{x}^{\mathbf{e_k}})$. Define the weight of this minor as
>
> $$\mathsf{wt}(S) = \sum_{i=1}^{k} i \cdot \mathsf{wt}(\mathbf{x}^{\mathbf{e_i}})$$
>
> where, recall, $\mathsf{wt}(\mathbf{x}^{\mathbf{e_i}}) = \sum_j w_j \cdot \mathbf{e_i}(j)$.

▷ Claim 3.3. There is a unique nonzero $k \times k$ minor of $A$ of maximum weight.

Proof. Suppose $S_1$ and $S_2$ are two different minors of $A$ with the same weight. We will just identify $S_1$ and $S_2$ by the set of column indices for simplicity. Say $S_1$ has columns indexed by $\mathbf{x}^{\mathbf{e_1}}, \ldots, \mathbf{x}^{\mathbf{e_k}}$ with $\mathsf{wt}(\mathbf{x}^{\mathbf{e_1}}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e_2}}) < \cdots < \mathsf{wt}(\mathbf{x}^{\mathbf{e_k}})$ and $S_2$ has columns indexed by $\mathbf{x}^{\mathbf{e'_1}}, \ldots, \mathbf{x}^{\mathbf{e'_k}}$ with $\mathsf{wt}(\mathbf{x}^{\mathbf{e'_1}}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e'_2}}) < \cdots < \mathsf{wt}(\mathbf{x}^{\mathbf{e'_k}})$.

Suppose $S_1$ and $S_2$ agree on the first $i$ columns, that is $\mathbf{e}_j = \mathbf{e}'_j$ for all $j \leq i$, and say $\mathsf{wt}(\mathbf{e}_{i+1}) < \mathsf{wt}(\mathbf{e}'_{i+1})$. By the matroid property, there must be some column $\mathbf{x}^{\mathbf{e}'_j}$ from $S_2$ that we can add to $S_1 \setminus \{\mathbf{x}^{\mathbf{e}_{i+1}}\}$ so that $S = S_1 \setminus \{\mathbf{x}^{\mathbf{e}_{i+1}}\} \cup \left\{\mathbf{x}^{\mathbf{e}'_j}\right\}$ is also a nonzero minor of $A$. Suppose that

$$\mathsf{wt}(\mathbf{x}^{\mathbf{e}_1}) < \cdots < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_{i+r}}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e}'_j}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_{i+r+1}}) < \cdots < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_k}).$$

Then,

$$\begin{aligned}\mathsf{wt}(S) &= \sum_{a=1}^{i} a \cdot \mathsf{wt}(\mathbf{x}^{\mathbf{e}_a}) + \sum_{a=i+2}^{i+r} (a-1) \cdot \mathsf{wt}(\mathbf{x}^{\mathbf{e}_a}) + (i+r)\,\mathsf{wt}(\mathbf{x}^{\mathbf{e}'_j}) + \sum_{a=i+r+1}^{k} a \cdot \mathsf{wt}(\mathbf{x}^{\mathbf{e}_a}) \\ &> \sum_{a=1}^{i} a \cdot \mathsf{wt}(\mathbf{x}^{\mathbf{e}_a}) + (i+1)\,\mathsf{wt}(\mathbf{x}^{\mathbf{e}'_j}) + \sum_{a=i+2}^{k} a \cdot \mathsf{wt}(\mathbf{x}^{\mathbf{e}_a}) > \sum_{a=1}^{k} a \cdot \mathsf{wt}(\mathbf{x}^{\mathbf{e}_a}) = \mathsf{wt}(S_1)\end{aligned}$$

Hence, there cannot be two different nonzero minors of $A$ of the same weight. Thus, the nonzero minor of largest weight is unique. ◁

We will now choose $k$ columns from $M'_\Phi$ as follows in such a way that the degree of the corresponding determinant agrees with the weight function. Note that the matrix $M'_\Phi$ has a natural block-diagonal structure based on the degree of the monomials indexing the rows and columns.

- Let $S_0$ be the unique $k \times k$ minor of $A$ having maximum weight. Further, assume its columns are indexed by $\mathbf{x}^{\mathbf{e_1}}, \ldots, \mathbf{x}^{\mathbf{e_k}}$ with $\mathsf{wt}(\mathbf{x}^{\mathbf{e_1}}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e_2}}) < \ldots < \mathsf{wt}(\mathbf{x}^{\mathbf{e_k}})$. Let $d_i = \deg(\mathbf{x}^{\mathbf{e}_i}) = \sum_j (\mathbf{e}_i)_j$.
- Choose the columns $T = \left\{y_1^{d_1}, y_2^{d_2}, \ldots, y_k^{d_k}\right\}$ of the matrix $M'_\Phi$.

By Lemma 3.1, for any set of $S' \subseteq \text{Columns}(A)$, we have $\deg(\det(M_\Phi[S',T])) \leq \mathsf{wt}(S')$ and furthermore we also have $\deg(M'_\Phi[S_0,T]) = \mathsf{wt}(S_0)$ as we chose the columns $T$ to ensure that the main diagonal of the sub-matrix has only nonzero elements. Hence,

$$\det(A \cdot M'_\Phi[T]) = \sum_{\substack{S \subseteq \text{Columns}(A) \\ |S|=k}} \det(A[S]) \cdot \det(M'_\Phi[S,T]) \neq 0$$

since the contribution from $A[S_0]\det(M'_\Phi[S_0,T])$ is the unique term of highest degree and so cannot be cancelled. ◀

## 4 Construction of Explicit Faithful Maps

We will be interested in applying a map $\Phi : \mathbb{F}[\mathbf{x}] \to \mathbb{F}(s)[\mathbf{y}]$ and study the transformation of the PSS-Jacobian. Since the entries of the PSS-Jacobian involve $\mathcal{H}_t(f(\mathbf{x})) = \deg_{\leq t}(f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z}))$, we would need to also work with $\mathcal{H}_t(g(\mathbf{y}))$ where $g(\mathbf{y}) = f \circ \Phi$. To make it easier to follow, we shall use a different name for the variables in the two cases. Hence,

$$\mathcal{H}_t(f(\mathbf{x})) := \deg_{\leq t}(f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z})) \quad , \quad \mathcal{H}_t(g(\mathbf{y})) := \deg_{\leq t}(g(\mathbf{y}+\mathbf{v}) - g(\mathbf{v})).$$

## 4.1 Recipe for constructing faithful maps

Let $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ be polynomials with $\mathsf{algrank}\,\{f_1, \ldots, f_m\} = k$ and inseparable degree $t$. We will work with linear transformations of the form:

$$\Phi : x_i \mapsto a_i y_0 + \sum_{j=1}^{k} s^{w_i \cdot j} y_j, \quad \text{for all } i \in [n],$$

$$\Phi_z : z_i \mapsto a_i v_0 + \sum_{j=1}^{k} s^{w_i \cdot j} v_j, \quad \text{for all } i \in [n].$$

where all the variables on the RHS are formal variables. Further, define $\{g_1, \ldots, g_m\} \in \mathbb{F}[\mathbf{z}]$ as $g_i = f_i \circ \Phi$ and $\boldsymbol{\mathcal{H}}_t(g_i) = \deg_{\leq t}(g_i(\mathbf{y} + \mathbf{v}) - g_i(\mathbf{v}))$.

The main lemma of this section is the following *recipe* for constructing faithful maps.

▶ **Lemma 4.1** (Recipe for faithful homomorphisms). *Let $f_1, \ldots, f_m \in \mathbb{F}[\mathbf{x}]$ be polynomials such that their algebraic rank is at most $k$ and suppose the inseparable degree is bounded by a constant $t$. Further,*

- *suppose $\mathcal{G} = (G_1(\alpha), \ldots, G_n(\alpha))$ is a* hitting-set generator (HSG) *for the class of all $k \times k$ minors of $\mathsf{PSSJac}_t(\mathbf{f}, h)$ for any $h \in \mathcal{U}_t(\mathbf{f})$.*
- *suppose $w : [n] \to \mathbb{N}$ is an isolating weight assignment for the set of $n$-variate monomials of degree at most $t$.*

*Then, the homomorphism $\Phi : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}(s, \alpha)[y_0, \ldots, y_k]$ defined as*

$$\Phi : x_i \mapsto y_0 G_i(\alpha) + \sum_{j=1}^{k} y_j \cdot s^{w(i)j},$$

*is an $\mathbb{F}$-faithful homomorphism for the set $\{f_1, \ldots, f_m\}$.*

As mentioned earlier, the rough proof sketch would be to first write the PSS-Jacobian of the transformed polynomials $\mathbf{g}$ in terms of $\mathbf{f}$, express that as a suitable matrix product, and use some *rank extractor* properties of the associated matrix, as described in Section 3. So first, let us see how we can get the required matrix product.

▶ **Lemma 4.2** (Evolution of polynomials under $\Phi$). *Let $\Phi : \mathbf{x} \to \mathbb{F}(s)[\mathbf{y}]$ and $\Phi_z : \mathbf{z} \to \mathbb{F}(s)[\mathbf{v}]$ be given as above. Further, for any polynomial $h'(a_1, \ldots, a_m) \in \mathbb{F}(\mathbf{g}(\mathbf{v}))[\mathbf{a}]$, define $h(a_1, \ldots, a_m) \in \mathbb{F}(\mathbf{f}(\mathbf{z}))[\mathbf{a}]$ as follows.*

$\mathsf{coeff}_{\mathbf{a}^{\mathbf{e}}}(h)$ *is got by replacing every occurrence of $g_i(\mathbf{v})$ by $f_i(\mathbf{z})$ in* $\mathsf{coeff}_{\mathbf{a}^{\mathbf{e}}}(h')$

*Then,*

$$h'(\boldsymbol{\mathcal{H}}_t(g_1), \ldots, \boldsymbol{\mathcal{H}}_t(g_m)) = \Phi \circ \Phi_z(h(\boldsymbol{\mathcal{H}}_t(f_1), \ldots, \boldsymbol{\mathcal{H}}_t(f_m))).$$

It is worth noting that the polynomial $h(a_1, \ldots, a_m)$ is independent of $s$. This would be crucial later on in the proof. The proof of this lemma is not too hard and can be found in the full version [4].

▶ **Corollary 4.3** (Matrix representation of the evolution). *Suppose $A'$ is a matrix whose columns are indexed by monomials in $\mathbf{y}$. Further suppose a row in $A'$ corresponds to a polynomial, say $h'(\boldsymbol{\mathcal{H}}_t(g_1), \ldots, \boldsymbol{\mathcal{H}}_t(g_m)) \in \mathbb{F}(\mathbf{g}(\mathbf{v}))[\mathbf{y}]$, whose entry in the column indexed by $\mathbf{y}^{\mathbf{e}}$ is $\mathsf{coeff}_{\mathbf{y}^{\mathbf{e}}}(h'(\boldsymbol{\mathcal{H}}_t(\mathbf{g}))) \in \mathbb{F}(\mathbf{v}, \mathbf{s})$. If $A$ is the corresponding matrix (having entries from $\mathbb{F}(\mathbf{z})$) with columns indexed by monomials in $\mathbf{x}$ and the corresponding row being $h(\boldsymbol{\mathcal{H}}_t(f_1), \ldots, \boldsymbol{\mathcal{H}}_t(f_m)) \in \mathbb{F}(\mathbf{f}(\mathbf{z}))[\mathbf{x}]$ as described in Lemma 4.2, then*

$$A' = \Phi_z(A) \times \widetilde{M_\Phi}$$

*where $\widetilde{M_\Phi}(\mathbf{x}^{\mathbf{e}}, \mathbf{y}^{\mathbf{d}}) = \mathsf{coeff}_{\mathbf{y}^{\mathbf{d}}}(\Phi(\mathbf{x}^{\mathbf{e}}))$.*

Using these and Lemma 3.2, we are now ready to prove Lemma 4.1.

**Proof of Lemma 4.1.** Without loss of generality, say $\{f_1, \ldots, f_k\}$ is an algebraically independent set. We wish to show that if $g_i = f_i \circ \Phi$, then $\{g_1, \ldots, g_k\}$ is an $\mathbb{F}$-algebraically independent set as well. Assume on the contrary that $\{g_1, \ldots, g_k\}$ is an $\mathbb{F}$-algebraically dependent set. Then for $t$ being the inseparable degree of $\{f_1, \ldots, f_k\}$, by Lemma 2.4, there exists

$$h' \in \mathcal{V}_t(g_1, \ldots, g_k) := \langle \boldsymbol{\mathcal{H}}_t(g_1), \ldots, \boldsymbol{\mathcal{H}}_t(g_k) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{g}(\mathbf{v}))} \bmod \langle \mathbf{y} \rangle^{t+1}$$

such that $\mathsf{PSSJac}_t(\mathbf{g}, h')$ is not full rank. Without loss of generality, we can assume that the entries of $\mathsf{PSSJac}_t(\mathbf{g}, h')$ are denominator-free by clearing out any denominators. Corresponding to $h'$, define $h$ as in Lemma 4.2, which would also satisfy that

$$h \in \mathcal{U}_t(f_1, \ldots, f_k) := \langle \boldsymbol{\mathcal{H}}_t(f_1), \ldots, \boldsymbol{\mathcal{H}}_t(f_k) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}.$$

It is worth stressing the fact that the polynomial $h$ is independent of the variable $s$. Then by Corollary 4.3 we get

$$\mathsf{PSSJac}_t(\mathbf{g}, h') = \Phi_z(\mathsf{PSSJac}_t(\mathbf{f}, h)) \times \widetilde{M_\Phi}.$$

Now, if we substitute $v_0 = 1$ and $v_i = 0$ for every $i \in [k]$, we get

$$\mathsf{PSSJac}_t(\mathbf{g}, h')(v_0 = 1, v_1 = \ldots = v_k = 0) = \mathsf{PSSJac}_t(\mathbf{f}, h)(\mathbf{z} = \mathbf{G}(\alpha)) \times \widetilde{M_\Phi}.$$

But since $\{f_1, \ldots, f_k\}$ is algebraically independent, Theorem 2.3 yields that $\mathsf{PSSJac}_t(\mathbf{f}, h)$ has full rank. Thus, $\mathsf{PSSJac}_t(\mathbf{f}, h)(\mathbf{z} = \mathbf{G}(\alpha))$ also has full rank since $\mathcal{G} = (G_1(\alpha), \ldots, G_n(\alpha))$ is a hitting-set generator for the class of all $k \times k$ minors of $\mathsf{PSSJac}_t(\mathbf{f}, h)$. Most crucially, the matrix $\mathsf{PSSJac}_t(\mathbf{f}, h)$ is independent of the variable $s$.

To complete the proof, we need to show that multiplication by $\widetilde{M_\Phi}$ continues to keep this full rank to contradict the initial assumption that $\mathsf{PSSJac}_t(\mathbf{g}, h')$ was not full rank.

Finally note that for the $\Phi$ we have defined, $\widetilde{M_\Phi}$ restricted to only the *pure monomial* columns

$$\left\{ y_i^j \ : \ i \in \{1, \ldots, k\} \ , \ j \in \{0, 1, \ldots, t\} \right\},$$

is the same as $M_\Phi$ as defined in Lemma 3.2. Further, $w$ is an isolating weight assignment for the set of $n$-variate monomials of degree at most $t$, we satisfy the requirements of Lemma 3.2. Hence, by Lemma 3.2,

$$\begin{aligned} \operatorname{rank}_{\mathbb{F}(s,\alpha)} \left( \mathsf{PSSJac}_t(\mathbf{g}, h')(v_0 = 1, v_1 = \ldots, v_k = 0) \right) &= \operatorname{rank}_{\mathbb{F}(\alpha)} \mathsf{PSSJac}_t(\mathbf{f}, h)(\mathbf{z} = \mathbf{G}(\alpha)) \\ \implies \operatorname{rank}_{\mathbb{F}(s,\alpha,\mathbf{v})} \left( \mathsf{PSSJac}_t(\mathbf{g}, h') \right) &\geq \operatorname{rank}_{\mathbb{F}(\alpha)} \mathsf{PSSJac}_t(\mathbf{f}, h)(\mathbf{z} = \mathbf{G}(\alpha)) \\ &= k, \end{aligned}$$

which contradicts our assumption that it was not full rank. Hence, it must indeed be the case that $\{f_1 \circ \Phi, \ldots, f_k \circ \Phi\}$ is $\mathbb{F}$ - algebraically independent. ◀

## 5 Explicit faithful maps and PIT applications in restricted settings

We now describe some specific instantiations of the recipe given by Lemma 4.1 in restricted settings. Let us first recall the statement of the main theorem.

▶ **Theorem 1.5.** *Let $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$ such that* $\mathsf{algrank}\{f_1, \dots, f_m\} = k$ *and the inseparable degree is $t$. If $t$ and $k$ are bounded by a constant, then we can construct a polynomial (in the input length) sized list of homomorphisms of the form $\Phi : \mathbb{F}[\mathbf{x}] \to \mathbb{F}(s)[y_0, y_1, \dots, y_k]$ such that at least one of them is guaranteed to be to $\mathbb{F}$-faithful for the set $\{f_1, \dots, f_m\}$, in the following two settings:*

- *When each of the $f_i$'s are sparse polynomials,*
- *When each of the $f_i$'s are products of variable disjoint, multilinear, sparse polynomials.*

**Proof.** By Lemma 4.1, $\Phi : \mathbb{F}[x_1, \dots, x_n] \to \mathbb{F}(s, \alpha)[y_0, \dots, y_k]$ defined as

$$\Phi : x_i \mapsto y_0 G_i(\alpha) + \sum_{j=1}^{k} y_j \cdot s^{w(i)j},$$

is a faithful homomorphism for the set $\{f_1, \dots, f_m\}$ if for any $h \in \mathcal{U}_t(\mathbf{f})$, $w = (w_1, \dots, w_n)$ is a basis isolating weight assignment for $\mathsf{PSSJac}(\mathbf{f}, h)$ and $\mathcal{G} = (G_1(\alpha), \dots, G_n(\alpha))$ is such that the rank of $\mathsf{PSSJac}_t(\mathbf{f}, h)$ is preserved after the substitution $\mathbf{z} \to \mathbf{a}$ for some $\mathbf{a} \in \mathcal{G}$. We define the weight using the standard hashing techniques [10, 1].

**Defining $w$:** Define $w : [n] \to \mathbb{N}$ as $w(i) = (t+1)^i \pmod{p}$, where $t$ is the inseparable degree.

Assuming $t$ to be a constant, there are only poly($n$) many distinct monomials in $\mathbf{x}$ of degree at most $t$. Thus, standard results by Klivans and Spielman [10] or Agrawal and Biswas [1] shows that it suffices to go over poly($n$) many '$p$'s before $w$ isolates all monomials in $\mathbf{x}$ of degree at most $t$.
Let $\mathsf{PSSJac}_t(\mathbf{f})$ be the matrix with columns indexed by monomials in $\mathbf{x}$ of degree at most $t$ and rows by $k$-variate monomials $\mathbf{a}^{\mathbf{e}}$ in degree at most $t$, defined as follows.

$$\mathsf{PSSJac}_t(\mathbf{f})[\mathbf{a}^{\mathbf{e}}, \mathbf{x}^{\mathbf{d}}] = \mathsf{coeff}_{\mathbf{x}^{\mathbf{d}}}(\boldsymbol{\mathcal{H}}_t(\mathbf{f})^{\mathbf{e}})$$

Set $K = \binom{k+t}{t}$ be the number of rows in $\mathsf{PSSJac}_t(\mathbf{f})$. Then the following is true.

▷ Claim 5.1. If $\mathcal{G}$ is a hitting set generator for every $K' \times K'$ minor of $\mathsf{PSSJac}_t(\mathbf{f})$ where $K' \leq K$, then the rank of $\mathsf{PSSJac}_t(\mathbf{f}, h)$ is preserved for every $h \in \mathcal{U}_t(\mathbf{f})$.

Proof. We need to show that there is an $\mathbf{a}$ in $\mathcal{G}$ which has the following property:

> For any $h \in \mathcal{U}_t(\mathbf{f})$, if $\{H_t(f_1) + h, H_t(f_2), \dots, H_t(f_k)\}$ are linearly independent, then so are $\{H_t(f_1)(\mathbf{a}) + h(\mathbf{a}), H_t(f_2)(\mathbf{a}), \dots, H_t(f_k)(\mathbf{a})\}$.

Now suppose this is not the case. Then it must be the case that without loss of generality, some $h \in \mathcal{U}_t(\mathbf{f})$, $\mathsf{PSSJac}_t(\mathbf{f}, h)$ has full rank but for any $\mathbf{a} \in \mathcal{G}$,

$$\alpha_1(H_t(f_1)(\mathbf{a}) + h(\mathbf{a})) + \sum_{i=2}^{k} (\alpha_i \cdot H_t(f_i)(\mathbf{a})) = 0.$$

Here, not all of $\{\alpha_i\}_{i \in [k]}$ are zero. However by our hypothesis, this would mean that

$$\alpha_1(H_t(f_1) + h) + \sum_{i=2}^{k} (\alpha_i \cdot H_t(f_i)) \neq 0.$$

Let $\mathcal{B}$ be a basis of the rows in $H_t(\mathbf{f})$. Then each of $\{H_t(f_1) + h, H_t(f_2), \ldots, H_t(f_k)\}$ can be written in terms of rows in $\mathcal{B}$. Thus, the above statement can be rewritten as

$$\sum_{i=1}^{K'} \beta_i \cdot b_i = \alpha_1(H_t(f_1) + h) + \sum_{i=2}^{k} (\alpha_i \cdot H_t(f_i)) \neq 0$$

where $\{\beta_i\}_{i \in [K']}$ are some scalars and $K' = |\mathcal{B}|$.

This shows that not all $\{\beta_i\}_{i=1}^{K'}$ can be zero. Now since $\mathcal{G}$ is a hitting set generator for every $K' \times K'$ minor in $\mathsf{PSSJac}_t(\mathbf{f})$, there is some $\mathbf{a} \in \mathcal{G}$ such that $\{b_i(\mathbf{a})\}_{i \in [K']}$ continue to remain linearly independent. Thus, $\sum_{i=1}^{K'} \beta_i \times b_i(\mathbf{a})! = 0$, since not all $\{\beta_i\}_{i \in [K']}$ is zero. However, this shows that

$$\alpha_1(H_t(f_1)(\mathbf{a}) + h(\mathbf{a})) + \sum_{i=2}^{k} (\alpha_i \cdot H_t(f_i)(\mathbf{a})) = \sum_{i=1}^{K'} \beta_i \times b_i(\mathbf{a}) \neq 0.$$

This contradicts our assumption, and so it must be the case that for any $h \in \mathcal{U}_t(\mathbf{f})$, the rank of $\mathsf{PSSJac}_t(\mathbf{f}, h)$ is preserved. ◁

Thus, now it is only a question of finding a hitting set generator of low degree, for every $K' \times K'$ minor of $\mathsf{PSSJac}_t(\mathbf{f})$ where $K' \leq K$. The definitions of these generators for both cases are similar to those in [2] and the details can be found in the full version [4]. ◀

### 5.1 Applications to PIT

As stated in Subsection 1.1, using Lemma 1.2, we get two straightforward corollaries for PIT for related models (Corollary 1.6 and Corollary 1.7). As mentioned there, the results are incomparable with the PIT results of Pandey et al. [14] and Kumar and Saraf [11]. For the proof idea, the interested reader may look at the full version [4].

## 6 Conclusion and open problems

We studied the task of constructing faithful homomorphisms in the finite characteristic setting and extended the results of Agrawal et al. [2] in the setting when the inseparable degree is bounded. There are some very natural open problems in this context.

- Are the homomorphisms constructed in the paper also $\mathbb{F}(s)$-faithful homomorphisms?

  Our proof only provides a recipe towards constructing $\mathbb{F}$-faithful homomorphisms due to technical obstacles involving the criterion for algebraic independence over finite characteristic fields. This is not an issue in characteristic zero fields; Agrawal et al. [2] construct $\mathbb{F}(s)$-faithful homomorphisms.

- How crucial is the notion of inseparable degree in the context of testing algebraic independence?

  The criterion of Pandey, Saxena and Sinhababu [14] crucially depends on this field theoretic notion and there seems to be compelling algebraic reasons to believe that this is necessary. However, as mentioned earlier, Guo, Saxena and Sinhababu [7] showed that algebraic independence testing is in $\mathsf{AM} \cap \mathsf{coAM}$ and this proof has absolutely no dependence on the inseparable degree.

## References

1 Manindra Agrawal and Somenath Biswas. Primality and identity testing via Chinese remaindering. *J. ACM*, 50(4):429–443, 2003. doi:10.1145/792538.792540.

2 Manindra Agrawal, Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. Jacobian Hits Circuits: Hitting Sets, Lower Bounds for Depth-D Occur-k Formulas and Depth-3 Transcendence Degree-k Circuits. *SIAM J. Comput.*, 45(4):1533–1562, 2016. doi:10.1137/130910725.

3 Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Information and Computing*, 222:2–19, 2013. doi:10.1016/j.ic.2012.10.004.

4 Prerona Chatterjee and Ramprasad Saptharishi. Constructing Faithful Homomorphisms over Fields of Finite Characteristic. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:212, 2018. URL: https://eccc.weizmann.ac.il/report/2018/212.

5 Richard A. DeMillo and Richard J. Lipton. A Probabilistic Remark on Algebraic Program Testing. *Inf. Process. Lett.*, 7(4):193–195, 1978. doi:10.1016/0020-0190(78)90067-4.

6 Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. *Combinatorica*, 28(4):415–440, 2008. doi:10.1007/s00493-008-2259-3.

7 Zeyu Guo, Nitin Saxena, and Amit Sinhababu. Algebraic Dependencies and PSPACE Algorithms in Approximative Complexity. In Rocco A. Servedio, editor, *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*, volume 102 of *LIPIcs*, pages 10:1–10:21. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018. doi:10.4230/LIPIcs.CCC.2018.10.

8 C.G.J. Jacobi. De Determinantibus functionalibus. *Journal für die reine und angewandte Mathematik*, 22:319–359, 1841. URL: http://eudml.org/doc/147138.

9 Neeraj Kayal. The Complexity of the Annihilating Polynomial. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 184–193, 2009. doi:10.1109/CCC.2009.37.

10 Adam R. Klivans and Daniel A. Spielman. Randomness efficient identity testing of multivariate polynomials. In Jeffrey Scott Vitter, Paul G. Spirakis, and Mihalis Yannakakis, editors, *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*, pages 216–223. ACM, 2001. doi:10.1145/380752.380801.

11 Mrinal Kumar and Shubhangi Saraf. Arithmetic Circuits with Locally Low Algebraic Rank. *Theory of Computing*, 13(1):1–33, 2017. doi:10.4086/toc.2017.v013a006.

12 Øystein Ore. Über höhere kongruenzen. *Norsk Mat. Forenings Skrifter*, 1(7):15, 1922.

13 James G. Oxley. *Matroid theory.* Oxford University Press, 1992.

14 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, 2018. doi:10.1007/s00037-018-0167-5.

15 Jacob T. Schwartz. Fast Probabilistic Algorithms for Verification of Polynomial Identities. *J. ACM*, 27(4):701–717, 1980. doi:10.1145/322217.322225.

16 Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and Algebraic Computation, EUROSAM '79, An International Symposiumon Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, 1979. doi:10.1007/3-540-09519-5_73.