TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9947(XX)0000-0

ALGEBRAIC INDEPENDENCE IN POSITIVE CHARACTERISTIC – A p-ADIC CALCULUS

JOHANNES MITTMANN, NITIN SAXENA, AND PETER SCHEIBLECHNER

Abstract. A set of multivariate polynomials, over a field of zero or large characteristic, can be tested for algebraic independence by the well-known Jacobian criterion. For fields of other characteristic $p > 0$, no analogous characterization is known. In this paper we give the first such criterion. Essentially, it boils down to a non-degeneracy condition on a lift of the Jacobian polynomial over (an unramified extension of) the ring of p-adic integers.

Our proof builds on the functorial de Rham-Witt complex, which was invented by Illusie (1979) for crystalline cohomology computations, and we deduce a natural explicit generalization of the Jacobian. This new avatar we call the Witt-Jacobian. In essence, we show how to faithfully differentiate polynomials over $\mathbb{F}_p$ (i.e., somehow avoid $\partial x^p/\partial x = 0$) and thus capture algebraic independence.

We give two applications of this criterion in algebraic complexity theory.

Contents

1. Introduction

Polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n] =: k[\boldsymbol{x}]$ over a field k are called *algebraically independent*, if there is no non-zero polynomial $P \in k[y_1, \ldots, y_m]$ such that $P(f_1, \ldots, f_m) = 0$. Otherwise, they are called *algebraically dependent* and P an *annihilating polynomial*. Algebraic independence is a fundamental concept in commutative algebra. It is to polynomial rings what *linear* independence is to vector spaces. Our paper is motivated by the computational aspects of this concept.

2010 *Mathematics Subject Classification.* 12Y05, 13N05, 14F30, 03D15, 68Q17, 68W30.

Key words and phrases. algebraic independence, crystalline cohomology, de Rham, differential, finite field, Galois ring, identity testing, Jacobian, Kähler, p-adic, Teichmüller, Witt, zeta function.

A priori it is not clear whether one can test algebraic independence of given *explicit* polynomials *effectively*. But this is possible – by Gröbner bases using [KR00, Proposition 3.6.2], or by invoking Perron's degree bound on the annihilating polynomial [Per27, Pło05] and finding a possible P by linear algebra. Now, can this be done *efficiently* (i.e., in polynomial time)? It is known that computing Gröbner bases takes doubly exponential time, whereas the latter technique can be implemented in polynomial *space*, putting the problem in the class PSPACE ($\subseteq$ EXP). A different approach is needed for a faster algorithm, and this is where Jacobi enters [Jac41]. The *Jacobian* of the polynomials $\boldsymbol{f} := (f_1, \ldots, f_m)$ is the matrix $\mathcal{J}_{\boldsymbol{x}}(\boldsymbol{f}) := (\partial_{x_j} f_i)_{ij}$, where $\partial_{x_j} f_i = \partial f_i / \partial x_j$ is the partial derivative of f_i with respect to x_j. It is easy to see that for $m > n$ the $f_1, \ldots, f_m$ are dependent, so we assume $m \leq n$. Now, the Jacobian criterion says: The matrix is of *full* rank over the function field iff $f_1, \ldots, f_m$ are algebraically independent (assuming zero or large characteristic, see [BMS13]). Since the rank of this matrix can be computed by its *randomized* evaluations [Sch80], we immediately get a randomized polynomial time algorithm. Thus, independence testing over zero, or large characteristic, is in the class BPP. The only question left is – What about the 'other' prime characteristic fields? Formally,

Problem (Independence testing over $\mathbb{F}_p$). Given polynomials (or arithmetic circuits) $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ over a finite field k of characteristic $p > 0$, decide whether they are algebraically independent in randomized polynomial time (in the bit-size of the input).

Thus, independence testing problem is in PSPACE for any p, and even in BPP when p is sufficiently large. When p is small, compared to the degrees of the input polynomials, nothing like the Jacobian criterion was known (before our work). Here we propose the first such criterion that works for *all* prime characteristic. In this sense we make partial progress on the algebraic independence question for 'small fields' [DGW09], but we do not yet know how to check this criterion in randomized polynomial time. We do, however, improve the complexity of independence testing from PSPACE to $\mathrm{NP}^{\#\mathrm{P}}$. To compare these various classes, we remind the reader of the tower BPP $\subseteq \mathrm{NP}^{\#\mathrm{P}} \subseteq$ PSPACE $\subseteq$ EXP, and of the conjecture that all these containments are strict [AB09, Chapters 7 & 17]. We believe that independence testing sits right at the bottom of the tower (i.e. BPP). Our new criterion is a first step in that direction.

The $m \times m$ minors of the Jacobian we call *Jacobian polynomials*. So the criterion can be rephrased: One of the Jacobian polynomials is nonzero iff $f_1, \ldots, f_m$ are algebraically independent (assuming zero or large characteristic). We believe that finding a Jacobian-type polynomial that captures algebraic independence in any characteristic $p > 0$ is a natural question in algebra and geometry. Furthermore, Jacobian has recently found several applications in complexity theory – circuit lower bound proofs [Kal85, ASSS12], pseudo-random objects construction [DGW09, Dvi09], identity testing [BMS13, ASSS12], cryptography [DGRV11], program invariants [L'v84, Kay09], and control theory [For91, DF92]. Thus, a suitably effective Jacobian-type criterion is desirable to make these applications work for any field. The criterion presented here is not yet effective enough, nevertheless, it is able to solve a modest case of identity testing that was left open in [BMS13].

In this paper, the new avatar of the Jacobian polynomial is called a *Witt-Jacobian*. For simplicity, say $k = \mathbb{F}_p$ and $m = n$. So for polynomials $f_1, \ldots, f_n \in$

$\mathbb{F}_p[\boldsymbol{x}]$ we lift the coefficients of f_i to the *p-adic integers* $\widehat{\mathbb{Z}}_p$ to get the *lifted* polynomials $\widehat{f_i} \in \widehat{\mathbb{Z}}_p[\boldsymbol{x}]$. Now, for $\ell \geq 1$, the ℓ-th Witt-Jacobian polynomial of $\widehat{\boldsymbol{f}} := (\widehat{f_1}, \ldots, \widehat{f_n})$ is $\mathrm{WJP}_\ell(\widehat{\boldsymbol{f}}) := (\widehat{f_1} \cdots \widehat{f_n})^{p^{\ell-1}-1}(x_1 \cdots x_n) \cdot \det \mathcal{J}_{\boldsymbol{x}}(\widehat{\boldsymbol{f}})$. Hence, the Witt-Jacobian is just a suitably 'scaled-up' version of the Jacobian polynomial over the integral domain $\widehat{\mathbb{Z}}_p$. E.g., if $n = 1$, $f_1 = x_1^p$, then $\mathrm{WJP}_\ell(\widehat{f_1}) = (x_1^p)^{p^{\ell-1}-1} x_1 \cdot p x_1^{p-1} = p x_1^{p^\ell}$ which is a nonzero p-adic polynomial. Thus, Witt-Jacobian avoids mapping x_1^p to zero. However, the flip side is that a lift of the polynomial $f_1 = 0$, say, $\widehat{f_1} = p x_1^p$ gets mapped to $\mathrm{WJP}_\ell(\widehat{f_1}) = (p x_1^p)^{p^{\ell-1}-1} x_1 \cdot p^2 x_1^{p-1} = p^{(p^{\ell-1}+1)} x_1^{p^\ell}$ which is also a nonzero p-adic polynomial. This shows that a Witt-Jacobian criterion cannot simply hinge on the zeroness of WJP_ℓ but has to be much more subtle. Indeed, we show that the terms of WJP_ℓ carry *precise* information about the algebraic independence of $f_1, \ldots, f_m$. In particular, in the two examples above, our Witt-Jacobian criterion checks whether the coefficient of the monomial $x_1^{p^\ell}$ in WJP_ℓ is divisible by p^ℓ (which is true in the second example, but not in the first for $\ell \geq 2$). It is the magic of abstract *differentials* that such a weird explicit property could be formulated at all, let alone proved.

1.1. **A brief p-adic history.** The idea of lifting polynomials over a finite field to an extension of the p-adic numbers is classical in algebraic geometry and number theory. Highlights are clearly the proofs of the rationality of the zeta-function of a variety defined over a finite field [Dwo60], and of some of the other Weil conjectures [Lub68]. Since the zeta-function involves integral coefficients, it can be studied both modulo p and modulo $\ell \neq p$. From a computational viewpoint, the p-adic methods have been more useful than the ℓ-adic methods (though the latter are crucial in the full proof of Weil conjectures [Gro65, Del74, Del80]). Certain point-counting algorithms also employ this idea. Those algorithms, in particular, p-adically compute the zeta-function of the common zero set of given polynomials over a finite field. This was done for elliptic curves [Sat00], hyperelliptic curves [Ked01], superelliptic curves [GG01], C_{ab} curves [DV06], smooth projective hypersurfaces [Ger07], and nondegenerate curves [CDV06], before Lauder and Wan found an algorithm for arbitrary affine varieties [LW08]. Their algorithm works in exponential time in the number of variables, and is likely to require PSPACE, as the zeta-function can have an exponential degree, so it is inapplicable in our context.

While it is true that the dimension of an affine domain equals its transcendence degree over k, the problem of computing the dimension of the variety $V := \{\boldsymbol{a} \in \overline{k}^n \mid f_1(\boldsymbol{a}) = \cdots = f_m(\boldsymbol{a}) = 0\}$ seems harder than testing the defining polynomials $f_1, \ldots, f_m$ for algebraic independence. The point is that the former question concerns the algebra $k[\boldsymbol{x}]/(\boldsymbol{f})$, whereas the latter asks about the dimension of $k[f_1, \ldots, f_m] = k[\boldsymbol{f}]$, which is the coordinate ring of the Zariski closure of the image of the morphism $\overline{k}^n \to \overline{k}^m$, $\boldsymbol{x} \mapsto \boldsymbol{f}(\boldsymbol{x})$. For instance, the sets $\{x_1\}$ and $\{x_1, x_1x_2\}$ define the same variety, but their transcendence degrees are different. Since the zeta-function is an invariant of V and carries e.g. its dimension, it cannot "know" the transcendence degree of $\{f_1, \ldots, f_m\}$, since this is not an invariant of V. Furthermore, there is no general relationship between the dimension of $k[\boldsymbol{f}]$ and the dimension of V. In the case $V \neq \emptyset$ at least we have $n - \dim V \leq \dim k[\boldsymbol{f}]$. But this inequality is proper in general, as the above example $n = 2, f_1 = x_1, f_2 = x_1x_2$

shows. Moreover, if the f_i have no common zero, it trivially fails due to the convention $\dim \emptyset = -1$ (We note that this remains true with any other convention for $\dim \emptyset$, take e.g. $f_1 = x_1, f_2 = x_1 + 1$ and various $n > 1$).

Since independence testing is unrelated to the zeta-function computation, it is also unclear whether ℓ-adic methods could have any role in our context. In this paper p-adic methods do play a role, but not zeta-functions. Our *explicit* p-adic calculus builds on the *functorial* de Rham-Witt complex [Ill79]. To our knowledge this is the first application of the de Rham-Witt techniques to a concrete computational problem.

1.2. **Main results.** We need some notation to properly state our results. Denote $\mathbb{Z}_{\geq 0}$ by $\mathbb{N}$. Let $[n] := \{1, \dots, n\}$, and let the set of all m-subsets of $[n]$ be denoted by $\binom{[n]}{m}$. Bold letters will always denote vectors, such as $\boldsymbol{x} = (x_1, \dots, x_n)$ for the variables. If $I \in \binom{[n]}{m}$ and $\boldsymbol{a} = (a_1, \dots, a_n)$, the notation $\boldsymbol{a}_I$ will be a short-hand for the m-vector $(a_i)_{i \in I}$. Let $k/\mathbb{F}_p$ be an algebraic field extension and $\mathrm{W}(k)$ its ring of Witt vectors. This ring is just a 'nice' extension of $\widehat{\mathbb{Z}}_p$, e.g., $\mathrm{W}(\mathbb{F}_p) = \widehat{\mathbb{Z}}_p$. Define the $\mathbb{F}_p$-algebra $A := k[\boldsymbol{x}]$ and the p-adic-algebra $B := \mathrm{W}(k)[\boldsymbol{x}]$.

For a nonzero $\boldsymbol{\alpha} \in \mathbb{N}^n$ denote by $v_p(\boldsymbol{\alpha})$ the maximal $v \in \mathbb{N}$ with $p^v | \alpha_i$ for all $i \in [n]$. Set $v_p(\mathbf{0}) := \infty$. We call $f \in B$ *degenerate* if the coefficient of $\boldsymbol{x}^{\boldsymbol{\alpha}}$ in f is divisible by $p^{v_p(\boldsymbol{\alpha})+1}$ for all $\boldsymbol{\alpha} \in \mathbb{N}^n$. For $\ell \in \mathbb{N}$, f is called $(\ell+1)$-*degenerate* if the coefficient of $\boldsymbol{x}^{\boldsymbol{\alpha}}$ in f is divisible by $p^{\min\{v_p(\boldsymbol{\alpha}), \ell\}+1}$ for all $\boldsymbol{\alpha} \in \mathbb{N}^n$.

We could show for algebraically dependent polynomials $f_1, \dots, f_m \in A$ and their p-adic lifts $g_1, \dots, g_m \in B$, that for any m variables $\boldsymbol{x}_I$, $I \in \binom{[n]}{m}$, the p-adic polynomial $\left(\prod_{j \in I} x_j\right) \cdot \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{g})$ is degenerate. This would have been a rather elegant criterion, if the converse did not fail (see Theorem 36). It turns out that we need to look at a more complicated polynomial (and use the graded version of degeneracy).

Let $\ell \in \mathbb{N}$, $\boldsymbol{g} = (g_1, \dots, g_m) \in B^m$, and $I \in \binom{[n]}{m}$. We call

$$\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g}) := (g_1 \cdots g_m)^{p^\ell - 1} \left(\prod_{j \in I} x_j\right) \cdot \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{g}) \in B$$

the $(\ell+1)$-*th Witt-Jacobian polynomial of* $\boldsymbol{g}$ *with respect to* I.

Theorem 1 (Witt-Jacobian criterion)**.** *Let $f_1, \dots, f_m \in A$ with f_i of degree at most $\delta_i \geq 1$, and fix $\ell \geq \lfloor \sum_i \log_p \delta_i \rfloor$. Choose $g_1, \dots, g_m \in B$ such that $f_i \equiv g_i \pmod{pB}$ for all $i \in [m]$. Then $f_1, \dots, f_m$ are algebraically independent over k if and only if there exists $I \in \binom{[n]}{m}$ such that $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g})$ is not $(\ell+1)$-degenerate, where $\boldsymbol{g} = (g_1, \dots, g_m)$.*

If $p > \delta_1 \cdots \delta_m$, this theorem subsumes the Jacobian criterion (choose $\ell = 0$). In computational situations we are given $f_1, \dots, f_m \in A$, say, in sparse encoding. Of course, we can efficiently lift them to $g_1, \dots, g_m \in B$. But $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g})$ may have *exponential* sparsity (number of nonzero monomials), even for $\ell = 1$. This makes it difficult to test the Witt-Jacobian polynomial efficiently even for 2-degeneracy. While we improve the basic upper bound of PSPACE for the problem of testing algebraic independence, there is some evidence that the *general* ℓ-degeneracy problem is outside the polynomial hierarchy [Men12] (Theorem 39).

Theorem 2 (Upper bound)**.** *The problem of testing algebraic independence of polynomials given by arithmetic circuits $C_1, \dots, C_m$ is in the class* $\mathrm{NP}^{\#\mathrm{P}}$.

We are in a better shape when $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g})$ is relatively sparse, which happens, for instance, when the f_i have 'sub-logarithmic' sparsity. This case can be applied to the question of *blackbox identity testing*: We are given an arithmetic circuit $C \in \mathbb{F}_p[\boldsymbol{x}]$ via a blackbox, and we need to decide whether $C = 0$. Blackbox access means that we can only evaluate C over field extensions of $\mathbb{F}_p$. Hence, blackbox identity testing boils down to efficiently constructing a *hitting-set* $\mathcal{H} \subset \overline{\mathbb{F}}_p^n$ such that any nonzero C (in our circuit family) has an $\boldsymbol{a} \in \mathcal{H}$ with $C(\boldsymbol{a}) \neq 0$. Designing efficient hitting-sets is an outstanding open problem in complexity theory; with close connections to circuit lower bounds and the algebraic version of NP vs. P question. See [SS95, Sax09, SY10, Mul11, ASSS12] and the references therein. We apply the Witt-Jacobian criterion to the following case of identity testing.

Theorem 3 (Hitting-set)**.** *Let $f_1, \ldots, f_m \in A$ be s-sparse polynomials of degree $\leq \delta$, transcendence degree $\leq r$, and assume $s, \delta, r \geq 1$. Let $C \in k[y_1, \ldots, y_m]$ such that the degree of $C(\boldsymbol{f})$ is bounded by d. We can construct a (hitting-)set $\mathcal{H} \subset \overline{\mathbb{F}}_p^n$ in time $\mathrm{poly}\big((nd)^r, (\delta r s)^{r^2 s}\big)$ such that*

$$C(\boldsymbol{f}) \neq 0 \quad \Longrightarrow \quad \exists \boldsymbol{a} \in \mathcal{H},\ \big(C(\boldsymbol{f})\big)(\boldsymbol{a}) \neq 0.$$

An interesting parameter setting is $r = O(1)$ and $s = O(\frac{\log d}{r^2 \log(\delta r \log d)})$. In other words, we have an efficient hitting-set, when $f_1, \ldots, f_m$ have constant transcendence degree and sub-logarithmic sparsity. This is new, though, for zero and large characteristic, a much better result is in [BMS13] (thanks to the classical Jacobian).

1.3. **Our approach.** Here we sketch the ideas for proving Theorem 1, without going into the definitions and technicalities (those come later in plenty). The central tool in the proof is the *de Rham-Witt complex* which was invented by Illusie, for $\mathbb{F}_p$-ringed topoi, in the seminal work [Ill79]. While it is fundamental for several cohomology theories for schemes in characteristic $p > 0$ (see the beautiful survey [Ill94]), we focus here on its algebraic strengths only. We will see that it is just the right machinery, though quite heavy, to churn a criterion. We lift a polynomial $f \in A$ to a more 'geometric' ring $\mathrm{W}(A)$, via the *Teichmüller lift* $[f]$. This process is the same functor that builds $\widehat{\mathbb{Z}}_p$ from $\mathbb{F}_p$ [Ser79]. The formalization of differentiation in this ring is by the $\mathrm{W}(A)$-module of *Kähler differentials* $\Omega^1_{\mathrm{W}(A)}$ [Eis95]. Together with its *exterior powers* it provides a fully-fledged linear algebra structure, the *de Rham complex* $\Omega^\bullet_{\mathrm{W}(A)}$. But this is all in zero characteristic and we have to do more to correctly extract the properties of A – which has characteristic p.

The ring $\mathrm{W}(A)$ admits a natural *filtration* by ideals $\mathrm{V}^\ell \mathrm{W}(A) \supseteq p^\ell \mathrm{W}(A)$, so we have *length-$\ell$ Witt vectors* $\mathrm{W}_\ell(A) := \mathrm{W}(A)/\mathrm{V}^\ell \mathrm{W}(A)$. This filtration is inherited by $\Omega^\bullet_{\mathrm{W}(A)}$, and a suitable quotient defines the *de Rham-Witt complex* $\mathrm{W}_\ell \Omega^\bullet_A$ of $\mathrm{W}_\ell(A)$-modules, and the *de Rham-Witt pro-complex* $\mathrm{W}_\bullet \Omega^\bullet_A$. This is still an abstractly defined object, but it can be explicitly realized as a subspace of the algebra $B' := \cup_{i \geq 0} \mathrm{W}(k)[\boldsymbol{x}_n^{p^{-i}}]$ (a *perfection* of B). Illusie defined a subalgebra $\mathrm{E}^0 \subset B'$ that is 'almost' isomorphic to $\mathrm{W}(A)$, and could then identify a *differential graded algebra* $\mathrm{E} \subset \Omega^\bullet_{B'}$ such that a suitable quotient $\mathrm{E}_\ell := \mathrm{E} \,/\, \mathrm{Fil}^\ell \mathrm{E}$ realizes $\mathrm{W}_\ell \Omega^\bullet_A$.

To prove Theorem 1 we consider the *Witt-Jacobian differential* $\mathrm{WJ}_\ell(\boldsymbol{f}) := d[f_1] \wedge \cdots \wedge d[f_m] \in \mathrm{W}_\ell \Omega^m_A$. By studying the behavior of $\mathrm{W}_\ell \Omega^m_A$ as we move from A to an extension ring, we show that $\mathrm{WJ}_\ell(\boldsymbol{f})$ vanishes iff $f_1, \ldots, f_m$ are algebraically dependent. The concept of *étale* extension is really useful here [Mil80]. In our

situation, it corresponds to a *separable* field extension. We try to 'force' separability, and here the Perron-like Theorem 4 helps to bound ℓ. Next, we realize $\mathrm{WJ}_\ell(\boldsymbol{f})$ as an element of E_ℓ^m. This is where the *Witt-Jacobian polynomials* $\mathrm{WJP}_{\ell,I}(\boldsymbol{g})$ appear and satisfy: $\mathrm{WJ}_\ell(\boldsymbol{f}) = 0$ iff its explicit version is in $\mathrm{Fil}^\ell \mathrm{E}^m$ iff $\mathrm{WJP}_{\ell,I}(\boldsymbol{g})$ is ℓ-degenerate for all I.

The idea in Theorem 2 is that, by the Witt-Jacobian criterion, the given polynomials are algebraically independent iff some $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g})$ has some monomial $\boldsymbol{x}^{\boldsymbol{\alpha}}$ whose coefficient is *not* divisible by $p^{\min\{v_p(\boldsymbol{\alpha}),\ell\}+1}$. An NP machine can 'guess' I and $\boldsymbol{\alpha}$, while computing the coefficient is harder. We do the latter following an idea of [KS11] by evaluating the exponentially large sum in an interpolation formula using a #P-oracle. In this part the isomorphism between truncated Witt vectors $\mathrm{W}_{\ell+1}(\mathbb{F}_{p^t})$ and the handier *Galois ring* $G_{\ell+1,t}$ [Rag69, Wan03] allows to evaluate $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g})$.

The main idea in Theorem 3 is that non-ℓ-degeneracy of $\mathrm{WJP}_{\ell,I}(\boldsymbol{g})$ is preserved under evaluation of the variables $\boldsymbol{x}_{[n]\setminus I}$. This implies with [BMS13] that algebraically independent $f_1, \dots, f_r$ can be made r-variate efficiently without affecting the zeroness of $C(\boldsymbol{f})$. The existence of the claimed hitting-sets follows easily from [Sch80].

1.4. **Organization.** In §2 we introduce all necessary prerequisites about algebraic independence and transcendence degree (§2.1), derivations, differentials and the de Rham complex (§2.2), separability (§2.3), the ring of Witt vectors (§2.4), and the de Rham-Witt complex (§2.5 and §2.6). To warm up the concept of differentials, we discuss the classical Jacobian criterion in a 'modern' language in §3.

Our main results are contained in §4. In §4.1 we define the Witt-Jacobian differential and prove the abstract Witt-Jacobian criterion, and in §4.2 we derive its explicit version. The necessary condition, on the p-adic Jacobian, for algebraic dependence is proved in §4.3. In §5 we discuss the computational problem of testing algebraic independence. The proof of the upper bound for this problem is contained in §5.1, and the lower bound for testing degeneracy is given in §5.2. Finally, in §6 we give the efficient hitting-set construction of Theorem 3.

2. Preliminaries

Unless stated otherwise, a ring in this paper is commutative with unity. For integers $m \le n$, we write $[m, n] := \{m, m+1, \dots, n\}$.

2.1. **Algebraic independence and transcendence degree.** Let k be a field and let A be a k-algebra. Elements $a_1, \dots, a_m \in A$ are called *algebraically independent over* k if $P(a_1, \dots, a_m) \neq 0$ for all nonzero polynomials $P \in k[y_1, \dots, y_m]$. For a subset $S \subseteq A$, the *transcendence degree of* S *over* k is defined as

$$\mathrm{trdeg}_k(S) := \sup\{\#T \mid T \subseteq S \text{ finite and algebraically independent over } k\}.$$

If A is an integral domain, then $\mathrm{trdeg}_k(A) = \mathrm{trdeg}_k(Q(A))$, where $Q(A)$ denotes the quotient field of A.

Now let $k[\boldsymbol{x}] = k[x_1, \dots, x_n]$ be a polynomial ring over k. It is well-known that $\mathrm{trdeg}_k\, k[\boldsymbol{x}] = n$. Consequently, for n algebraically independent polynomials $f_1, \dots, f_n \in k[\boldsymbol{x}]$, the field extension $k(\boldsymbol{x})/k(\boldsymbol{f})$ is finite, where $\boldsymbol{f} = (f_1, \dots, f_n)$. The Bézout-like theorem [Kem96, Corollary 1.8] implies an effective bound on the degree of this field extension, which is stronger than Perron's classical bound [Per27].

Theorem 4 (Degree bound)**.** *Let k be a field, $f_1, \dots, f_n \in k[x_1, \dots, x_n] = k[\boldsymbol{x}]$ be algebraically independent, and set $\delta_i := \deg(f_i)$ for $i \in [n]$. Then*

$$[k(\boldsymbol{x}) : k(\boldsymbol{f})] \leq \delta_1 \cdots \delta_n.$$

Proof. Define for each $i \in [n]$ the *homogenization* $F_i := z^{\delta_i} \cdot f_i(\boldsymbol{x}/z) \in k[z, \boldsymbol{x}]$ of f_i with respect to degree δ_i. As usual denote $\boldsymbol{F} := (F_1, \dots, F_n)$.

Firstly, $z, \boldsymbol{F}$ are algebraically independent over k. For otherwise, there is an irreducible polynomial $P \in k[y_0, \dots, y_n]$ such that $P(z, \boldsymbol{F}) = 0$. Evaluation at $z = 1$ yields $P(1, \boldsymbol{f}) = 0$. The algebraic independence of $\boldsymbol{f}$ implies $P(1, y_1, \dots, y_n) = 0$, hence $(y_0 - 1)$ divides P, which contradicts the irreducibility of P.

Thus, $d' := [k(z, \boldsymbol{x}) : k(z, \boldsymbol{F})]$ is finite. We will now compare it with $[k(\boldsymbol{x}) : k(\boldsymbol{f})] =: d$. The vector space $k(\boldsymbol{x})$ over $k(\boldsymbol{f})$ admits a finite basis consisting of monomials in $\boldsymbol{x}$ only. Let $S = \{\boldsymbol{x}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in I\}$ for some $I \subset \mathbb{N}^n$ be such a basis. We show that S is also linearly independent in the vector space $k(z, \boldsymbol{x})$ over $k(z, \boldsymbol{F})$. Assume

$$\sum_{\boldsymbol{\alpha} \in I} h_{\boldsymbol{\alpha}}(z, \boldsymbol{F}) \cdot \boldsymbol{x}^{\boldsymbol{\alpha}} = 0, \quad \text{where} \quad h_{\boldsymbol{\alpha}}(z, \boldsymbol{F}) \in k[z, \boldsymbol{F}]. \tag{2.1}$$

By separating the homogeneous parts, we can assume that all summands in the left hand side of (2.1) are homogeneous of the same degree. Since the F_i are homogeneous, this process yields again polynomials in $\boldsymbol{F}$. By evaluating (2.1) at $z = 1$ we get

$$\sum_{\boldsymbol{\alpha} \in I} h_{\boldsymbol{\alpha}}(1, \boldsymbol{f}) \cdot \boldsymbol{x}^{\alpha} = 0.$$

From the linear independence of the $x^{\boldsymbol{\alpha}}$ over $k(\boldsymbol{f})$ we conclude $h_{\boldsymbol{\alpha}}(1, \boldsymbol{f}) = 0$ for all $\boldsymbol{\alpha} \in I$. Since the $h_{\boldsymbol{\alpha}}(z, \boldsymbol{F})$ are homogeneous, they cannot be divisible by $z - 1$, unless they vanish. Hence, $d \leq d'$.

In fact we have $d = d'$, but we don't need this here. Finally, we complete the proof by noting that [Kem96, Corollary 1.8] implies $d' \leq \delta_1 \cdots \delta_n$. □

2.2. **Differentials and the de Rham complex.** Let R be a ring and let A be an R-algebra. The *module of Kähler differentials* of A over R, denoted by $\Omega^1_{A/R}$, is the A-module generated by the set of symbols $\{da \mid a \in A\}$ subject to the relations

$$\begin{aligned} d(ra + sb) &= r\,da + s\,db \quad (R\text{-linearity}), \\ d(ab) &= a\,db + b\,da \quad (\text{Leibniz rule}) \end{aligned}$$

for all $r, s \in R$ and $a, b \in A$. The map $d\colon A \to \Omega^1_{A/R}$ defined by $a \mapsto da$ is an R-derivation called the *universal R-derivation* of A.

For $m \geq 0$, let $\Omega^m_{A/R} := \bigwedge^m \Omega^1_{A/R}$ be the m-th exterior power over A. The universal derivation $d\colon A = \Omega^0_{A/R} \to \Omega^1_{A/R}$ extends to the *exterior derivative* $d^m\colon \Omega^m_{A/R} \to \Omega^{m+1}_{A/R}$ by $d^m(a\,da_1 \wedge \cdots \wedge da_m) = da \wedge da_1 \wedge \cdots \wedge da_m$ for $a, a_1, \dots, a_m \in A$. It satisfies $d^{m+1} \circ d^m = 0$ and hence defines a complex of R-modules

$$\Omega^\bullet_{A/R}\colon \quad 0 \to A \xrightarrow{d} \Omega^1_{A/R} \xrightarrow{d^1} \cdots \to \Omega^m_{A/R} \xrightarrow{d^m} \Omega^{m+1}_{A/R} \to \cdots$$

called the *de Rham complex* of A over R. The exterior product also defines an A-algebra structure on this complex. The Kähler differentials satisfy the following properties, which make it convenient to study algebra extensions.

Lemma 5 (Base change)**.** *Let R be a ring, let A and R' be R-algebras. Then $A' := R' \otimes_R A$ is an R'-algebra, and for all $m \geq 0$ there is an A'-module isomorphism*

$$R' \otimes_R \Omega^m_{A/R} \xrightarrow{\sim} \Omega^m_{A'/R'}$$

given by $a' \otimes (da_1 \wedge \cdots \wedge da_m) \mapsto (a' \otimes 1)\, d(1 \otimes a_1) \wedge \cdots \wedge d(1 \otimes a_m)$.

Lemma 6 (Localization)**.** *Let R be a ring, let A be an R-algebra and let $B = S^{-1}A$ for some multiplicatively closed set $S \subset A$. Then for all $m \geq 0$ there is a B-module isomorphism*

$$B \otimes_A \Omega^m_{A/R} \xrightarrow{\sim} \Omega^m_{B/R}$$

given by $b \otimes (da_1 \wedge \cdots \wedge da_m) \mapsto b\, da_1 \wedge \cdots \wedge da_m$. The universal R-derivation $d\colon B \to \Omega^1_{B/R}$ satisfies $d(s^{-1}) = -s^{-2}\, ds$ for $s \in S$.

For $m = 1$ these lemmas are proved in [Eis95] as Propositions 16.4 and 16.9, respectively, and for $m \geq 2$ they follow from [Eis95, Proposition A2.2 b].

The Jacobian emerges quite naturally in this setting.

Definition 7. Let $\boldsymbol{a} = (a_1, \ldots, a_m) \in A^m$. We call

$$\mathrm{J}_{A/R}(\boldsymbol{a}) := da_1 \wedge \cdots \wedge da_m \in \Omega^m_{A/R}$$

the *Jacobian differential of* $\boldsymbol{a}$.

Now consider the polynomial ring $A = k[\boldsymbol{x}]$ over a field k. Then $\Omega^1_{k[\boldsymbol{x}]/k}$ is the free $k[\boldsymbol{x}]$-module of rank n with basis $dx_1, \ldots, dx_n$. It follows that $\Omega^m_{k[\boldsymbol{x}]/k} = 0$ for $m > n$. For $m \leq n$ and $I = \{j_1 < \cdots < j_m\} \in \binom{[n]}{m}$ we use the notation $\bigwedge_{j \in I} dx_j := dx_{j_1} \wedge \cdots \wedge dx_{j_m}$. The $k[\boldsymbol{x}]$-module $\Omega^m_{k[\boldsymbol{x}]/k}$ is free of rank $\binom{n}{m}$ with basis $\left\{\bigwedge_{j \in I} dx_j \mid I \in \binom{[n]}{m}\right\}$. The universal derivation $d\colon k[\boldsymbol{x}] \to \Omega^1_{k[\boldsymbol{x}]/k}$ is given by $f \mapsto \sum_{i=1}^n (\partial_{x_i} f) dx_i$.

Recall that the *Jacobian matrix* of $\boldsymbol{f} \in k[\boldsymbol{x}]^m$ is defined as $\mathcal{J}_{\boldsymbol{x}}(\boldsymbol{f}) := (\partial_{x_j} f_i)_{i,j} \in k[\boldsymbol{x}]^{m \times n}$. Furthermore, for an index set $I = \{j_1 < \cdots < j_r\} \in \binom{[n]}{r}$, we write $\boldsymbol{x}_I = (x_{j_1}, \ldots, x_{j_r})$ and $\mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{f}) = (\partial_{x_{j_k}} f_i)_{i,k} \in k[\boldsymbol{x}]^{m \times r}$. A standard computation shows

$$df_1 \wedge \cdots \wedge df_m = \sum_I \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{f}) \cdot \bigwedge_{j \in I} dx_j,$$

where the sum runs over all $I \in \binom{[n]}{m}$, which implies the following relationship between the Jacobian differential and the rank of the Jacobian matrix.

Lemma 8. *For $\boldsymbol{f} \in k[\boldsymbol{x}]^m$ we have*

$$\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}) \neq 0 \iff \mathrm{rk}_{k(\boldsymbol{x})}\, \mathcal{J}_{\boldsymbol{x}}(\boldsymbol{f}) = m.$$

2.3. **Separability.** A univariate polynomial $f \in k[x]$ is called *separable* if it has no multiple roots in $\overline{k}$. If f is irreducible, then it is separable if and only if $\partial_x f \neq 0$, which is always the case in characteristic zero. If $\mathrm{char}(k) = p > 0$, then f is separable if and only if $f \notin k[x^p]$. Now let L/k be a field extension. An algebraic element $a \in L$ over k is called *separable* if its minimal polynomial in $k[x]$ is separable. The separable elements form a field $k \subseteq k_{\mathrm{sep}} \subseteq L$ which is called the *separable closure* of k in L. Now let L/k be an algebraic extension. Then $[L : k]_{\mathrm{sep}} := [k_{\mathrm{sep}} : k]$ and $[L : k]_{\mathrm{insep}} := [L : k_{\mathrm{sep}}]$ are called the *separable* and *inseparable degree* of L/k, respectively. If $L = k_{\mathrm{sep}}$, then L/k is called *separable*. The extension L/k_{sep} is *purely inseparable*, i.e., for all $a \in L$ we have $a^{p^e} \in k_{\mathrm{sep}}$ for some $e \geq 0$.

More generally, a finitely generated extension L/k is *separable* if it has a transcendence basis $B \subset L$ such that the finite extension $L/k(B)$ is separable. In this case, B is called a *separating transcendence basis* of L/k. If L/k is separable, then every generating system of L over k contains a separating transcendence basis. If k is perfect, then every finitely generated field extension of k is separable [Lan84, §X.6].

Lemma 16.15 in [Eis95] implies that a separable field extension adds no new linear relations in the differential module, and Proposition A2.2 b [loc.cit.] yields

Lemma 9 (Separable extension)**.** *Let L/k be a separable algebraic field extension and let R be a subring of k. Then for all $m \geq 0$ there is an L-vector space isomorphism*

$$L \otimes_k \Omega^m_{k/R} \xrightarrow{\sim} \Omega^m_{L/R}$$

given by $b \otimes (da_1 \wedge \cdots \wedge da_r) \mapsto b\, da_1 \wedge \cdots \wedge da_r$.

2.4. **The ring of Witt vectors.** The Witt ring was defined in [Wit36]. For its precise definition and basic properties we also refer to [Lan84, Ser79, Haz78].

Fix a prime p and a ring A. As a set, the *ring* $\mathrm{W}(A)$ *of (p-typical) Witt vectors* of A (or *Witt ring* for short) is defined as $A^{\mathbb{N}}$. An element $a \in \mathrm{W}(A)$ is written $(a_0, a_1, \dots)$ and is called a *Witt vector* with *coordinates* $a_i \in A$. The ring structure of $\mathrm{W}(A)$ is given by universal polynomials $S_i, P_i \in \mathbb{Z}[x_0, \dots, x_i, y_0, \dots, y_i]$ such that

$$\begin{aligned} a + b &= (S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), \dots), \\ ab &= (P_0(a_0, b_0), P_1(a_0, a_1, b_0, b_1), \dots) \end{aligned}$$

for all $a, b \in \mathrm{W}(A)$. The first few terms are

$$\begin{aligned} S_0 &= x_0 + y_0, & S_1 &= x_1 + y_1 - \sum_{i=1}^{p-1} p^{-1} \tbinom{p}{i} x_0^i y_0^{p-i}, \\ P_0 &= x_0 y_0, & P_1 &= x_0^p y_1 + x_1 y_0^p + p x_1 y_1. \end{aligned}$$

The additive and multiplicative identity elements of $\mathrm{W}(A)$ are $(0, 0, 0, \dots)$ and $(1, 0, 0, \dots)$, respectively. The ring structure is uniquely determined by a universal property, which we refrain from stating. If p is invertible in A, then $\mathrm{W}(A)$ is isomorphic to $A^{\mathbb{N}}$ with componentwise operations.

The projection $\mathrm{W}_\ell(A)$ of $\mathrm{W}(A)$ to the first $\ell \geq 1$ coordinates is a ring with the same rules for addition and multiplication as for $\mathrm{W}(A)$, which is called the *ring of Witt vectors of A of length ℓ*. We have $\mathrm{W}_1(A) = A$. The ring epimorphisms

$$\mathrm{R}\colon \mathrm{W}_{\ell+1}(A) \to \mathrm{W}_\ell(A), \qquad (a_0, \dots, a_\ell) \mapsto (a_0, \dots, a_{\ell-1})$$

are called *restriction*, and $((\mathrm{W}_\ell(A))_{\ell \geq 1}, \mathrm{R}\colon \mathrm{W}_{\ell+1}(A) \to \mathrm{W}_\ell(A))$ is a projective (inverse) system of rings with limit $\mathrm{W}(A)$. The additive group homomorphism

$$\mathrm{V}\colon \mathrm{W}(A) \to \mathrm{W}(A), \qquad (a_0, a_1, \dots) \mapsto (0, a_0, a_1, \dots)$$

is called *Verschiebung* (shift). For $\ell, r \geq 1$, we have exact sequences

$$\begin{aligned} 0 \to \mathrm{W}(A) \xrightarrow{\mathrm{V}^\ell} \mathrm{W}(A) \to \mathrm{W}_\ell(A) \to 0, \\ 0 \to \mathrm{W}_r(A) \xrightarrow{\mathrm{V}^\ell} \mathrm{W}_{\ell+r}(A) \xrightarrow{\mathrm{R}^r} \mathrm{W}_\ell(A) \to 0. \end{aligned}$$

The Verschiebung also induces additive maps $\mathrm{V}\colon \mathrm{W}_\ell(A) \to \mathrm{W}_{\ell+1}(A)$.

The *Teichmüller lift* of $a \in A$ is defined as $[a] := (a, 0, 0, \dots) \in \mathrm{W}(A)$. The image of $[a]$ in $\mathrm{W}_\ell(A)$ is denoted by $[a]_{\le \ell}$. We have

$$[a] \cdot w = \big(aw_0, a^p w_1, \dots, a^{p^i} w_i, \dots\big)$$

for all $w \in \mathrm{W}(A)$. In particular, the map $A \to \mathrm{W}(A)$, $a \mapsto [a]$ is multiplicative, i.e., $[ab] = [a][b]$ for all $a, b \in A$. Every $a \in \mathrm{W}(A)$ can be written as $a = \sum_{i=0}^{\infty} \mathrm{V}^i[a_i]$.

We are only interested in the case where A has characteristic p. The most basic example is the prime field $A = \mathbb{F}_p$, for which $\mathrm{W}(\mathbb{F}_p)$ is the ring $\widehat{\mathbb{Z}}_p$ of p-adic integers. More generally, the Witt ring $\mathrm{W}(\mathbb{F}_{p^t})$ of a finite field $\mathbb{F}_{p^t}$ is the ring of integers $\widehat{\mathbb{Z}}_p^{(t)}$ in the unique unramified extension $\mathbb{Q}_p^{(t)}$ of $\mathbb{Q}_p$ of degree t [Kob84, III.3].

Now let A be an $\mathbb{F}_p$-algebra. Then the *Frobenius endomorphism* $\mathrm{F}\colon A \to A$, $a \mapsto a^p$ induces a ring endomorphism

$$\mathrm{F}\colon \mathrm{W}(A) \to \mathrm{W}(A), \qquad (a_0, a_1, \dots) \mapsto (a_0^p, a_1^p, \dots). \tag{2.2}$$

We have $\mathrm{V}\,\mathrm{F} = \mathrm{F}\,\mathrm{V} = p$ and $a\,\mathrm{V}\,b = \mathrm{V}(\mathrm{F}\,a \cdot b)$ for all $a, b \in \mathrm{W}(A)$. In particular, $\mathrm{V}([1]) = p$. The Frobenius further induces endomorphisms on $\mathrm{W}_\ell(A)$. An $\mathbb{F}_p$-algebra A is called *perfect*, if F is an automorphism. In this case, the induced endomorphism F on $\mathrm{W}(A)$ is an automorphism as well.

The following lemma shows that p-th powering in $\mathrm{W}(A)$ amplifies congruence with respect to its natural filtration.

Lemma 10 (p-th powering)**.** *Let A be an $\mathbb{F}_p$-algebra and let $a, b \in \mathrm{W}(A)$ such that $a - b \in \mathrm{V}\,\mathrm{W}(A)$. Then $a^{p^\ell} - b^{p^\ell} \in \mathrm{V}^{\ell+1}\,\mathrm{W}(A)$ for all $\ell \ge 0$.*

Proof. We use induction on ℓ, where the base case $\ell = 0$ holds by assumption. Now let $\ell \ge 1$. By the induction hypothesis, there is $c \in \mathrm{V}^\ell\,\mathrm{W}(A)$ such that $a^{p^{\ell-1}} = b^{p^{\ell-1}} + c$. Using $\mathrm{V}\,\mathrm{F} = p$ and $p^{-1}\binom{p}{i} \in \mathbb{N}$ for $i \in [p-1]$, we conclude $a^{p^\ell} - b^{p^\ell} = \big(b^{p^{\ell-1}} + c\big)^p - b^{p^\ell} = c^p + \sum_{i=1}^{p-1} p^{-1}\binom{p}{i}\,\mathrm{V}\,\mathrm{F}\big(b^{p^{\ell-1}(p-i)} c^i\big) \in \mathrm{V}^{\ell+1}\,\mathrm{W}(A)$. □

Let $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ denote the *p-adic valuation* of $\mathbb{Q}$. Recall that for a nonzero $q \in \mathbb{Q}$, $v_p(q)$ is defined as the unique integer $v \in \mathbb{Z}$ such that $q = p^v \frac{a}{b}$ where $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$. Moreover, $v_p(0) := \infty$. We generalize this notion to vectors $\boldsymbol{i} \in \mathbb{Q}^s$ by setting $v_p(\boldsymbol{i}) := \min\{v_p(i_1), \dots, v_p(i_s)\} \in \mathbb{Z} \cup \{\infty\}$.

Lemma 11 (Multinomials [Sin80, Theorem 32])**.** *Let $\ell, s \ge 1$ and let $\boldsymbol{i} \in \mathbb{N}^s$ such that $|\boldsymbol{i}| = p^\ell$. Then $p^{\ell - v_p(\boldsymbol{i})}$ divides the multinomial coefficient $\binom{p^\ell}{\boldsymbol{i}} := \binom{p^\ell}{i_1, \dots, i_s}$.*

We have the following important formula for the Teichmüller lift.

Lemma 12 (Expanding Teichmüller)**.** *Let $A = R[\boldsymbol{a}]$ be an R-algebra, where R is an $\mathbb{F}_p$-algebra and $\boldsymbol{a} \in A^n$, and let $f = \sum_{i=1}^s c_i \boldsymbol{a}^{\boldsymbol{\alpha}_i} \in A$, where $c_i \in R$ and $\boldsymbol{\alpha}_i \in \mathbb{N}^n$. Then, in $\mathrm{W}_{\ell+1}(A)$, we have*

$$[f] = \sum_{|\boldsymbol{i}| = p^\ell} p^{-\ell + v_p(\boldsymbol{i})} \tbinom{p^\ell}{\boldsymbol{i}} \cdot \mathrm{V}^{\ell - v_p(\boldsymbol{i})}\,\mathrm{F}^{-v_p(\boldsymbol{i})}\big([c_1 \boldsymbol{a}^{\boldsymbol{\alpha}_1}]^{i_1} \cdots [c_s \boldsymbol{a}^{\boldsymbol{\alpha}_s}]^{i_s}\big). \tag{2.3}$$

where the sum runs over $\boldsymbol{i} \in \mathbb{N}^s$.

Remark 13. Note that the RHS of (2.3) is a well-defined element of $\mathrm{W}(A)$, because $p^{-\ell + v_p(\boldsymbol{i})} \cdot \binom{p^\ell}{\boldsymbol{i}} \in \mathbb{N}$ by Lemma 11, $v_p(\boldsymbol{i}) \le \ell$, and $p^{-v_p(\boldsymbol{i})} \cdot \boldsymbol{i} \in \mathbb{N}^s$.

Proof. Denote by w the RHS of (2.3). We have $[f] = \sum_{i=1}^{s} [c_i \boldsymbol{a}^{\boldsymbol{\alpha}_i}]$ in $\mathrm{W}_1(A)$, so Lemma 10 implies

$$\mathrm{F}^\ell [f] = [f]^{p^\ell} = \left(\sum_{i=1}^{s} [c_i \boldsymbol{a}^{\boldsymbol{\alpha}_i}] \right)^{p^\ell} = \sum_{|\boldsymbol{i}|=p^\ell} \tbinom{p^\ell}{\boldsymbol{i}} \cdot [c_1 \boldsymbol{a}^{\boldsymbol{\alpha}_1}]^{i_1} \cdots [c_s \boldsymbol{a}^{\boldsymbol{\alpha}_s}]^{i_s}$$

in $\mathrm{W}_{\ell+1}(A)$. Since $\mathrm{V}\,\mathrm{F} = \mathrm{F}\,\mathrm{V} = p$, we see that this is equal to $\mathrm{F}^\ell\, w$. The injectivity of F implies $[f] = w$ in $\mathrm{W}_{\ell+1}(A)$. □

2.5. **The de Rham-Witt complex.** For this section we refer to [Ill79]. Let R be a ring. Recall that a *differential graded R-algebra* (R-*dga* for short) is a graded R-algebra $M = \bigoplus_{i \geq 0} M^i$ which is graded skew-commutative, i.e., $ab = (-1)^{ij} ba$ for $a \in M^i, b \in M^j$ (in fact, we also assume that $a^2 = 0$ for $a \in M^{2j+1}$), together with an R-linear differential $d\colon M^i \to M^{i+1}$ satisfying $d \circ d = 0$ and the graded Leibniz rule $d(ab) = b\,da + (-1)^i a\,db$ for $a \in M^i$, $b \in M$. A $\mathbb{Z}$-dga is simply called *dga*. An important example is the R-dga $\Omega_{A/R} := \bigoplus_{i \geq 0} \Omega^i_{A/R}$ together with $d := \bigoplus_{i \geq 0} d^i$.

Definition 14. Fix a prime p. A *de Rham* V*-pro-complex* (*VDR* for short) is a projective system $M_\bullet = ((M_\ell)_{\ell \geq 1}, \mathrm{R}\colon M_{\ell+1} \to M_\ell)$ of dga's together with additive homomorphisms $(\mathrm{V}\colon M_\ell^r \to M_{\ell+1}^r)_{r \geq 0, \ell \geq 1}$ such that $\mathrm{R}\,\mathrm{V} = \mathrm{V}\,\mathrm{R}$ and the following properties are satisfied:

(a) M_1^0 is an $\mathbb{F}_p$-algebra and $M_\ell^0 = \mathrm{W}_\ell(M_1^0)$ with the restriction and Verschiebung maps of Witt rings $\mathrm{R}\colon M_{\ell+1}^0 \to M_\ell^0$ and $\mathrm{V}\colon M_\ell^0 \to M_{\ell+1}^0$,
(b) $\mathrm{V}(\omega\, d\eta) = (\mathrm{V}\,\omega) d\,\mathrm{V}\,\eta$ for all $\omega \in M_\ell^i, \eta \in M_\ell^j$,
(c) $(\mathrm{V}\,w)\, d[a] = \mathrm{V}([a]^{p-1} w)\, d\,\mathrm{V}[a]$ for all $a \in M_1^0, w \in M_\ell^0$.

Illusie [Ill79] constructs for any $\mathbb{F}_p$-algebra A a functorial de Rham V-pro-complex $\mathrm{W}_\bullet\,\Omega_A^\bullet$ with $\mathrm{W}_\ell\,\Omega_A^0 = \mathrm{W}_\ell(A)$, which is called the *de Rham-Witt pro-complex of* A. We have a surjection $\Omega^\bullet_{\mathrm{W}_\ell(A)/\,\mathrm{W}_\ell(\mathbb{F}_p)} \twoheadrightarrow \mathrm{W}_\ell\,\Omega_A^\bullet$, which restricts to the identity on $\mathrm{W}_\ell(A)$ and for $\ell = 1$ is an isomorphism $\Omega^\bullet_{\mathrm{W}_1(A)/\mathbb{F}_p} = \Omega^\bullet_{A/\mathbb{F}_p} \xrightarrow{\sim} \mathrm{W}_1\,\Omega_A^\bullet$.

Like the Kähler differentials, $\mathrm{W}_\bullet\,\Omega_A^\bullet$ satisfy properties that make it convenient to study algebra extensions.

Lemma 15 (Base change [Ill79, Proposition I.1.9.2])**.** *Let k'/k be an extension of perfect fields of characteristic p. Let A be a k-algebra and set $A' := k' \otimes_k A$. Then for all $\ell \geq 1$ and $m \geq 0$ there is a natural $\mathrm{W}_\ell(k')$-module isomorphism*

$$\mathrm{W}_\ell(k') \otimes_{\mathrm{W}_\ell(k)} \mathrm{W}_\ell\,\Omega_A^m \cong \mathrm{W}_\ell\,\Omega_{A'}^m.$$

Lemma 16 (Localization [Ill79, Proposition I.1.11])**.** *Let A be an $\mathbb{F}_p$-algebra and let $B = S^{-1}A$ for some multiplicatively closed set $S \subset A$. Then for all $\ell \geq 1$ and $m \geq 0$ there is a natural $\mathrm{W}_\ell(B)$-module isomorphism*

$$\mathrm{W}_\ell(B) \otimes_{\mathrm{W}_\ell(A)} \mathrm{W}_\ell\,\Omega_A^m \cong \mathrm{W}_\ell\,\Omega_B^m.$$

Lemma 17 (Separable extension)**.** *Let L/K be a finite separable field extension of characteristic p. Then for all $\ell \geq 1$ and $m \geq 0$ there is a natural $\mathrm{W}_\ell(L)$-module isomorphism*

$$\mathrm{W}_\ell(L) \otimes_{\mathrm{W}_\ell(K)} \mathrm{W}_\ell\,\Omega_K^m \cong \mathrm{W}_\ell\,\Omega_L^m.$$

Proof. Proposition I.1.14 of [Ill79] states this for an étale morphism $K \to L$, which means flat and unramified. A vector space over a field is immediately flat, and a finite separable field extension is unramified by definition (see e.g. [Mil80]). □

Remark 18. The proofs in [Ill79] show that the isomorphisms of Lemmas 15 – 17 are in fact isomorphisms of VDR's with appropriately defined VDR-structures.

According to [Ill79, Théorème I.2.17], the morphism of projective systems of rings $\mathrm{R}\,\mathrm{F} = \mathrm{F}\,\mathrm{R}\colon \mathrm{W}_\bullet(A) \to \mathrm{W}_{\bullet-1}(A)$ uniquely extends to a morphism of projective systems of graded algebras $\mathrm{F}\colon \mathrm{W}_\bullet\,\Omega^\bullet_A \to \mathrm{W}_{\bullet-1}\,\Omega^\bullet_A$ such that

$$\mathrm{F}\,d[a]_{\le \ell+1} = [a]^{p-1}_{\le \ell} d[a]_{\le \ell} \quad \text{for all} \quad a \in A,$$
$$\mathrm{F}\,d\,\mathrm{V} = d \text{ in } \mathrm{W}_\ell\,\Omega^1_A \quad \text{for all} \quad \ell \ge 1.$$

Define the *canonical filtration* as $\mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega^\bullet_A := \ker\big(\mathrm{R}^i\colon \mathrm{W}_{\ell+i}\,\Omega^\bullet_A \to \mathrm{W}_\ell\,\Omega^\bullet_A\big)$ for all $\ell \ge 1$, $i \ge 0$.

Now consider the function field $L := k(\boldsymbol{x})$ over a perfect field k. The following fact is quite useful for our differential calculations.

Lemma 19 (Frobenius kernel)**.** *We have*

$$\ker\big(\mathrm{W}_{\ell+i}\,\Omega^m_L \xrightarrow{\mathrm{F}^i} \mathrm{W}_\ell\,\Omega^m_L\big) \subseteq \mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega^m_L.$$

Proof. Let $\omega \in \mathrm{W}_{\ell+i}\,\Omega^m_L$ with $\mathrm{F}^i\,\omega = 0$. Applying $\mathrm{V}^i\colon \mathrm{W}_\ell\,\Omega^m_L \to \mathrm{W}_{\ell+i}\,\Omega^m_L$ and noting that $\mathrm{V}^i\,\mathrm{F}^i = p^i$, we conclude that $p^i\omega = 0$. Proposition I.3.4 of [Ill79] implies $\omega \in \mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega^m_L$. □

2.6. **The de Rham-Witt complex of a polynomial ring.** Let $k/\mathbb{F}_p$ be an algebraic extension and consider the polynomial ring $A := k[\boldsymbol{x}] = k[x_1, \dots, x_n]$. In [Ill79, §I.2] there is an explicit description of $\mathrm{W}_\bullet\,\Omega^\bullet_A$ in the case $k = \mathbb{F}_p$. We generalize this construction by invoking Lemma 15 (note that k is perfect).

Denote by $K := Q(\mathrm{W}(k))$ the quotient field of the Witt ring, and consider the rings $B := \mathrm{W}(k)[\boldsymbol{x}]$ and $C := \bigcup_{i\ge 0} K[\boldsymbol{x}^{p^{-i}}]$. For $m \ge 0$, we write $\Omega^m_B := \Omega^m_{B/\,\mathrm{W}(k)}$ and $\Omega^m_C := \Omega^m_{C/K}$. Since the universal derivation $d\colon C \to \Omega^1_C$ satisfies

$$d\big(x_j^{p^{-i}}\big) = p^{-i} x_j^{p^{-i}}\, dx_j/x_j \quad \text{for all} \quad i \ge 0,\ j \in [n],$$

every differential form $\omega \in \Omega^m_C$ can be written uniquely as

$$\omega = \sum_I c_I \cdot \bigwedge_{j\in I} d\log x_j, \tag{2.4}$$

where the sum is over all $I \in \binom{[n]}{m}$, the $c_I \in C$ are divisible by $(\prod_{j\in I} x_j)^{p^{-s}}$ for some $s \ge 0$, and $d\log x_j := dx_j/x_j$. The c_I in (2.4) are called *coordinates* of ω. A form ω is called *integral* if all its coordinates have coefficients in $\mathrm{W}(k)$. We define

$$\mathrm{E}^m := \mathrm{E}^m_A := \{\omega \in \Omega^m_C \mid \text{both } \omega \text{ and } d\omega \text{ are integral}\}.$$

Then, $\mathrm{E} := \bigoplus_{m\ge 0} \mathrm{E}^m$ is a differential graded subalgebra of Ω_C containing Ω_B.

Let $\mathrm{F}\colon C \to C$ be the unique $\mathbb{Q}_p$-algebra automorphism extending the Frobenius of $\mathrm{W}(k)$ defined by (2.2) and sending $x_j^{p^{-i}}$ to $x_j^{p^{-i+1}}$. The map F extends to an automorphism $\mathrm{F}\colon \Omega^m_C \to \Omega^m_C$ of dga's by acting on the coordinates of the differential forms (keeping $d\log x_j$ fixed), and we define $\mathrm{V}\colon \Omega^m_C \to \Omega^m_C$ by $\mathrm{V} := p\,\mathrm{F}^{-1}$. We have $d\,\mathrm{F} = p\,\mathrm{F}\,d$ and $\mathrm{V}\,d = p d\,\mathrm{V}$, in particular, E is closed under F and V.

We define a filtration $\mathrm{E} = \mathrm{Fil}^0\,\mathrm{E} \supset \mathrm{Fil}^1\,\mathrm{E} \supset \cdots$ of differential graded ideals by

$$\mathrm{Fil}^\ell\,\mathrm{E}^m := \mathrm{V}^\ell\,\mathrm{E}^m + d\,\mathrm{V}^\ell\,\mathrm{E}^{m-1} \quad \text{for} \quad \ell, m \ge 0,$$

and thus obtain a projective system $\mathrm{E}_\bullet$ of dga's

$$\mathrm{E}_\ell := \mathrm{E} \,/\, \mathrm{Fil}^\ell \mathrm{E}, \quad \mathrm{R}\colon \mathrm{E}_{\ell+1} \twoheadrightarrow \mathrm{E}_\ell\,.$$

Theorem 20 (Explicit forms)**.** *The system* $\mathrm{E}_\bullet$ *is a VDR, isomorphic to* $\mathrm{W}_\bullet \Omega^\bullet_A$*.*

Proof. The case $k = \mathbb{F}_p$ follows from [Ill79, Théorème I.2.5]. Lemma 15 yields $\mathrm{W}_\bullet \Omega^\bullet_A \cong \mathrm{W}_\bullet(k) \otimes_{\mathrm{W}(\mathbb{F}_p)} \mathrm{W}_\bullet \Omega^\bullet_{\mathbb{F}_p[\boldsymbol{x}]}$ as VDR's. In particular, the Verschiebung restricts to the Verschiebung of $\mathrm{W}_\bullet(A)$, so it coincides with the map V defined above. □

Lemma 21 ([Ill79, Corollaire I.2.13])**.** *Multiplication with* p *in* E *induces for all* $\ell \geq 0$ *a well-defined injective map* $m_p\colon \mathrm{E}_\ell \to \mathrm{E}_{\ell+1}$ *with* $m_p \circ \mathrm{R} = p$*.*

3. The classical Jacobian criterion

Consider a polynomial ring $k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$ over any field k. In this section we characterize the zeroness of the Jacobian differential which, combined with Lemma 8, gives a criterion on the Jacobian matrix.

Theorem 22 (Jacobian criterion – abstract)**.** *Let* $\boldsymbol{f} = (f_1, \ldots, f_m) \in k[\boldsymbol{x}]^m$*, and assume that* $k(\boldsymbol{x})$ *is a separable extension of* $k(\boldsymbol{f})$*. Then,* $f_1, \ldots, f_m$ *are algebraically independent over* k *if and only if* $\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}) \neq 0$*.*

Proof. Let $f_1, \ldots, f_m$ be algebraically independent over k. Since $k(\boldsymbol{x})$ is separable over $k(\boldsymbol{f})$, we can extend our system to a separating transcendence basis of $k(\boldsymbol{x})$ over k, so we can assume $m = n$. Since $k[\boldsymbol{f}]$ is isomorphic to a polynomial ring, we have $\mathrm{J}_{k[\boldsymbol{f}]/k}(\boldsymbol{f}) \neq 0$. Lemmas 6 and 9 imply $\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}) \neq 0$.

Now let $f_1, \ldots, f_m$ be algebraically dependent over k. The polynomials remain dependent over the algebraic closure $L := \overline{k}$, which is perfect. Hence, $L(\boldsymbol{f})$ is separable over L, and [Eis95, Corollary 16.17 a] implies $m > \mathrm{trdeg}_L(L(\boldsymbol{f})) = \dim_{L(\boldsymbol{f})} \Omega^1_{L(\boldsymbol{f})/L}$. Thus $df_1, \ldots, df_m$ are linearly dependent, so $\mathrm{J}_{L(\boldsymbol{f})/L}(\boldsymbol{f}) = 0$, implying $\mathrm{J}_{L[\boldsymbol{f}]/L}(\boldsymbol{f}) = 0$ by Lemma 6. The inclusion $L[\boldsymbol{f}] \subseteq L[\boldsymbol{x}]$ induces an $L[\boldsymbol{f}]$-module homomorphism $\Omega^m_{L[\boldsymbol{f}]/L} \to \Omega^m_{L[\boldsymbol{x}]/L}$, hence $\mathrm{J}_{L[\boldsymbol{x}]/L}(\boldsymbol{f}) = 0$. Lemma 5 implies $\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}) = 0$. □

Remark 23. Note that also without the separability hypothesis the algebraic dependence of $f_1, \ldots, f_m$ implies $\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}) = 0$.

As a consequence of Theorem 4, the separability hypothesis of Theorem 22 is satisfied in sufficiently large characteristic.

Lemma 24. *Let* $f_1, \ldots, f_m \in k[\boldsymbol{x}]$ *have transcendence degree* r *and degree at most* δ*, and assume* $\mathrm{char}(k) = 0$ *or* $\mathrm{char}(k) > \delta^r$*. Then the extension* $k(\boldsymbol{x})/k(\boldsymbol{f})$ *is separable.*

Proof. In the case $\mathrm{char}(k) = 0$ there is nothing to prove, so let $\mathrm{char}(k) = p > \delta^r$. After renaming polynomials and variables, we may assume that $\boldsymbol{f}_{[r]}$, $\boldsymbol{x}_{[r+1,n]}$ are algebraically independent over k. We claim that $\boldsymbol{x}_{[r+1,n]}$ is a separating transcendence basis of $k(\boldsymbol{x})/k(\boldsymbol{f})$. A transcendence degree argument shows that they form a transcendence basis, hence it suffices to show that x_i is separable over $K := k(\boldsymbol{f}, \boldsymbol{x}_{[r+1,n]})$ for all $i \in [r]$. By Theorem 4, we have $[k(\boldsymbol{x}) : K] \leq [k(\boldsymbol{x}) : k(\boldsymbol{f}_{[r]}, \boldsymbol{x}_{[r+1,n]})] \leq \delta^r < p$. Therefore, the degree of the minimal polynomial of x_i over K is $< p$, thus x_i is indeed separable for all $i \in [r]$. □

4. The Witt-Jacobian criterion: Proving Theorem 1

We proceed in two steps. First, we prove an abstract criterion (zeroness of a differential), and second, an explicit one (degeneracy of a p-adic polynomial).

4.1. The Witt-Jacobian differential.

Definition 25. Let A be an $\mathbb{F}_p$-algebra, $\boldsymbol{a} = (a_1, \dots, a_m) \in A^m$, and $\ell \geq 1$. We call

$$\mathrm{WJ}_{\ell,A}(\boldsymbol{a}) := d[a_1]_{\leq \ell} \wedge \cdots \wedge d[a_m]_{\leq \ell} \in \mathrm{W}_\ell\, \Omega^m_A$$

the *(ℓ-th) Witt-Jacobian differential of $\boldsymbol{a}$ in* $\mathrm{W}_\ell\, \Omega^m_A$.

Let k be an algebraic extension field of $\mathbb{F}_p$ (hence, $k \subseteq \overline{\mathbb{F}}_p$).

Lemma 26. *Let L/k be a finitely generated field extension and let $\ell \geq 1$. Then*

$$\mathrm{W}_\ell\, \Omega^m_L = 0 \iff m > \mathrm{trdeg}_k(L).$$

Proof. Let $r := \mathrm{trdeg}_k(L)$. Since L is finitely generated over a perfect field, it has a separating transcendence basis $\{a_1, \dots, a_r\} \subset L$. This means that L is a finite separable extension of $K := k(a_1, \dots, a_r)$. Since $A := k[a_1, \dots, a_r]$ is isomorphic to a polynomial ring over k, we have $\mathrm{W}_\ell\, \Omega^m_A = 0$ iff $m \geq r+1$ by §2.6. Finally, Lemmas 16 and 17 imply

$$\mathrm{W}_\ell\, \Omega^r_A = 0 \iff \mathrm{W}_\ell\, \Omega^r_K = 0 \iff \mathrm{W}_\ell\, \Omega^r_L = 0. \qquad \square$$

Corollary 27. *For an affine k-domain A and $\ell \geq 1$ we have*

$$\mathrm{W}_\ell\, \Omega^m_A = 0 \iff m > \mathrm{trdeg}_k(A).$$

Proof. Apply Lemma 26 to the quotient field of A and use Lemma 16. $\square$

Now let $A := k[\boldsymbol{x}] = k[x_1, \dots, x_n]$ be a polynomial ring over k, and let $\boldsymbol{f} = (f_1, \dots, f_m) \in A^m$.

Lemma 28 (Zeroness)**.** *If the $f_1, \dots, f_m$ are algebraically dependent, then*

$$\mathrm{WJ}_{\ell,A}(\boldsymbol{f}) = 0 \quad \textit{for all} \quad \ell \geq 1.$$

Proof. Assume that $f_1, \dots, f_m$ are algebraically dependent, and set $R := k[\boldsymbol{f}]$. Corollary 27 implies $\mathrm{W}_\ell\, \Omega^r_R = 0$, thus $\mathrm{WJ}_{\ell,R}(\boldsymbol{f}) = 0$. The inclusion $R \subseteq A$ induces a homomorphism $\mathrm{W}_\ell\, \Omega^m_R \to \mathrm{W}_\ell\, \Omega^m_A$, hence $\mathrm{WJ}_{\ell,A}(\boldsymbol{f}) = 0$. $\square$

We extend the *inseparable degree* to finitely generated field extensions L/K by

$$[L : K]_{\mathrm{insep}} := \min\big\{[L : K(B)]_{\mathrm{insep}} \mid B \subset L \text{ is a transcendence basis of } L/K\big\}.$$

Note that $[L : K]_{\mathrm{insep}}$ is a power of $\mathrm{char}(K)$, and equals 1 iff L/K is separable.

Lemma 29 (Non-zeroness)**.** *If $f_1, \dots, f_m \in A$ are algebraically independent, then*

$$\mathrm{WJ}_{\ell,A}(\boldsymbol{f}) \neq 0 \quad \textit{for all} \quad \ell > \log_p [k(\boldsymbol{x}) : k(\boldsymbol{f})]_{\mathrm{insep}}.$$

Proof. It suffices to consider the case $\ell = e+1$, where $e := \log_p [k(\boldsymbol{x}) : k(\boldsymbol{f})]_{\mathrm{insep}}$. By definition of e, there exist $f_{m+1}, \dots, f_n \in k(\boldsymbol{x})$ such that $L := k(\boldsymbol{x})$ is algebraic over $K = k(f_1, \dots, f_n)$ with $[L : K]_{\mathrm{insep}} = p^e$. So we can assume $m = n$. Let K_{sep} be the separable closure of K in L, thus L/K_{sep} is purely inseparable. For $i \in [0, n]$, define the fields $K_i := K_{\mathrm{sep}}[x_1, \dots, x_i]$, hence we have a tower $K \subseteq K_{\mathrm{sep}} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$. For $i \in [n]$, let $e_i \geq 0$ be minimal such that $x_i^{p^{e_i}} \in K_{i-1}$ (e_i

exists, since K_i/K_{i-1} is purely inseparable). Set $q_i := p^{e_i}$. By the multiplicativity of field extension degrees, we have $e = \sum_{i=1}^n e_i$.

Since $\mathrm{WJ}_{1,A}(\boldsymbol{x}) \neq 0$, we have $p^e \cdot \mathrm{WJ}_{\ell,A}(\boldsymbol{x}) = m_p^e \,\mathrm{WJ}_{1,A}(\boldsymbol{x}) \neq 0$ by Lemma 21. Lemma 16 implies $p^e \cdot \mathrm{WJ}_{\ell,L}(\boldsymbol{x}) \neq 0$. We conclude

$$\mathrm{WJ}_{\ell,L}(x_1^{q_1}, \dots, x_n^{q_n}) = p^e \cdot [x_1]^{q_1-1} \cdots [x_n]^{q_n-1} \cdot \mathrm{WJ}_{\ell,L}(\boldsymbol{x}) \neq 0, \tag{4.1}$$

since $[x_1]^{q_1-1} \cdots [x_n]^{q_n-1}$ is a unit in $\mathrm{W}_\ell(L)$.

Now assume for the sake of contradiction that $\mathrm{WJ}_{\ell,L}(\boldsymbol{f}) = 0$. We show inductively for $j = 0, \dots, n-1$ that the induced map $\Psi_j \colon \mathrm{W}_\ell \,\Omega^n_{K_j} \to \mathrm{W}_\ell \,\Omega^n_L$ satisfies

$$\Psi_j\big(d[x_1^{q_1}] \wedge \cdots \wedge d[x_j^{q_j}] \wedge d[a_{j+1}] \wedge \cdots \wedge d[a_n]\big) = 0 \quad \text{for all } a_{j+1}, \dots, a_n \in K_j. \tag{4.2}$$

To prove this claim for $j = 0$, we first show that for $R := k[\boldsymbol{f}]$ the induced map $\Psi \colon \mathrm{W}_\ell \,\Omega^n_R \to \mathrm{W}_\ell \,\Omega^n_L$ is zero. By Lemma 12, every element $\overline{\omega} \in \mathrm{W}_\ell \,\Omega^n_R$ is a $\mathbb{Z}$-linear combination of products of elements of the form $\mathrm{V}^i[c\boldsymbol{f}^{\boldsymbol{\alpha}}]$ and $d\,\mathrm{V}^i[c\boldsymbol{f}^{\boldsymbol{\alpha}}]$ for some $i \in [0, \ell-1]$, $c \in k$, and $\boldsymbol{\alpha} \in \mathbb{N}^n$. W.l.o.g. let

$$\overline{\omega} = \mathrm{V}^{i_0}[c_0 \boldsymbol{f}^{\boldsymbol{\alpha}_0}] \cdot d\,\mathrm{V}^{i_1}[c_1 \boldsymbol{f}^{\boldsymbol{\alpha}_1}] \wedge \cdots \wedge d\,\mathrm{V}^{i_n}[c_n \boldsymbol{f}^{\boldsymbol{\alpha}_n}].$$

Let $\omega \in \mathrm{W}_{\ell+i} \,\Omega^n_R$ be a lift of $\overline{\omega}$ for i sufficiently large (say $i = \ell$). Using $\mathrm{F}\, d\,\mathrm{V} = d$ and $\mathrm{F}\, d[w] = [w]^{p-1} d[w]$ for $w \in R$, we deduce $\mathrm{F}^\ell\, \omega = g \cdot d[c_1 \boldsymbol{f}^{\boldsymbol{\alpha}_1}] \wedge \cdots \wedge d[c_n \boldsymbol{f}^{\boldsymbol{\alpha}_n}]$ for some $g \in \mathrm{W}_i(R)$. By the Leibniz rule, we can simplify to $\mathrm{F}^\ell\, \omega = g' \cdot d[f_1] \wedge \cdots \wedge d[f_n]$ for some $g' \in \mathrm{W}_i(R)$. Since $\mathrm{WJ}_{\ell,L}(\boldsymbol{f}) = 0$ by assumption, we obtain $\mathrm{F}^\ell\, \Psi(\omega) = \Psi(\mathrm{F}^\ell\, \omega) \in \mathrm{Fil}^\ell\, \mathrm{W}_i \,\Omega^n_L$, thus $\Psi(\omega) \in \mathrm{Fil}^\ell\, \mathrm{W}_{\ell+i} \,\Omega^n_L$ by Lemma 19. This shows $\Psi(\overline{\omega}) = 0$, so Ψ is zero. Lemmas 16 and 17 imply that the map Ψ_0 is zero, proving (4.2) for $j = 0$.

Now let $j \geq 1$ and let $\overline{\omega} = d[x_1^{q_1}] \wedge \cdots \wedge d[x_j^{q_j}] \wedge d[a_{j+1}] \wedge \cdots \wedge d[a_n] \in \mathrm{W}_\ell \,\Omega^n_{K_j}$ with $a_{j+1}, \dots, a_n \in K_j$. Since $K_j = K_{j-1}[x_j]$, we may assume by Lemma 12 that

$$\overline{\omega} = d[x_1^{q_1}] \wedge \cdots \wedge d[x_j^{q_j}] \wedge d\,\mathrm{V}^{i_{j+1}}[c_{j+1} x_j^{\alpha_{j+1}}] \wedge \cdots \wedge d\,\mathrm{V}^{i_n}[c_n x_j^{\alpha_n}],$$

where $i_{j+1}, \dots, i_n \in [0, \ell-1]$, $c_{j+1}, \dots, c_n \in K_{j-1}$, and $\alpha_{j+1}, \dots, \alpha_n \geq 0$. Let $\omega \in \mathrm{W}_{\ell+i} \,\Omega^n_{K_j}$ be a lift of $\overline{\omega}$ for i sufficiently large (say $i = \ell$). As above, we deduce $\mathrm{F}^\ell\, \omega = g \cdot d[x_1^{q_1}] \wedge \cdots \wedge d[x_j^{q_j}] \wedge d[c_{j+1} x_j^{\alpha_{j+1}}] \wedge \cdots \wedge d[c_n x_j^{\alpha_n}]$ for some $g \in \mathrm{W}_i(K_j)$, and by the Leibniz rule, we can write $\mathrm{F}^\ell\, \omega = g' \cdot d[x_1^{q_1}] \wedge \cdots \wedge d[x_j^{q_j}] \wedge d[c_{j+1}] \wedge \cdots \wedge d[c_n]$ for some $g' \in \mathrm{W}_i(K_j)$. Since $x_1^{q_1}, \dots, x_j^{q_j}$, $c_{j+1}, \dots, c_n \in K_{j-1}$, we obtain $\mathrm{F}^\ell\, \Psi_j(\omega) = \Psi_j(\mathrm{F}^\ell\, \omega) \in \mathrm{Fil}^\ell\, \mathrm{W}_i \,\Omega^n_L$ by induction, hence $\Psi_j(\omega) \in \mathrm{Fil}^\ell\, \mathrm{W}_{\ell+i} \,\Omega^n_L$ by Lemma 19. This shows $\Psi_j(\overline{\omega}) = 0$, completing the induction.

Equation (4.2) for $j = n-1$ and $a_n = x_n^{q_n} \in K_{n-1}$ yields $\mathrm{WJ}_{\ell,L}(x_1^{q_1}, \dots, x_n^{q_n}) = 0$, which contradicts (4.1). We conclude $\mathrm{WJ}_{\ell,L}(\boldsymbol{f}) \neq 0$, and thus $\mathrm{WJ}_{\ell,A}(\boldsymbol{f}_r) \neq 0$ by Lemma 16. □

Remark 30. The bound for ℓ in Lemma 29 is tight. To see this, consider $s_i \geq 0$ and $f_i := x_i^{p^{s_i}}$ for $i \in [m]$.

Theorem 31 (Witt-Jacobian criterion – abstract)**.** *Let $\boldsymbol{f} = (f_1, \dots, f_m) \in A^m$, where the degree of f_i is at most $\delta_i \geq 1$ for all $i \in [m]$, and fix $\ell > \lfloor \sum_i \log_p \delta_i \rfloor$. Then $f_1, \dots, f_m$ are algebraically independent over k if and only if $\mathrm{WJ}_{\ell,A}(\boldsymbol{f}) \neq 0$.*

Proof. Let $\boldsymbol{x}_I$ be a transcendence basis of $k(\boldsymbol{x})/k(\boldsymbol{f})$ for some $I \in \binom{[n]}{n-m}$. Then

$$[k(\boldsymbol{x}) : k(\boldsymbol{f})]_{\mathrm{insep}} \leq [k(\boldsymbol{x}) : k(\boldsymbol{f}, \boldsymbol{x}_I)]_{\mathrm{insep}} \leq [k(\boldsymbol{x}) : k(\boldsymbol{f}, \boldsymbol{x}_I)] \leq \delta_1 \cdots \delta_m$$

by Theorem 4. The assertion follows from Lemmas 28 and 29. □

4.2. **The Witt-Jacobian polynomial.** We adopt the notations and assumptions of §2.6. In particular, $k/\mathbb{F}_p$ is an algebraic extension, $A = k[\boldsymbol{x}]$, $B = \mathrm{W}(k)[\boldsymbol{x}]$, $K = Q(\mathrm{W}(k))$, and $C = \bigcup_{i\geq 0} K[\boldsymbol{x}^{p^{-i}}]$. Recall that $\mathrm{E} = \mathrm{E}_A$ is a subalgebra of $\Omega^\bullet_C$ containing $\Omega^\bullet_B$, in particular, $B \subseteq \mathrm{E}^0$. Since k is perfect, we have $\mathrm{W}(k)/p\,\mathrm{W}(k) \cong \mathrm{W}_1(k) = k$ and hence $B/pB \cong A$. In the following, we will use these identifications.

Lemma 32 (Realizing Teichmüller)**.** *Let $f \in A$ and let $g \in B$ such that $f \equiv g \pmod{pB}$. Let $\ell \geq 0$ and let*

$$\tau\colon \mathrm{W}_{\ell+1}(A) \to \mathrm{E}^0_{\ell+1} = \mathrm{E}^0 \,/\, \mathrm{Fil}^{\ell+1}\,\mathrm{E}^0$$

be the $\mathrm{W}(k)$-algebra isomorphism from Theorem 20. Then we have

$$\tau([f]_{\leq \ell+1}) = (\mathrm{F}^{-\ell}\, g)^{p^\ell}.$$

Proof. Write $g = \sum_{i=1}^s c_i \boldsymbol{x}^{\boldsymbol{\alpha}_i}$, where $c_i \in \mathrm{W}(k)$ and $\boldsymbol{\alpha}_i \in \mathbb{N}^n$. By assumption, we have $[f] = \sum_{i=1}^s c_i [\boldsymbol{x}^{\boldsymbol{\alpha}_i}]$ in $\mathrm{W}_1(A)$. By Lemma 10, we obtain

$$\mathrm{F}^\ell[f] = [f]^{p^\ell} = \left(\sum_{i=1}^s c_i[\boldsymbol{x}^{\boldsymbol{\alpha}_i}]\right)^{p^\ell} = \sum_{|\boldsymbol{i}|=p^\ell} \tbinom{p^\ell}{\boldsymbol{i}} \cdot \boldsymbol{c}^{\boldsymbol{i}} [\boldsymbol{x}^{\boldsymbol{\alpha}_1}]^{i_1} \cdots [\boldsymbol{x}^{\boldsymbol{\alpha}_s}]^{i_s} \quad \text{in } \mathrm{W}_{\ell+1}(A),$$

where $\boldsymbol{c} := (c_1, \ldots, c_s)$. As in the proof of Lemma 12, this implies

$$[f] = \sum_{|\boldsymbol{i}|=p^\ell} p^{-\ell+v_p(\boldsymbol{i})} \tbinom{p^\ell}{\boldsymbol{i}} \cdot \mathrm{V}^{\ell-v_p(\boldsymbol{i})}\, \mathrm{F}^{-v_p(\boldsymbol{i})} \big(c_1^{i_1}[\boldsymbol{x}^{\boldsymbol{\alpha}_1}]^{i_1} \cdots c_s^{i_s}[\boldsymbol{x}^{\boldsymbol{\alpha}_s}]^{i_s}\big) \quad \text{in } \mathrm{W}_{\ell+1}(A).$$

Since k is perfect, F is an automorphism of $\mathrm{W}(k)$, so this is well-defined. Denoting $m_i := c_i \boldsymbol{x}^{\alpha_i} \in B$, and using $\tau\,\mathrm{V} = \mathrm{V}\,\tau$ as well as $\tau([x_i]) = x_i$, we conclude

$$\begin{aligned}\tau([f]) &= \sum_{|\boldsymbol{i}|=p^\ell} p^{-\ell+v_p(\boldsymbol{i})} \tbinom{p^\ell}{\boldsymbol{i}}\, \mathrm{V}^{\ell-v_p(\boldsymbol{i})}\, \mathrm{F}^{-v_p(\boldsymbol{i})} (m_1^{i_1} \cdots m_s^{i_s}) \\ &= \sum_{|\boldsymbol{i}|=p^\ell} \tbinom{p^\ell}{\boldsymbol{i}}\, \mathrm{F}^{-\ell}(m_1^{i_1} \cdots m_s^{i_s}) = \left(\sum_{i=1}^s \mathrm{F}^{-\ell}\, m_i\right)^{p^\ell} = \big(\mathrm{F}^{-\ell}\, g\big)^{p^\ell} \quad \text{in } \mathrm{E}^0_{\ell+1}.\end{aligned}$$

Note that the intermediate expression $\mathrm{F}^{-\ell}\, g \in C$ need not be an element of E^0. □

The algebra C is graded in a natural way by $G := \mathbb{N}[p^{-1}]^n$. The homogeneous elements of C of degree $\boldsymbol{\beta} \in G$ are of the form $c\boldsymbol{x}^{\boldsymbol{\beta}}$ for some $c \in K$. This grading extends to Ω_C by defining $\omega \in \Omega^m_C$ to be homogeneous of degree $\boldsymbol{\beta} \in G$ if its coordinates in (2.4) are. We denote the homogeneous part of degree $\boldsymbol{\beta}$ of ω by $(\omega)_{\boldsymbol{\beta}}$.

Lemma 33 (Explicit filtration [Ill79, Proposition I.2.12])**.** *Let $\ell \geq 0$ and let $\boldsymbol{\beta} \in G$. Define*

$$\nu(\ell+1, \boldsymbol{\beta}) := \min\big\{\max\{0, \ell+1+v_p(\boldsymbol{\beta})\}, \ell+1\big\} \in [0, \ell+1].$$

Then $(\mathrm{Fil}^{\ell+1}\,\mathrm{E})_{\boldsymbol{\beta}} = p^{\nu(\ell+1,\boldsymbol{\beta})}(\mathrm{E})_{\boldsymbol{\beta}}$.

The following lemma shows how degeneracy is naturally related to ν.

Lemma 34. *Let $\ell \geq 0$ and let $f \in B \subset \mathrm{E}^0$. Then f is $(\ell+1)$-degenerate if and only if the coefficient of $\boldsymbol{x}^{\boldsymbol{\beta}}$ in $\mathrm{F}^{-\ell}\, f$ is divisible by $p^{\nu(\ell+1,\boldsymbol{\beta})}$ for all $\boldsymbol{\beta} \in G$.*

Proof. The map $\mathrm{F}^{-\ell}$ defines a bijection between the terms of f and the terms of $\mathrm{F}^{-\ell} f$ mapping $c\boldsymbol{x}^{\boldsymbol{\alpha}} \mapsto u\boldsymbol{x}^{\boldsymbol{\beta}}$ with $u = \mathrm{F}^{-\ell}(c)$ and $\boldsymbol{\beta} = p^{-\ell}\boldsymbol{\alpha}$. Since $\boldsymbol{\alpha} \in \mathbb{N}^n$, we have $v_p(\boldsymbol{\beta}) = v_p(p^{-\ell}\boldsymbol{\alpha}) = v_p(\boldsymbol{\alpha}) - \ell \geq -\ell$, thus $\nu(\ell+1, \boldsymbol{\beta}) = \min\{\ell + v_p(\boldsymbol{\beta}), \ell\} + 1 = \min\{v_p(\boldsymbol{\alpha}), \ell\} + 1$, which implies the claim. □

Lemma 35 (Zeroness vs. degeneracy)**.** *Let $\ell \geq 0$, let $\boldsymbol{g} = (g_1, \dots, g_m) \in B^m$, and define $\omega := d(\mathrm{F}^{-\ell} g_1)^{p^\ell} \wedge \cdots \wedge d(\mathrm{F}^{-\ell} g_m)^{p^\ell} \in \mathrm{E}^m$. Then $\omega \in \mathrm{Fil}^{\ell+1} \mathrm{E}^m$ if and only if $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g})$ is $(\ell+1)$-degenerate for all $I \in \binom{[n]}{m}$.*

Proof. From the formula $d\,\mathrm{F} = p\,\mathrm{F}\,d$ [Ill79, (I.2.2.1)] we infer

$$\mathrm{F}^\ell\, d(\mathrm{F}^{-\ell} g_i)^{p^\ell} = \mathrm{F}^\ell\, d\,\mathrm{F}^{-\ell}(g_i^{p^\ell}) = p^{-\ell} dg_i^{p^\ell} = g_i^{p^\ell - 1} dg_i,$$

hence $\mathrm{F}^\ell\, \omega = (g_1 \cdots g_m)^{p^\ell - 1}\, dg_1 \wedge \cdots \wedge dg_m$. A standard computation shows

$$dg_1 \wedge \cdots \wedge dg_m = \sum_I \Big(\prod_{j \in I} x_j \Big) \cdot \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{g}) \cdot \bigwedge_{j \in I} d \log x_j,$$

where the sum runs over all $I \in \binom{[n]}{m}$. This yields the unique representation

$$\omega = \sum_I \mathrm{F}^{-\ell}\, \mathrm{WJP}_{\ell+1,I}(\boldsymbol{g}_r) \cdot \bigwedge_{j \in I} d \log x_j.$$

By Lemma 33, we have $\mathrm{Fil}^{\ell+1} \mathrm{E}^m = \bigoplus_{\boldsymbol{\beta} \in G} \big(\mathrm{Fil}^{\ell+1} \mathrm{E}^m\big)_{\boldsymbol{\beta}} = \bigoplus_{\boldsymbol{\beta} \in G} p^{\nu(\ell+1,\boldsymbol{\beta})} \big(\mathrm{E}^m\big)_{\boldsymbol{\beta}}$, and we conclude

$$\begin{aligned}
\omega \in \mathrm{Fil}^{\ell+1} \mathrm{E}^m &\iff \forall \boldsymbol{\beta} \in G\colon\ (\omega)_{\boldsymbol{\beta}} \in p^{\nu(\ell+1,\boldsymbol{\beta})} \big(\mathrm{E}^m\big)_{\boldsymbol{\beta}} \\
&\iff \forall \boldsymbol{\beta} \in G, I \in \tbinom{[n]}{m}\colon\ (\mathrm{F}^{-\ell}\, \mathrm{WJP}_{\ell+1,I}(\boldsymbol{g}))_{\boldsymbol{\beta}} \in p^{\nu(\ell+1,\boldsymbol{\beta})}\, \mathrm{F}^{-\ell} B \\
&\iff \forall I \in \tbinom{[n]}{m}\colon\ \ \mathrm{WJP}_{\ell+1,I}(\boldsymbol{g}) \text{ is } (\ell+1)\text{-degenerate},
\end{aligned}$$

where we used Lemma 34. □

Proof of Theorem 1. Using Lemmas 32 and 35, this follows from Theorem 31. □

4.3. **Degeneracy of the p-adic Jacobian.**

Theorem 36 (Necessity)**.** *Let $\boldsymbol{f} \in A^m$ and $\boldsymbol{g} \in B^m$ such that $f_i \equiv g_i \pmod{pB}$ for all $i \in [m]$. If $f_1, \dots, f_m$ are algebraically dependent, then the p-adic polynomial*

$$\widehat{J}_{\boldsymbol{x}_I}(\boldsymbol{g}) := \Big(\prod_{j \in I} x_j \Big) \cdot \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{g})$$

is degenerate for any $I \in \binom{[n]}{m}$. The converse does not hold.

Proof. Fix $\ell \in \mathbb{N}$ such that p^ℓ is at least the degree of $\widehat{J}_{\boldsymbol{x}_I}(\boldsymbol{g})$. Consider the differential form $\gamma := d\,\mathrm{V}^\ell[f_1]_{\leq \ell+1} \wedge \cdots \wedge d\,\mathrm{V}^\ell[f_m]_{\leq \ell+1} \in \mathrm{W}_{\ell+1}\,\Omega^m_A$.

Assume that $f_1, \dots, f_m$ are algebraically dependent and set $R := k[\boldsymbol{f}]$. Corollary 27 implies $\mathrm{W}_{\ell+1}\,\Omega^m_R = 0$, thus γ vanishes in $\mathrm{W}_{\ell+1}\,\Omega^m_R$. The inclusion $R \subseteq A$ induces a homomorphism $\mathrm{W}_{\ell+1}\,\Omega^m_R \to \mathrm{W}_{\ell+1}\,\Omega^m_A$, hence γ vanishes in $\mathrm{W}_{\ell+1}\,\Omega^m_A$ itself.

As in the proof of Lemma 32, we first make $\mathrm{V}^\ell[f]_{\leq \ell+1}$ explicit for $f \in A$. Let $g \in B$ such that $f \equiv g \pmod{pB}$, and write $g = \sum_{i=1}^s c_i \boldsymbol{x}^{\boldsymbol{\alpha}_i}$, where $c_i \in \mathrm{W}(k)$ and $\boldsymbol{\alpha}_i \in \mathbb{N}^n$ for $i \in [s]$. Note that for $w := \mathrm{V}^\ell(\sum_{i=1}^s c_i[\boldsymbol{x}^{\boldsymbol{\alpha}_i}]) \in \mathrm{W}_{\ell+1}(A)$ we have $\mathrm{F}^\ell(w) = p^\ell \sum_{i=1}^s c_i[\boldsymbol{x}^{\boldsymbol{\alpha}_i}]$. Since by assumption $[f] - \sum_{i=1}^s c_i[\boldsymbol{x}^{\boldsymbol{\alpha}_i}] \in \mathrm{V}\,\mathrm{W}(A)$, we

get $p^\ell([f] - \sum_{i=1}^s c_i[\boldsymbol{x}^{\boldsymbol{\alpha}_i}]) \in \mathrm{V}^{\ell+1}\,\mathrm{W}(A)$. This proves $\mathrm{F}^\ell(\mathrm{V}^\ell[f]_{\le \ell+1}) = \mathrm{F}^\ell(w)$. The injectivity of F^ℓ implies $\mathrm{V}^\ell[f]_{\le\ell+1} = w$. Finally, we apply $\tau\colon \mathrm{W}_{\ell+1}(A) \to \mathrm{E}^0_{\ell+1}$ to get $\tau(\mathrm{V}^\ell[f]_{\le\ell+1}) = \tau(w) = \mathrm{V}^\ell(g)$.

So we have the explicit condition $\gamma' := \tau(\gamma) = d\,\mathrm{V}^\ell(g_1) \wedge \cdots \wedge d\,\mathrm{V}^\ell(g_m) \in \mathrm{Fil}^{\ell+1}\,\mathrm{E}^m$. Now we continue to calculate γ' much like in Lemma 35. The formula $d\,\mathrm{F} = p\,\mathrm{F}\,d$ (see [Ill79, (I.2.2.1)]) implies $d = \mathrm{F}\,dp\,\mathrm{F}^{-1} = \mathrm{F}\,d\,\mathrm{V}$, hence $d = \mathrm{F}^\ell\,d\,\mathrm{V}^\ell$. We infer $\mathrm{F}^\ell\,d(V^\ell g_i) = dg_i$, thus $\mathrm{F}^\ell\,\gamma' = dg_1 \wedge \cdots \wedge dg_m$. Moreover,

$$dg_1 \wedge \cdots \wedge dg_m = \sum_I \Big(\prod_{j\in I} x_j\Big) \cdot \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{g}) \cdot \bigwedge_{j\in I} d\log x_j,$$

where the sum runs over all $I \in \binom{[n]}{r}$. This yields

$$\gamma' = \sum_I \mathrm{F}^{-\ell}\,\widehat{J}_{\boldsymbol{x}_I}(\boldsymbol{g}) \cdot \bigwedge_{j\in I} d\log x_j,$$

and this representation is unique.

As in the proof of Lemma 35 we conclude

$$\begin{aligned}
\gamma' \in \mathrm{Fil}^{\ell+1}\,\mathrm{E}^m &\iff \forall \boldsymbol{\beta} \in G\colon\ (\gamma')_{\boldsymbol{\beta}} \in p^{\nu(\ell+1,\boldsymbol{\beta})}\big(\mathrm{E}^m\big)_{\boldsymbol{\beta}} \\
&\iff \forall \boldsymbol{\beta} \in G, I \in \tbinom{[n]}{m}\colon\ (\mathrm{F}^{-\ell}\,\widehat{J}_{\boldsymbol{x}_I}(\boldsymbol{g}))_{\boldsymbol{\beta}} \in p^{\nu(\ell+1,\boldsymbol{\beta})}\,\mathrm{F}^{-\ell}\,B \\
&\iff \forall I \in \tbinom{[n]}{m}\colon\ \widehat{J}_{\boldsymbol{x}_I}(\boldsymbol{g}) \text{ is } (\ell+1)\text{-degenerate},
\end{aligned}$$

where we used Lemma 34. Since our ℓ is large enough, this is finally equivalent to the degeneracy of $\widehat{J}_{\boldsymbol{x}_I}(\boldsymbol{g})$. This finishes the proof of one direction.

The converse is false, because if we fix $f_1 := x_1^p$ and $f_2 := x_2^p$, then $\widehat{J}_{\boldsymbol{x}_2}(x_1^p, x_2^p) = p^2 x_1^p x_2^p$. This is clearly degenerate, but f_1, f_2 are algebraically independent. □

5. Independence testing: Proving Theorem 2

5.1. **Testing degeneracy is 'easy'.** In this section, let $A = k[\boldsymbol{x}]$ be a polynomial ring over an algebraic extension k of $\mathbb{F}_p$. For the computational problem of algebraic independence testing, we consider k as part of the input, so we may assume that $k = \mathbb{F}_{p^e}$ is a finite field. The algorithm works with the truncated Witt ring $\mathrm{W}_{\ell+1}(\mathbb{F}_{p^t})$ of a small extension $\mathbb{F}_{p^t}/k$. For computational purposes, we will use the fact that $\mathrm{W}_{\ell+1}(\mathbb{F}_{p^t})$ is isomorphic to the *Galois ring* $G_{\ell+1,t}$ of characteristic $p^{\ell+1}$ and size $p^{(\ell+1)t}$ (see [Rag69, (3.5)]).

This ring can be realized as follows. There exists a monic polynomial $h \in \mathbb{Z}/(p^{\ell+1})[x]$ of degree t dividing $x^{p^t-1} - 1$ in $\mathbb{Z}/(p^{\ell+1})[x]$, such that $\overline{h} := h \pmod p$ is irreducible in $\mathbb{F}_p[x]$, and $\overline{\xi} := x + (\overline{h})$ is a primitive (p^t-1)-th root of unity in $\mathbb{F}_p[x]/(\overline{h})$. Then we may identify $G_{\ell+1,t} = \mathbb{Z}/(p^{\ell+1})[x]/(h)$ and $\mathbb{F}_{p^t} = \mathbb{F}_p[x]/(\overline{h})$, and $\xi := x + (h)$ is a primitive (p^t-1)-th root of unity in $G_{\ell+1,t}$ (see the proof of [Wan03, Theorem 14.8]). The ring $G_{\ell+1,t}$ has a unique maximal ideal (p), and $G_{\ell+1,t}/(p) \cong \mathbb{F}_{p^t}$. Furthermore, $G_{\ell+1,t}$ is a free $\mathbb{Z}/(p^{\ell+1})$-module with basis $1, \xi, \ldots, \xi^{t-1}$, so that any $\overline{a} \in \mathbb{F}_{p^t}$ can be lifted coordinate-wise to $a \in G_{\ell+1,t}$ satisfying $\overline{a} \equiv a \pmod p$. To map elements of k to $\mathbb{F}_{p^t}$ efficiently, we use [Len91].

The following two lemmas show that the coefficient of a monomial in an arithmetic circuit over $G_{\ell+1,t}[z]$ can be computed by a #P-oracle (see [Val79] for a definition of #P). The first gives an interpolation formula inspired by [KS11].

Lemma 37 (Interpolation)**.** *In the above situation, let $f \in G_{\ell+1,t}[z]$ be a polynomial of degree $D < p^t - 1$. Then*

$$\operatorname{coeff}(z^d, f) = (p^t - 1)^{-1} \cdot \sum_{j=0}^{p^t-2} \xi^{-jd} f(\xi^j) \quad \text{for all } d \in [0, D].$$

Proof. Set $u := p^t - 1$. Note that u is a unit in $G_{\ell+1,t}$, because $u \notin (p)$. It suffices to show that $\sum_{j=0}^{u-1} \xi^{-jd}\xi^{ij} = u \cdot \delta_{di}$ for all $d, i \in [0, u-1]$. This is clear for $d = i$, so let $d \neq i$. Then $\sum_{j=0}^{u-1} \xi^{-jd}\xi^{ij} = \sum_{j=0}^{u-1} \xi^{j(i-d)} = 0$, because ξ^{i-d} is a u-th root of unity $\neq 1$ and $\xi^{i-d} - 1$ is a non-zerodivisor in $G_{\ell+1,t}$. □

This exponentially large sum can be evaluated using a #P-oracle.

Lemma 38 (#P-oracle)**.** *Given $G_{\ell+1,t}$, a primitive $(p^t - 1)$-th root of unity $\xi \in G_{\ell+1,t}$ as above, an arithmetic circuit C over $G_{\ell+1,t}[z]$ of degree $D < p^t - 1$ and $d \in [0, D]$, the $\operatorname{coeff}(z^d, C)$ can be computed in $\mathrm{FP}^{\#\mathrm{P}}$ (with a single #P-oracle query).*

Proof. Set $u := p^t - 1$. Lemma 37 shows that we obtain the coefficient by computing a sum $S := \sum_{i=0}^{u-1} a_i$, where each summand $a_i \in G_{\ell+1,t}$ can be computed in polynomial time, because C can be efficiently evaluated.

Each a_i can be written as $a_i = \sum_{j=0}^{t-1} c_{i,j}\xi^j$ with $c_{i,j} \in \mathbb{Z}/(p^{\ell+1})$. Hence, we can represent a_i by a tuple $\boldsymbol{c}_i \in [0, p^{\ell+1} - 1]^t$ of integers, and a representation of S can be obtained by computing the componentwise integer sum $\boldsymbol{s} = \sum_{i=0}^{u-1} \boldsymbol{c}_i$. Set $N := u \cdot p^{\ell+1} \in \mathbb{N}$. Then $\boldsymbol{s}, \boldsymbol{c}_i \in [0, N-1]^t$, so we can encode the tuples $\boldsymbol{s}$ and $\boldsymbol{c}_i$ into single integers via the bijection

$$\iota\colon [0, N-1]^t \to [0, N^t - 1], \quad (n_0, \ldots, n_{t-1}) \mapsto \sum_{j=0}^{t-1} n_j N^j.$$

This bijection and its inverse are efficiently computable. Moreover, ι is compatible with the sum under consideration, i.e., $\iota(\boldsymbol{s}) = \sum_{i=0}^{u-1} \iota(\boldsymbol{c}_i)$, thus we reduced our problem to the summation of integers which are easy to compute.

To show that $\iota(\boldsymbol{s})$ can be computed in #P, we design a non-deterministic polynomial time Turing machine that, given $\boldsymbol{c}_0, \ldots, \boldsymbol{c}_{t-1}$ as input, has exactly $\iota(\boldsymbol{s})$ accepting computation paths. This can be done as follows. First we branch over all integers $i \in [0, u-1]$. In each branch i, we (deterministically) compute the integer $\iota(\boldsymbol{c}_i)$ and branch again into exactly $\iota(\boldsymbol{c}_i)$ computation paths that all accept. This implies that the machine has altogether $\sum_{i=0}^{u-1} \iota(\boldsymbol{c}_i) = \iota(\boldsymbol{s})$ accepting computation paths. □

Proof of Theorem 2. We set up some notation. Let $s := \sum_{i=1}^{m} \operatorname{size}(C_i)$ be the size of the input circuits. Then $\delta := 2^{s^2}$ is an upper bound for their degrees. Set $\ell := \lfloor m \log_p \delta \rfloor$ and $D := m\delta^{m+1} + 1$. The constants of the C_i lie in $k = \mathbb{F}_{p^e}$, which is also given as input. Let $t \geq 1$ be a multiple of e satisfying $p^t - 1 \geq D^n$. Theorem 1 implies that the following procedure decides the algebraic independence of $C_1, \ldots, C_m$.

(1) Using non-determinism, guess $I \in \binom{[n]}{m}$ and $\boldsymbol{\alpha} \in [0, D-1]^n$.
(2) Determine $G_{\ell+1,t}$ and ξ as follows. Using non-determinism, guess a monic degree-t polynomial $h \in \mathbb{Z}/(p^{\ell+1})[x]$. Check that h divides $x^{p^t-1} - 1$, $\overline{h} := h$

(mod p) is irreducible and $\overline{\xi} := x + (\overline{h})$ has order $p^t - 1$ (for the last test, also guess a prime factorization of $p^t - 1$), otherwise `reject`. Set $\xi := x + (h)$.

(3) By lifting the constants of the circuits C_i from k to $G_{\ell+1,t}$, compute circuits $C'_1, \dots, C'_m$ over $G_{\ell+1,t}[\boldsymbol{x}]$ such that $C'_i \equiv C_i \pmod p$ for all $i \in [m]$. Furthermore, compute a circuit C for $\mathrm{WJP}_{\ell+1,I}(C'_1, \dots, C'_m)$ over $G_{\ell+1,t}[\boldsymbol{x}]$.

(4) Compute the univariate circuit $C' := C(z, z^D, \dots, z^{D^{n-1}})$ over $G_{\ell+1,t}[z]$. The term $c\boldsymbol{x}^{\boldsymbol{\alpha}}$ of C is mapped to the term cz^d of C', where $d := \sum_{i=1}^n \alpha_i D^{i-1}$.

(5) Compute $c = \mathrm{coeff}(z^d, C') \in G_{\ell+1,t}$. If c is divisible by $p^{\min\{v_p(\boldsymbol{\alpha}),\ell\}+1}$, then `reject`, otherwise `accept`.

In step (2), the irreducibility of $\overline{h}$ can be tested efficiently by checking whether $\gcd(\overline{h}, x^{p^i} - x) = 1$ for $i \le \lfloor t/2 \rfloor$ (see [Wan03, Theorem 10.1]). For the order test, verify $\overline{\xi}^j \neq 1$ for all maximal divisors j of $p^t - 1$ (using its prime factorization).

The lifting in step (3) can be done as described in the beginning of this section. To obtain C in polynomial time, we use [BS83] and [Ber84] for computing the partial derivatives and the determinant respectively, and repeated squaring for the high power.

We have $\deg(C) \le m\delta(p^\ell - 1) + m + m(\delta - 1) \le m\delta^{m+1} < D$, so the *Kronecker substitution* in step (4) preserves terms. Since $\deg_z(C') < D^n \le p^t - 1$, step (5) is in $\mathrm{FP}^{\#\mathrm{P}}$ by Lemma 38. Altogether we get an $\mathrm{NP}^{\#\mathrm{P}}$-algorithm. □

5.2. **Testing degeneracy is hard.** Here we state the lower bound for testing degeneracy proved by Mengel [Men12]. For the standard complexity notation one can refer to the book [AB09]. Let ℓ-Degen denote the following problem. Given a univariate arithmetic circuit computing $f \in \mathbb{Q}_p[x]$, test whether f is ℓ-degenerate. Note that for $\ell = 1$ this is the same as the identity test $f \equiv 0 \pmod p$, so that 1-Degen $\in$ BPP. The situation drastically changes when $\ell > 1$.

Theorem 39. [Men12] *For $\ell > 1$, ℓ-Degen is $\mathrm{C}_=\mathrm{P}$-hard under* ZPP*-reductions.*

Proof sketch. Consider the problem ZMC: Given $\alpha \in \mathbb{N}$ and a univariate arithmetic circuit computing $f \in \mathbb{Z}[x]$, test whether $\mathrm{coeff}(x^\alpha, f) = 0$. By [FMM12] ZMC is $\mathrm{C}_=\mathrm{P}$-hard. The idea is to reduce ZMC to ℓ-Degen. Randomly pick a sufficiently large prime p, in particular, larger than all coefficients of f. Compute a circuit for $g := p^{\ell-1} x^{p^{\ell-1}-\alpha} \cdot f$. It can be shown that g is ℓ-degenerate iff $\mathrm{coeff}(x^\alpha, f) = 0$. □

Corollary 40. [Men12] *Let $\ell > 1$. If ℓ-Degen $\in$ PH, then* PH *collapses.*

Proof sketch. Classically, we have

$$\mathrm{PH} \subseteq \mathrm{NP}^{\#\mathrm{P}} \subseteq \mathrm{NP}^{\mathrm{C}_=\mathrm{P}}.$$

By Theorem 39 it follows that

$$\mathrm{PH} \subseteq \mathrm{NP}^{\mathrm{ZPP}^{\ell\text{-Degen}}} \subseteq \mathrm{NP}^{\mathrm{NP}^{\ell\text{-Degen}}}.$$

Thus, if ℓ-Degen $\in \Sigma_i$, then PH $\subseteq \Sigma_{i+2}$. □

6. Identity testing: Proving Theorem 3

The aim of this section is to construct an efficiently computable hitting-set (Theorem 47) for polynomial degree circuits involving input polynomials of constant transcendence degree and small sparsity, which works in any characteristic. It will involve sparse PIT techniques and our Witt-Jacobian criterion.

As before, we consider a polynomial ring $A = k[\boldsymbol{x}]$ over an algebraic extension k of $\mathbb{F}_p$. Moreover, we set $R := \mathrm{W}(k)$ and $B := R[\boldsymbol{x}]$. For a prime q and an integer a we denote by $\lfloor a \rfloor_q$ the unique integer $0 \le b < q$ such that $a \equiv b \pmod q$. Finally, for a polynomial f we denote by $\mathrm{sp}(f)$ its sparsity.

Lemma 41 (Using sparsity)**.** *Let $\ell \ge 0$ and let $g \in B$ be an s-sparse polynomial of degree less than $D \ge 2$ which is not $(\ell+1)$-degenerate. Let $S \subset R$ be a subset such that $|S/pR| \ge (ns\lceil \log_2 D \rceil)^2 D$, and let $r \in [n]$.*

Then there exist $c \in S$ and a prime $q \le (ns\lceil \log_2 D \rceil)^2$ such that $g(\boldsymbol{x}_{[r]}, \boldsymbol{c}) \in R[\boldsymbol{x}_{[r]}]$ is not $(\ell+1)$-degenerate, where $\boldsymbol{c} := \big(c^{\lfloor D^0 \rfloor_q}, c^{\lfloor D^1 \rfloor_q}, \dots, c^{\lfloor D^{n-r-1} \rfloor_q}\big) \in R^{n-r}$.

Proof. Write $g = \sum_{\boldsymbol{\beta} \in \mathbb{N}^r} g_{\boldsymbol{\beta}} \boldsymbol{x}_{[r]}^{\boldsymbol{\beta}}$ with $g_{\boldsymbol{\beta}} \in R[\boldsymbol{x}_{[r+1,n]}]$. Since g is not $(\ell+1)$-degenerate, there exists $\boldsymbol{\alpha} \in \mathbb{N}^n$ such that the coefficient $c_{\boldsymbol{\alpha}} \in R$ of $\boldsymbol{x}^{\boldsymbol{\alpha}}$ in g is not divisible by $p^{\min\{v_p(\boldsymbol{\alpha}), \ell\}+1}$. Write $\boldsymbol{\alpha} = (\boldsymbol{\alpha'}, \boldsymbol{\alpha''}) \in \mathbb{N}^r \times \mathbb{N}^{n-r}$. Since $c_{\boldsymbol{\alpha}}$ is the coefficient of $\boldsymbol{x}_{[r+1,n]}^{\boldsymbol{\alpha''}}$ in $g_{\boldsymbol{\alpha'}}$, this polynomial cannot be divisible by $p^{\min\{v_p(\boldsymbol{\alpha}), \ell\}+1}$. Our aim is to find $\boldsymbol{c} \in R^{n-r}$ such that $g_{\boldsymbol{\alpha'}}(\boldsymbol{c})$ is not divisible by $p^{\min\{v_p(\boldsymbol{\alpha}), \ell\}+1}$, since then it is neither by the possibly higher power $p^{\min\{v_p(\boldsymbol{\alpha''}), \ell\}+1}$. In other words, if we write $g_{\boldsymbol{\alpha'}} = p^e g'$, where g' is not divisible by p, we have an instance of PIT over the field $R/pR \cong k$.

We solve it using a *Kronecker substitution*, so consider the univariate polynomial $h' := g'\big(t^{D^0}, t^{D^1}, \dots, t^{D^{n-r-1}}\big) \in R[t]$ in the new variable t. Since $\deg g' = \deg g_{\alpha'} \le \deg g < D$, the substitution preserves terms, so $h' \notin pR[t]$. Furthermore, h' is s-sparse and of degree $< D^n$. For any $q \in \mathbb{N}$, let

$$h_q := g'\big(t^{\lfloor D^0 \rfloor_q}, t^{\lfloor D^1 \rfloor_q}, \dots, t^{\lfloor D^{n-r-1} \rfloor_q}\big) \in R[t].$$

By [BHLV09, Lemma 13], there are $< ns \log_2 D$ many primes q such that $h_q \in pR[t]$. Since the interval $[N^2]$ contains at least N primes for $N \ge 2$ (this follows e.g. from [RS62, Corollary 1]), there is a prime $q \le (ns\lceil \log_2 D \rceil)^2$ with $h_q \notin pR[t]$. Since $\deg(h_q) < qD \le (ns\lceil \log_2 D \rceil)^2 D \le |S/pR|$, there exists $c \in S$ with $h_q(c) \notin pR$. □

Lemma 42 (p-adic triangle is isosceles)**.** *Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{Q}^s$. Then*

$$v_p(\boldsymbol{\alpha} + \boldsymbol{\beta}) \ge \min\{v_p(\boldsymbol{\alpha}), v_p(\boldsymbol{\beta})\},$$

with equality if $v_p(\boldsymbol{\alpha}) \ne v_p(\boldsymbol{\beta})$.

Proof. Let $i \in [s]$ such that $v_p(\boldsymbol{\alpha} + \boldsymbol{\beta}) = v_p(\alpha_i + \beta_i)$. Then

$$v_p(\boldsymbol{\alpha} + \boldsymbol{\beta}) = v_p(\alpha_i + \beta_i) \ge \min\{v_p(\alpha_i), v_p(\beta_i)\} \ge \min\{v_p(\boldsymbol{\alpha}), v_p(\boldsymbol{\beta})\}.$$

Now assume $v_p(\boldsymbol{\alpha}) < v_p(\boldsymbol{\beta})$, say. Let $i \in [s]$ such that $v_p(\boldsymbol{\alpha}) = v_p(\alpha_i)$. Then $v_p(\alpha_i) < v_p(\beta_i)$, therefore

$$\begin{aligned} v_p(\boldsymbol{\alpha} + \boldsymbol{\beta}) &\le v_p(\alpha_i + \beta_i) = \min\{v_p(\alpha_i), v_p(\beta_i)\} = v_p(\alpha_i) = v_p(\boldsymbol{\alpha}) \\ &= \min\{v_p(\boldsymbol{\alpha}), v_p(\boldsymbol{\beta})\} \le v_p(\boldsymbol{\alpha} + \boldsymbol{\beta}). \end{aligned}$$

□

Lemma 43. *Let $\ell \ge 0$, let $g \in B$ and let $\boldsymbol{\alpha} \in \mathbb{N}^n$ with $v_p(\boldsymbol{\alpha}) \ge \ell$. Then g is $(\ell+1)$-degenerate if and only if $\boldsymbol{x}^{\boldsymbol{\alpha}} \cdot g$ is $(\ell+1)$-degenerate.*

Proof. It suffices to show that $\min\{v_p(\boldsymbol{\beta}), \ell\} = \min\{v_p(\boldsymbol{\alpha} + \boldsymbol{\beta}), \ell\}$ for all $\boldsymbol{\beta} \in \mathbb{N}^n$. But the assumption implies that $\min\{v_p(\boldsymbol{\beta}), \ell\} = \min\{v_p(\boldsymbol{\alpha}), v_p(\boldsymbol{\beta}), \ell\}$, which is $\le \min\{v_p(\boldsymbol{\alpha}+\boldsymbol{\beta}), \ell\}$ by Lemma 42 with equality, if $v_p(\boldsymbol{\alpha}) \ne v_p(\boldsymbol{\beta})$. If $v_p(\boldsymbol{\alpha}) = v_p(\boldsymbol{\beta})$, then $\min\{v_p(\boldsymbol{\beta}), \ell\} = \min\{v_p(\boldsymbol{\alpha}), \ell\} = \ell \ge \min\{v_p(\boldsymbol{\alpha} + \boldsymbol{\beta}), \ell\}$. □

Lemma 44 (Variable reduction)**.** *Let $f_1, \dots, f_r \in A$ be polynomials of sparsity at most $s \geq 1$ and degree at most $\delta \geq 1$. Assume that $f_1, \dots, f_r, x_{r+1}, \dots, x_n$ are algebraically independent. Let $D := r\delta^{r+1} + 1$ and let $S \subseteq k$ be of size $|S| \geq n^2(2\delta rs)^{4r^2 s}\lceil \log_2 D\rceil^2 D$.*

Then there exist $c \in S$ and a prime $2 \leq q \leq n^2(2\delta rs)^{4r^2 s}\lceil \log_2 D\rceil^2$ such that $f_1(\boldsymbol{x}_{[r]}, \boldsymbol{c}), \dots, f_r(\boldsymbol{x}_{[r]}, \boldsymbol{c}) \in k[\boldsymbol{x}_{[r]}]$ are algebraically independent over k, where $\boldsymbol{c} = \big(c^{\lfloor D^0\rfloor_q}, c^{\lfloor D^1\rfloor_q}, \dots, c^{\lfloor D^{n-r-1}\rfloor_q}\big) \in k^{n-r}$.

Proof. Let $g_i \in B$ be obtained from f_i by lifting each coefficient, so that g_i is s-sparse and $f_i \equiv g_i \pmod{pB}$. Set $\boldsymbol{g} := (g_1, \dots, g_r)$. Theorem 1 implies that with $\ell := \lfloor r \log_p \delta \rfloor$ the polynomial $g := \mathrm{WJP}_{\ell+1,[n]}(\boldsymbol{g}, \boldsymbol{x}_{[r+1,n]}) \in B$ is not $(\ell+1)$-degenerate. We have

$$\begin{aligned} g &= (g_1 \cdots g_r \cdot x_{r+1} \cdots x_n)^{p^\ell - 1}(x_1 \cdots x_n) \cdot \det \mathcal{J}_{\boldsymbol{x}}(\boldsymbol{g}, \boldsymbol{x}_{[r+1,n]}) \\ &= (x_{r+1} \cdots x_n)^{p^\ell} \cdot (g_1 \cdots g_r)^{p^\ell - 1}(x_1 \cdots x_r) \cdot \det \mathcal{J}_{\boldsymbol{x}_{[r]}}(\boldsymbol{g}), \end{aligned}$$

since the Jacobian matrix $\mathcal{J}_{\boldsymbol{x}}(\boldsymbol{g}, \boldsymbol{x}_{[r+1,n]})$ is block-triangular with the lower right block being the $(n-r) \times (n-r)$ identity matrix. Define

$$g' := (g_1 \cdots g_r)^{p^\ell - 1}(x_1 \cdots x_r) \cdot \det \mathcal{J}_{\boldsymbol{x}_{[r]}}(\boldsymbol{g}) = \mathrm{WJP}_{\ell+1,[r]}(\boldsymbol{g}) \in B.$$

Then $g = (x_{r+1} \cdots x_n)^{p^\ell} g'$, and g' is not $(\ell+1)$-degenerate by Lemma 43. Moreover, we have $\deg(g') \leq r\delta(p^\ell - 1) + r + r(\delta - 1) \leq r\delta^{r+1} < D$ and

$$\mathrm{sp}(g') \leq \binom{s + (p^\ell - 1) - 1}{s - 1}^r \cdot r! s^r \leq \big(s + \delta^r\big)^{rs} \cdot (rs)^r \leq (2\delta rs)^{2r^2 s}.$$

By Lemma 41, there exist $c \in S$ and a prime $q \leq n^2(2\delta rs)^{4r^2 s}\lceil \log_2 D\rceil^2$ such that $h := g'(\boldsymbol{x}_{[r]}, \boldsymbol{c}') \in R[\boldsymbol{x}_{[r]}]$ is not $(\ell+1)$-degenerate, where

$$\boldsymbol{c} := \big(c^{\lfloor D^0\rfloor_q}, c^{\lfloor D^1\rfloor_q}, \dots, c^{\lfloor D^{n-r-1}\rfloor_q}\big) \in k^{n-r},$$

and $\boldsymbol{c}' \in R^{n-r}$ is the componentwise lift of $\boldsymbol{c}$ to R. Since $h = \mathrm{WJP}_{\ell+1,[r]}\big(\boldsymbol{g}(\boldsymbol{x}_{[r]}, \boldsymbol{c}')\big)$ and $f_i(\boldsymbol{x}_{[r]}, \boldsymbol{c}) \equiv g_i(\boldsymbol{x}_{[r]}, \boldsymbol{c}') \pmod{pB}$ for all $i \in [r]$, Theorem 1 implies that $f_1(\boldsymbol{x}_{[r]}, \boldsymbol{c}), \dots, f_r(\boldsymbol{x}_{[r]}, \boldsymbol{c})$ are algebraically independent over k. □

Let $\boldsymbol{f} = (f_1, \dots, f_m) \in A^m$ and let $\varphi\colon A \to A'$ be a k-algebra homomorphism. We say that φ is *faithful to* $\boldsymbol{f}$ if $\mathrm{trdeg}_k(\boldsymbol{f}) = \mathrm{trdeg}_k(\varphi(\boldsymbol{f}))$.

Lemma 45 (Faithful is useful [BMS13, Theorem 14])**.** *Let $\varphi\colon A \to k[\boldsymbol{x}_{[r]}]$ be a k-algebra homomorphism and $\boldsymbol{f} \in A^m$. Then, φ is faithful to $\boldsymbol{f}$ iff $\varphi|_{k[\boldsymbol{f}]}$ is injective.*

Lemma 46. [Sch80, Corollary 1] *Let $f \in k[\boldsymbol{x}_r]$ be a non-zero polynomial and $S \subseteq k$ with $|S| > \deg f$. Then there exists $\boldsymbol{b} \in S^r$ such that $f(\boldsymbol{b}) \neq 0$.*

For an index set $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$ denote its complement by $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$. Define the map $\pi_I\colon k^n \to k^n$, $(a_1, \dots, a_n) \mapsto (a_{i_1}, \dots, a_{i_n})$. We now restate, in more detail, and prove Theorem 3.

Theorem 47 (Hitting-set)**.** *Let $f_1, \dots, f_m \in A$ be s-sparse, of degree at most δ, having transcendence degree at most r, and assume $s, \delta, r \geq 1$. Let $C \in k[y_1, \dots, y_m]$ such that the degree of $C(\boldsymbol{f})$ is bounded by d. Define the subset*

$$\mathcal{H} := \Big\{\pi_I\big(\boldsymbol{b}, c^{\lfloor D^0\rfloor_q}, c^{\lfloor D^1\rfloor_q}, \dots, c^{\lfloor D^{n-r-1}\rfloor_q}\big) \;\Big|\; I \in \tbinom{[n]}{r}, \boldsymbol{b} \in S_1^r, c \in S_2, q \in [N]\Big\}$$

of k^n, where $S_1, S_2 \subseteq k$ are arbitrary subsets of size $d+1$ and $n^2(2\delta rs)^{9r^2s}$, respectively, $D := r\delta^{r+1}+1$, and $N := n^2(2\delta rs)^{7r^2s}$.

If $C(f_1,\dots,f_m) \neq 0$, then there exists $\boldsymbol{a} \in \mathcal{H}$ such that $\big(C(f_1,\dots,f_m)\big)(\boldsymbol{a}) \neq 0$. The set $\mathcal{H}$ can be constructed in $\operatorname{poly}\big((nd)^r, (\delta rs)^{r^2s}\big)$-time.

Proof. We may assume that $f_1,\dots,f_r$ are algebraically independent over k. There exists $I \in \binom{[n]}{r}$ with complement $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$ such that $f_1,\dots,f_r, x_{i_{r+1}},\dots,x_{i_n}$ are algebraically independent. By the definition of $\mathcal{H}$, we may assume that $I = [r]$. By Lemma 44, there exist $c \in S_2$ and a prime $q \in [N]$ such that $f_1(\boldsymbol{x}_{[r]}, \boldsymbol{c}),\dots,f_r(\boldsymbol{x}_{[r]}, \boldsymbol{c}) \in k[\boldsymbol{x}_{[r]}]$ are algebraically independent, where $\boldsymbol{c} = \big(c^{\lfloor D^0 \rfloor_q}, c^{\lfloor D^1 \rfloor_q}, \dots, c^{\lfloor D^{n-r-1} \rfloor_q}\big) \in k^{n-r}$. In other words, this substitution is faithful to $\boldsymbol{f}$. If $C(\boldsymbol{f}) \neq 0$, then Lemma 45 implies $\big(C(\boldsymbol{f})\big)(\boldsymbol{x}_{[r]}, \boldsymbol{c}) \neq 0$. From Lemma 46 we obtain $\boldsymbol{b} \in S_1^r$ such that $\big(C(\boldsymbol{f})\big)(\boldsymbol{b}, \boldsymbol{c}) \neq 0$. Hence, $\boldsymbol{a} := (\boldsymbol{b}, \boldsymbol{c}) \in \mathcal{H}$ satisfies the first assertion. The last one is clear by construction. □

7. Discussion

In this paper we generalized the Jacobian criterion for algebraic independence to any characteristic. The new criterion raises several questions. The most important one from the computational point of view: Can the degeneracy condition in Theorem 1 be efficiently tested? The hardness result for the general degeneracy problem shows that an affirmative answer to that question must exploit the special structure of WJP. Anyhow, for constant or logarithmic p an efficient algorithm for this problem is conceivable.

Even a weaker complexity result, e.g. independence testing in the polynomial hierarchy PH, would be interesting. A careful study of the WJP evaluations at points in the Galois ring might be helpful here.

In §6, we used the explicit Witt-Jacobian criterion to construct faithful homomorphisms which are useful for testing polynomial identities. However, the complexity of this method is exponential in the sparsity of the given polynomials. Can we exploit the special form of the WJP to improve the complexity bound? Or, can we prove a criterion involving only the Jacobian polynomial (which in this case is sparse)? An attempt is Theorem 36.

Acknowledgements. We are grateful to the Hausdorff Center for Mathematics, Bonn, for its kind support. The work was done while the authors were employed there. J.M. would like to thank the Bonn International Graduate School in Mathematics for research funding. N.S. thanks Chandan Saha for explaining his results on finding coefficients of monomials in a circuit [KS11]. We also thank Stefan Mengel for pointing out the hardness of the degeneracy-problem.

References

[AB09] S. Arora and B. Barak, *Computational complexity – a modern approach*, Cambridge University Press, 2009.

[ASSS12] 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*, Proceedings of the 44th ACM Symposium on Theory of Computing (STOC), 2012, `http://eccc.hpi-web.de/report/2011/143/`, pp. 599–614.

[Ber84] S.J. Berkowitz, *On computing the determinant in small parallel time using a small number of processors*, Inform. Process. Lett. **18** (1984), no. 3, 147–150.

[BHLV09] M. Bläser, M. Hardt, R.J. Lipton, and N.K. Vishnoi, *Deterministically testing sparse polynomial identities of unbounded degree*, Inform. Process. Lett. **109** (2009), no. 3, 187–192.

[BMS13] M. Beecken, J. Mittmann, and N. Saxena, *Algebraic Independence and Blackbox Identity Testing*, Inf. Comput. **222** (2013), 2–19, (Conference version in ICALP 2011).

[BS83] W. Bauer and V. Strassen, *The complexity of partial derivatives*, Theoretical Computer Science **22** (1983), no. 3, 317–330.

[CDV06] W. Castryck, J. Denef, and F. Vercauteren, *Computing zeta functions of nondegenerate curves*, Int. Math. Res. Papers **12** (2006), 1–57.

[Del74] P. Deligne, *La conjecture de Weil. I*, Publications Mathématiques de L'IHÉS **43** (1974), 273–307.

[Del80] ———, *La conjecture de Weil. II*, Publications Mathématiques de L'IHÉS **52** (1980), 137–252.

[DF92] E. Delaleau and M. Fliess, *An algebraic interpretation of the structure algorithm with an application to feedback decoupling*, 2nd IFAC Symposium Nonlinear Control Systems Design, 1992, pp. 489–494.

[DGRV11] Z. Dvir, D. Gutfreund, G.N. Rothblum, and S.P. Vadhan, *On approximating the entropy of polynomial mappings*, Innovations in Computer Science (ICS), 2011, pp. 460–475.

[DGW09] Z. Dvir, A. Gabizon, and A. Wigderson, *Extractors and rank extractors for polynomial sources*, Comput. Complex. **18** (2009), no. 1, 1–58, (Conference version in FOCS 2007).

[DV06] J. Denef and F. Vercauteren, *Counting points on C_{ab} curves using Monsky-Washnitzer cohomology*, Finite Fields and their Applications **12** (2006), no. 1, 78–102.

[Dvi09] Z. Dvir, *Extractors for varieties*, Proceedings of the 24th IEEE Conference on Computational Complexity (CCC), 2009, pp. 102–113.

[Dwo60] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, American Journal of Mathematics **82** (1960), no. 3, 631–648.

[Eis95] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 1995.

[FMM12] H. Fournier, G. Malod, and S. Mengel, *Monomials in arithmetic circuits: Complete problems in the counting hierarchy*, Proceeding of the Symposium on Theoretical Aspects of Computer Science (STACS), 2012, `http://arxiv.org/abs/1110.6271`, pp. 362–373.

[For91] K. Forsman, *Constructive commutative algebra in nonlinear control theory*, Ph.D. thesis, Dept. of Electrical Engg., Linköping University, Sweden, 1991.

[Ger07] R. Gerkmann, *Relative rigid cohomology and deformation of hypersurfaces*, Int. Math. Res. Papers (2007), article ID rpm003 (67 pages).

[GG01] P. Gaudry and N. Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494.

[Gro65] A. Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki **9** (1965), 41–55.

[Haz78] M. Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, no. 78, Academic Press Inc., New York, 1978.

[Ill79] L. Illusie, *Complexe de de Rham-Witt et cohomologie cristalline*, Ann. Scient. Éc. Norm. Sup. **12** (1979), no. 4, 501–661.

[Ill94] ———, *Crystalline cohomology*, Proc. Sympos. Pure Math., vol. 55, 1994, Motives (Seattle, WA, 1991), pp. 43–70.

[Jac41] C. G. J. Jacobi, *De determinantibus functionalibus*, J. Reine Angew. Math. **22** (1841), no. 4, 319–359.

[Kal85] K. A. Kalorkoti, *A Lower Bound for the Formula Size of Rational Functions*, SIAM J. Comp. **14** (1985), no. 3, 678–687, (Conference version in ICALP 1982).

[Kay09] N. Kayal, *The Complexity of the Annihilating Polynomial*, Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC), 2009, pp. 184–193.

[Ked01] K. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338.

[Kem96] G. Kemper, *A constructive approach to Noether's problem*, Manuscripta mathematica **90** (1996), 343–363.

[Kob84] N. Koblitz, *P-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Springer-Verlag, 1984.

[KR00] M. Kreuzer and L. Robbiano, *Computational commutative algebra I*, Springer-Verlag, 2000.

[KS11] N. Kayal and C. Saha, *On the sum of square roots of polynomials and related problems*, IEEE Conference on Computational Complexity (CCC), 2011, pp. 292–299.

[Lan84] S. Lang, *Algebra*, 2nd ed., Addison-Wesley, 1984.

[Len91] H.W. Lenstra Jr., *Finding Isomorphisms Between Finite Fields*, Mathematics of Computation **56** (1991), no. 193, 329–347.

[Lub68] S. Lubkin, *A p-adic proof of Weil's conjectures*, Annals of Mathematics **87** (1968), no. 1-2, 105–255.

[L'v84] M.S. L'vov, *Calculation of invariants of programs interpreted over an integrality domain*, Cybernetics and Systems Analysis **20** (1984), 492–499.

[LW08] A. Lauder and D. Wan, *Counting points on varieties over finite fields of small characteristic*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 579–612.

[Men12] S. Mengel, *On degenerate polynomials*, Private communication, 2012.

[Mil80] J. Milne, *Étale cohomology*, Princeton Math. Series, no. 33, Princeton Univ. Press, Princeton, N.J., 1980.

[Mul11] K. D. Mulmuley, *On P vs. NP and geometric complexity theory: Dedicated to Sri Ramakrishna*, J. ACM **58** (2011), no. 2, 5:1–5:26.

[Per27] O. Perron, *Algebra I (Die Grundlagen)*, W. de Gruyter, Berlin, 1927.

[Pło05] A. Płoski, *Algebraic Dependence of Polynomials After O. Perron and Some Applications*, Computational Commutative and Non-Commutative Algebraic Geometry, 2005, pp. 167–173.

[Rag69] R. Raghavendran, *Finite associative rings*, Compositio Mathematica **21** (1969), no. 2, 195–229.

[RS62] J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), no. 1, 64–94.

[Sat00] T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15** (2000), no. 4, 247–270.

[Sax09] N. Saxena, *Progress on Polynomial Identity Testing*, BEATCS (2009), no. 90, 49–79.

[Sch80] J.T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM **27** (1980), no. 4, 701–717.

[Ser79] J.P. Serre, *Local fields*, Graduate Texts in Mathematics, no. 67, Springer-Verlag, New York, 1979.

[Sin80] D. Singmaster, *Divisiblity of binomial and multinomial coefficients by primes and prime powers*, A Collection of Manuscripts Related to the Fibonacci Sequence, 18th Anniversary Volume of the Fibonacci Association (1980), 98–113.

[SS95] M. Shub and S. Smale, *On the intractibility of Hilberts Nullstellensatz and an algebraic version of NP not equal to P?*, Duke Math. J. **81** (1995), 47–54.

[SY10] A. Shpilka and A. Yehudayoff, *Arithmetic Circuits: A survey of recent results and open questions*, Foundations and Trends in Theoretical Computer Science **5** (2010), no. 3-4, 207–388.

[Val79] L.G. Valiant, *The complexity of computing the permanent*, Theoretical Computer Science **8** (1979), no. 2, 189–201.

[Wan03] Z.-X. Wan, *Lectures on finite fields and Galois rings*, World Scientific, Singapore, 2003.

[Wit36] E. Witt, *Zyklische Körper und Algebren der Characteristik p vom Grade p^n*, J. Reine Angew. Math. (1936), no. 176, 126–140.

Hausdorff Center for Mathematics, Endenicher Allee 62, D-53115 Bonn, Germany
E-mail address: johannes.mittmann@hcm.uni-bonn.de

Department of Computer Science & Engineering, IIT Kanpur, 208016 Kanpur, India
E-mail address: nitin@cse.iitk.ac.in

Hochschule Luzern - Technik & Architektur, Technikumstrasse 21, CH-6048 Horw, Switzerland
E-mail address: peter.scheiblechner@hslu.ch