Electronic Colloquium on Computational Complexity, Report No. 14 (2012)

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 $p > 0$, there is no analogous characterization 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 de Rham-Witt complex, which was invented by Illusie (1979) for crystalline cohomology computations, and we deduce a natural 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 apply the new criterion to put the problem of testing algebraic independence in the complexity class $\mathrm{NP}^{\#\mathrm{P}}$ (previously best was PSPACE). Also, we give a modest application to the problem of identity testing in algebraic complexity theory.

1. Introduction

Polynomials $\boldsymbol{f} = \{f_1, \ldots, f_m\} \subset k[x_1, \ldots, x_n]$ are called *algebraically independent* over a field k, if there is no nonzero $F \in k[y_1, \ldots, y_m]$ such that $F(\boldsymbol{f}) = 0$. Otherwise, they are algebraically *dependent* and F is 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.

A priori it is not clear whether, for given *explicit* polynomials, one can test algebraic independence *effectively*. But this is possible – by Gröbner bases, or, by invoking Perron's degree bound on the annihilating polynomial [Per27] and finding a possible F. Now, can this be done *efficiently* (i.e. in polynomial time)? It can be seen that both the above algorithmic techniques take *exponential* time, though the latter gives a PSPACE algorithm. Hence, a different approach is needed for a faster algorithm, and here enters Jacobi [Jac41]. The *Jacobian* of the polynomials $\boldsymbol{f}$ is the matrix $\mathcal{J}_{\boldsymbol{x}}(\boldsymbol{f}) := (\partial_{x_j} f_i)_{m \times n}$, 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 $\boldsymbol{f}$ are dependent, so we always assume $m \leq n$. Now, the Jacobian criterion says: The matrix is of *full* rank over the function field iff $\boldsymbol{f}$ are algebraically independent (assuming zero or large characteristic, see [BMS11]). Since the rank of this matrix can be computed by its *randomized* evaluations [Sch80, DGW09], we immediately get a randomized polynomial time algorithm. The only question left is – What about the 'other' prime characteristic fields? In those situations nothing like the Jacobian criterion

2000 *Mathematics Subject Classification.* 12Y05, 13N05, 14F30, 03D15, 68Q17, 68W30.

ISSN 1433-8092

was known. 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 polynomial time. We do, however, improve the complexity of algebraic independence testing from PSPACE to $\mathrm{NP}^{\#\mathrm{P}}$.

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 $\boldsymbol{f}$ 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 [BMS11, 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 [BMS11].

In this paper, the new avatar of the Jacobian polynomial is called a *Witt-Jacobian*. For polynomials $\boldsymbol{f} = \{f_1, \ldots, f_n\} \subset \mathbb{F}_p[x_1, \ldots, x_n]$ we simply lift the coefficients of $\boldsymbol{f}$ to the *p-adic integers* $\hat{\mathbb{Z}}_p$, to get the *lifted* polynomials $\hat{\boldsymbol{f}} \subset \hat{\mathbb{Z}}_p[x_1, \ldots, x_n]$. Now, for $\ell \geq 1$, the ℓ-th Witt-Jacobian polynomial is $\mathrm{WJP}_\ell := (\hat{f}_1 \cdots \hat{f}_n)^{p^{\ell-1}-1}(x_1 \cdots x_n) \cdot \det \mathcal{J}_{\boldsymbol{x}}(\hat{\boldsymbol{f}})$. Hence, the Witt-Jacobian is just a suitably 'scaled-up' version of the Jacobian polynomial over the integral domain $\hat{\mathbb{Z}}_p$. E.g., if $n = 1, f_1 = x_1^p$, then $\mathrm{WJP}_\ell = (x_1^p)^{p^{\ell-1}-1}(x_1) \cdot (px_1^{p-1}) = px_1^{p^\ell}$ 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, $\hat{f}_1 = px_1^p$ gets mapped to $\mathrm{WJP}_\ell = (px_1^p)^{p^{\ell-1}-1}(x_1) \cdot (p^2 x_1^{p-1}) = p^{(p^{\ell-1}+1)} x_1^{p^\ell}$ 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 in WJP_ℓ carry *precise* information about the algebraic independence of $\boldsymbol{f}$. 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. **Main results.** We need some notation to properly state the results. Denote $\mathbb{Z}^{\geq 0}$ by $\mathbb{N}$. Let $[n] := \{1, \ldots, n\}$, and the set of all r-subsets of $[n]$ be denoted by $\binom{[n]}{r}$. If $I \in \binom{[n]}{r}$, the bold-notation $\boldsymbol{a}_I$ will be a short-hand for a_i, $i \in I$, and we write $\boldsymbol{a}_i$ for $\boldsymbol{a}_{[i]}$. Let $k/\mathbb{F}_p$ be an algebraic field extension, and $\mathrm{W}(k)$ be the ring of Witt vectors of k ($\mathrm{W}(k)$ is just a 'nice' extension of $\hat{\mathbb{Z}}_p$). Define the $\mathbb{F}_p$-algebra $A := k[\boldsymbol{x}_n]$ and the p-adic-algebra $B := \mathrm{W}(k)[\boldsymbol{x}_n]$. For a nonzero $\alpha \in \mathbb{N}^n$ denote by $v_p(\alpha)$ the maximal $v \in \mathbb{N}$ with $p^v | \alpha_i, i \in [n]$. Set $v_p(\mathbf{0}) := \infty$.

[Degeneracy] We call $f \in B$ *degenerate* if the coefficient of $\boldsymbol{x}^\alpha$ in f is divisible by $p^{v_p(\alpha)+1}$ for all $\alpha \in \mathbb{N}^n$. For $\ell \in \mathbb{N}$, f is called $(\ell+1)$-*degenerate* if the coefficient of $\boldsymbol{x}^\alpha$ in f is divisible by $p^{\min\{v_p(\alpha), \ell\}+1}$ for all $\alpha \in \mathbb{N}^n$.

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

[Witt-Jacobian polynomial] Let $\ell\in\mathbb{N}$, $\boldsymbol{g}_r\in B$, and $I\in\binom{[n]}{r}$. We call

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

the $(\ell+1)$-*th Witt-Jacobian polynomial of* $\boldsymbol{g}_r$ *w.r.t.* I.

Theorem 1 (Witt-Jacobian criterion)**.** *Let $\boldsymbol{f}_r\in A$ be of degree at most $\delta\geq 1$, and fix $\ell\geq\lfloor r\log_p\delta\rfloor$. Choose $\boldsymbol{g}_r\in B$ such that $\forall i\in[r], f_i\equiv g_i \pmod{pB}$.*

Then, $\boldsymbol{f}_r$ are algebraically independent over k if and only if there exists $I\in\binom{[n]}{r}$ such that $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g}_r)$ is not $(\ell+1)$-degenerate.

If $p>\delta^r$, this theorem subsumes the Jacobian criterion (choose $\ell=0$). In computational situations we are given $\boldsymbol{f}_r\in A$, say, explicitly. Of course, we can efficiently lift them to $\boldsymbol{g}_r\in B$. But $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g}_r)$ may have *exponential* sparsity (number of nonzero monomials), even for $\ell=1$. This makes it difficult to test the Witt-Jacobian polynomial efficiently for 2-degeneracy. While we improve the basic upper bound of PSPACE for this problem, there is some evidence that the *general* 2-degeneracy problem is outside the polynomial hierarchy [Men12] (Theorem 40).

Theorem 2 (Upper bound)**.** *Given arithmetic circuits $\boldsymbol{C}_r$ computing in A, the problem of testing algebraic independence of polynomials $\boldsymbol{C}_r$ is in the class $\mathrm{NP}^{\#\mathrm{P}}$.*

We are in a better shape when $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g}_r)$ is relatively sparse, which happens, for instance, when $\boldsymbol{f}_r$ have 'sub-logarithmic' sparsity. This case can be applied to the question of *blackbox identity testing*: We are given an arithmetic circuit $C\in\mathbb{F}_p[\boldsymbol{x}_n]$ 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, see [SS95, Sax09, SY10, ASSS12] and the references therein. We apply the Witt-Jacobian criterion to the following case of identity testing.

Theorem 3 (Hitting-set)**.** *Let $\boldsymbol{f}_m\in A$ be s-sparse polynomials of degree $\leq\delta$, transcendence degree $\leq r$, and assume $s,\delta,r\geq 1$. Let $C\in k[\boldsymbol{y}_m]$ such that the degree of $C(\boldsymbol{f}_m)$ is bounded by d. We can construct a (hitting-)set $\mathcal{H}\subset\overline{\mathbb{F}}_p^n$ in $\mathrm{poly}\big((nd)^r,(\delta rs)^{r^2s}\big)$-time such that: If $C(\boldsymbol{f}_m)\neq 0$ then $\exists\boldsymbol{a}\in\mathcal{H},\big(C(\boldsymbol{f}_m)\big)(\boldsymbol{a})\neq 0$.*

An interesting parameter setting is $r=O(1)$ and $s=O(\log d/r^2\log(\delta r\log d))$. In other words, we have an efficient hitting-set, when $\boldsymbol{f}_m$ have constant transcendence degree and sub-logarithmic sparsity. This is new, though, for zero and large characteristic, a much better result is in [BMS11] (thanks to the classical Jacobian).

1.2. **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 $\hat{\mathbb{Z}}_p$ 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* $\Omega^{\cdot}_{\mathrm{W}(A)}$. 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 $\Omega^{\cdot}_{\mathrm{W}(A)}$, and a suitable quotient defines the *de Rham-Witt complex* $\mathrm{W}_\ell \Omega^{\cdot}_A$ of $\mathrm{W}_\ell(A)$-modules, and the *de Rham-Witt pro-complex* $\mathrm{W}_\bullet \Omega^{\cdot}_A$. 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* $\mathrm{E} \subset \Omega^{\cdot}_{B'}$ such that a suitable quotient $\mathrm{E}_\ell := \mathrm{E} / \mathrm{Fil}^\ell \mathrm{E}$ realizes $\mathrm{W}_\ell \Omega^{\cdot}_A$.

To prove Theorem 1 we consider the *Witt-Jacobian differential* $\mathrm{WJ}_\ell := d[f_1] \wedge \cdots \wedge d[f_r] \in \mathrm{W}_\ell \Omega^r_A$. By studying the behavior of $\mathrm{W}_\ell \Omega^r_A$ as we move from A to an extension ring, we show that WJ_ℓ vanishes iff $\boldsymbol{f}_r$ 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 Perron-like Theorem 4 helps to bound ℓ. Next, we realize WJ_ℓ as an element of E^r_ℓ. It is here where the *Witt-Jacobian polynomials* $\mathrm{WJP}_{\ell,I}$ appear and satisfy: $\mathrm{WJ}_\ell = 0$ iff its explicit version is in $\mathrm{Fil}^\ell \mathrm{E}^r$ iff $\mathrm{WJP}_{\ell,I}$ 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 $\mathrm{WJP}_{\ell+1,I}$ has some monomial $\boldsymbol{x}^\alpha$ whose coefficient is *not* divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$. An NP machine can 'guess' I and α, 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 $\mathrm{W}_{\ell+1}(\mathbb{F}_{p^t})$ and the handier *Galois ring* $G_{\ell+1,t}$ [Rag69, Wan03] allows to evaluate $\mathrm{WJP}_{\ell+1,I}$.

The main idea in Theorem 3 is that non-ℓ-degeneracy of $\mathrm{WJP}_{\ell,I}$ is preserved under evaluation of the variables $\boldsymbol{x}_{[n]\setminus I}$. This implies with [BMS11] that algebraically independent $\boldsymbol{f}_r$ can be made r-variate efficiently without affecting the zeroness of $C(\boldsymbol{f}_r)$. The existence of the claimed hitting-sets follows easily from [Sch80].

1.3. **Organization.** In §2 we introduce all necessary preliminaries 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 Theorem 1. In §5 and §6 we prove Theorems 2 resp. 3. To save space we have skipped several worthy references and moved some proofs to Appendix A.

2. Preliminaries

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

2.1. **Algebraic independence and transcendence degree.** Let k be a field and let A be a k-algebra. Elements $\boldsymbol{a}_r \in A$ are called *algebraically independent over* k if $F(\boldsymbol{a}_r) \neq 0$ for all nonzero polynomials $F \in k[\boldsymbol{y}_r]$. For a subset $S \subseteq A$, the *transcendence degree of* S *over* k is defined as $\operatorname{trdeg}_k(S) := \sup\{\#T \mid T \subseteq S \text{ finite and algebraically independent over } k\}$. For an integral domain A we have $\operatorname{trdeg}_k(A) = \operatorname{trdeg}_k(Q(A))$, where $Q(A)$ denotes the quotient field of A.

Now let $k[\boldsymbol{x}] = k[\boldsymbol{x}_n]$ be a polynomial ring over k. We have the following effective criterion for testing algebraic independence, which is stronger than the classical Perron's bound [Per27]. We prove it in §A.2 using [Kem96, Corollary 1.8].

Theorem 4 (Degree bound)**.** *Let k be a field, $\boldsymbol{f}_n \in k[\boldsymbol{x}]$ be algebraically independent, and set $\delta_i := \deg(f_i)$ for $i \in [n]$. Then $[k(\boldsymbol{x}_n) : k(\boldsymbol{f}_n)] \leq \delta_1 \cdots \delta_n$.*

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

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

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 $r \geq 0$, let $\Omega^r_{A/R} := \bigwedge^r \Omega^1_{A/R}$ be the r-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* $d^r\colon \Omega^r_{A/R} \to \Omega^{r+1}_{A/R}$ by $d^r(a\,da_1 \wedge \cdots \wedge da_r) = da \wedge da_1 \wedge \cdots \wedge da_r$ for $a, a_1, \ldots, a_r \in A$. It satisfies $d^{r+1} \circ d^r = 0$ and hence defines a complex of R-modules

$$\Omega^{\cdot}_{A/R}\colon \quad 0 \to A \xrightarrow{d} \Omega^1_{A/R} \xrightarrow{d^1} \cdots \to \Omega^r_{A/R} \xrightarrow{d^r} \Omega^{r+1}_{A/R} \to \cdots$$

called the *de Rham complex* of A over R. This complex also has an R-algebra structure with the exterior product. 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 $r \geq 0$, there is an A'-module isomorphism $R' \otimes_R \Omega^r_{A/R} \to \Omega^r_{A'/R'}$ given by $r' \otimes (da_1 \wedge \cdots \wedge da_r) \mapsto (r' \otimes 1)\, d(1 \otimes a_1) \wedge \cdots \wedge d(1 \otimes a_r)$.*

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 there is a B-module isomorphism $B \otimes_A \Omega^r_{A/R} \to \Omega^r_{B/R}$ given by $b \otimes (da_1 \wedge \cdots \wedge da_r) \mapsto b\, da_1 \wedge \cdots \wedge da_r$. The universal R-derivation $d\colon B \to \Omega^1_{B/R}$ satisfies $d(s^{-1}) = -s^{-2}\,ds$ for $s \in S$.*

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

The Jacobian emerges quite naturally in this setting.

Definition 7. The *Jacobian differential of* $\boldsymbol{a}_r \in A$ is defined as $\mathrm{J}_{A/R}(\boldsymbol{a}_r) := da_1 \wedge \cdots \wedge da_r \in \Omega^r_{A/R}$.

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

The *Jacobian matrix* of $\boldsymbol{f}_m \in k[\boldsymbol{x}]$ is $\mathcal{J}_{\boldsymbol{x}}(\boldsymbol{f}_m) := (\partial_{x_j} f_i)_{i,j} \in k[\boldsymbol{x}]^{m\times n}$. 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 $\mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{f}_m) := (\partial_{x_{j_k}} f_i)_{i,k} \in k[\boldsymbol{x}]^{m\times r}$. A standard computation shows

$$df_1 \wedge \cdots \wedge df_r = \sum\nolimits_I \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{f}_r) \cdot \bigwedge\nolimits_{j\in I} dx_j,$$

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

Lemma 8. *For $\boldsymbol{f}_r \in k[\boldsymbol{x}]$ we have $\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}_r) \neq 0$ if and only if $\mathrm{rk}_{k(\boldsymbol{x})}\, \mathcal{J}_{\boldsymbol{x}}(\boldsymbol{f}_r) = r$.*

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 $[L : k]_{\mathrm{sep}} := [k_{\mathrm{sep}} : k]$ resp. $[L : k]_{\mathrm{insep}} := [L : k_{\mathrm{sep}}]$ are called *separable* resp. *inseparable degree* of L/k. If $L = k_{\mathrm{sep}}$, then L/k is called *separable.* The extension L/k_{sep} is *purely inseparable*, i.e. $a^{p^e} \in k_{\mathrm{sep}}$ for some $e \geq 0$, where $p = \mathrm{char}(k)$.

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 there is an L-vector space isomorphism $L \otimes_k \Omega^r_{k/R} \cong \Omega^r_{L/R}$ 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 $(a_0, a_1, \ldots)$ and is called a *Witt vector* with *coordinates* $a_i \in A$. The ring structure of $\mathrm{W}(A)$ is given by universal polynomials $S_i, P_i \in \mathbb{Z}[x_0, \ldots, x_i, y_0, \ldots, y_i]$ such that

$$a + b = (S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), \ldots), \quad ab = (P_0(a_0, b_0), P_1(a_0, a_1, b_0, b_1), \ldots)$$

for all $a, b \in \mathrm{W}(A)$. The first few terms are $S_0 = x_0 + y_0$, $P_0 = x_0 y_0$,

$$S_1 = x_1 + y_1 - \sum\nolimits_{i=1}^{p-1} p^{-1} \tbinom{p}{i} x_0^i y_0^{p-i}, \quad P_1 = x_0^p y_1 + x_1 y_0^p + p x_1 y_1.$$

The additive and multiplicative identity elements of $\mathrm{W}(A)$ are $(0, 0, 0, \ldots)$ and $(1, 0, 0, \ldots)$, 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

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

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 $[a]_{\leq \ell}$. 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 $\hat{\mathbb{Z}}_p$ 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 $\hat{\mathbb{Z}}_p^{(t)}$ in the unique unramified extension $\mathbb{Q}_p^{(t)}$ of $\mathbb{Q}_p$ of degree t [Kob84].

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

$$\mathrm{F}\colon\ \mathrm{W}(A) \to \mathrm{W}(A), \qquad (a_0, a_1, \dots) \mapsto (a_0^p, a_1^p, \dots). \tag{1}$$

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 $a, b \in \mathrm{W}(A)$. 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.

Let $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ denote the *p-adic valuation* of $\mathbb{Q}$. For a nonzero $q \in \mathbb{Q}$, $v_p(q)$ is defined as the unique integer $v \in \mathbb{Z}$ such that $q = p^v \frac{a}{b}$ for $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$. For tuples $\alpha \in \mathbb{Q}^s$, $s \geq 1$, set $v_p(\alpha) := \min_{1 \leq i \leq s} v_p(\alpha_i) \in \mathbb{Z} \cup \{\infty\}$.

Lemma 10 (Expanding Teichmüller)**.** *Let $A = R[\boldsymbol{a}] = R[\boldsymbol{a}_n]$ be an R-algebra, where R is an $\mathbb{F}_p$-algebra, and let $f = \sum_{i=1}^s c_i \boldsymbol{a}^{\alpha_i} \in A$, where $c_i \in R$ and $\alpha_i \in \mathbb{N}^n$. Then, in $\mathrm{W}_{\ell+1}(A)$, we have the sum over $\boldsymbol{i} \in \mathbb{N}^s$ and $\binom{p^\ell}{\boldsymbol{i}} = \binom{p^\ell}{i_1, \dots, i_s}$:*

$$[f] = \sum_{|\boldsymbol{i}| = p^\ell} p^{-\ell + v_p(\boldsymbol{i})} \tbinom{p^\ell}{\boldsymbol{i}} \cdot \mathrm{V}^{\ell - v_p(\boldsymbol{i})}\, \mathrm{F}^{-v_p(\boldsymbol{i})} \big([c_1 \boldsymbol{a}^{\alpha_1}]^{i_1} \cdots [c_s \boldsymbol{a}^{\alpha_s}]^{i_s}\big). \tag{2}$$

Proof. Note that the RHS w of (2) 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 38, $v_p(\boldsymbol{i}) \leq \ell$ and $p^{-v_p(\boldsymbol{i})} \cdot \boldsymbol{i} \in \mathbb{N}^s$. We have $[f] = \sum_{i=1}^s [c_i \boldsymbol{a}^{\alpha_i}]$ in $\mathrm{W}_1(A)$, so Lemma 37 implies

$$\mathrm{F}^\ell[f] = [f]^{p^\ell} = \big(\textstyle\sum_{i=1}^s [c_i \boldsymbol{a}^{\alpha_i}]\big)^{p^\ell} = \displaystyle\sum_{|\boldsymbol{i}| = p^\ell} \tbinom{p^\ell}{\boldsymbol{i}} \cdot [c_1 \boldsymbol{a}^{\alpha_1}]^{i_1} \cdots [c_s \boldsymbol{a}^{\alpha_s}]^{i_s} \quad \text{in } \mathrm{W}_{\ell+1}(A).$$

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 $M = \bigoplus_{r\geq 0} M^r$ together with an R-linear differential $d\colon M^r \to M^{r+1}$ such that M is graded skew-commutative, i.e., $ab = (-1)^{rs}ba$ for $a \in M^r, b \in M^s$ (in fact, we also assume that $a^2 = 0$ for $a \in M^{2r+1}$), and d satisfies: $d \circ d = 0$ and the graded Leibniz rule $d(ab) = b\,da + (-1)^r a\,db$ for $a \in M^r$, $b \in M$. A $\mathbb{Z}$-dga is simply called *dga*. An important example is the R-dga $\Omega^{\cdot}_{A/R} := \bigoplus_{r\geq 0} \Omega^r_{A/R}$ together with $d := \bigoplus_{r\geq 0} d^r$.

Definition 11. 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 $(\mathrm{V}\colon M^r_\ell \to M^r_{\ell+1})_{r\geq 0,\ell\geq 1}$ such that $\mathrm{R}\,\mathrm{V} = \mathrm{V}\,\mathrm{R}$ and we have

(a) M^0_1 is an $\mathbb{F}_p$-algebra and $M^0_\ell = \mathrm{W}_\ell(M^0_1)$ with the restriction and Verschiebung maps of Witt rings $\mathrm{R}\colon M^0_{\ell+1} \to M^0_\ell$ and $\mathrm{V}\colon M^0_\ell \to M^0_{\ell+1}$,
(b) $\mathrm{V}(\omega\, d\eta) = (\mathrm{V}\,\omega) d\,\mathrm{V}\,\eta$ for all $\omega \in M^r_\ell, \eta \in M^s_\ell$,
(c) $(\mathrm{V}\,w)d[a] = \mathrm{V}([a]^{p-1}w)d\,\mathrm{V}[a]$ for all $a \in M^0_1, w \in M^0_\ell$.

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

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

Lemma 12 (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 there is a natural $\mathrm{W}_\ell(k')$-module isomorphism $\mathrm{W}_\ell(k') \otimes_{\mathrm{W}_\ell(k)} \mathrm{W}_\ell\,\Omega^r_A \cong \mathrm{W}_\ell\,\Omega^r_{A'}$ for all $\ell \geq 1$ and $r \geq 0$.*

Lemma 13 (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 there is a natural $\mathrm{W}_\ell(B)$-module isomorphism $\mathrm{W}_\ell(B) \otimes_{\mathrm{W}_\ell(A)} \mathrm{W}_\ell\,\Omega^r_A \cong \mathrm{W}_\ell\,\Omega^r_B$ for all $\ell \geq 1$ and $r \geq 0$.*

Lemma 14 (Separable extension)**.** *Let L/K be a finite separable field extension of characteristic p. Then there is a natural $\mathrm{W}_\ell(L)$-module isomorphism $\mathrm{W}_\ell(L) \otimes_{\mathrm{W}_\ell(K)} \mathrm{W}_\ell\,\Omega^r_K \cong \mathrm{W}_\ell\,\Omega^r_L$ for all $\ell \geq 1$ and $r \geq 0$.*

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 15. The proofs in [Ill79] show that the isomorphisms of Lemmas 12 – 14 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 $\mathrm{F}\colon\ \mathrm{W}_\bullet\,\Omega^{\cdot}_A \to \mathrm{W}_{\bullet-1}\,\Omega^{\cdot}_A$ such that $\mathrm{F}\,d[a]_{\leq\ell+1} = [a]^{p-1}_{\leq\ell} d[a]_{\leq\ell}$ for all $a \in A$, and $\mathrm{F}\,d\,\mathrm{V} = d$ in $\mathrm{W}_\ell\,\Omega^1_A$ for all $\ell \geq 1$. Define the *canonical filtration* as $\mathrm{Fil}^\ell\,\mathrm{W}_m\,\Omega^{\cdot}_A := \ker\left(\mathrm{R}^{m-\ell}\colon\ \mathrm{W}_m\,\Omega^{\cdot}_A \to \mathrm{W}_\ell\,\Omega^{\cdot}_A\right)$ for $\ell, m \geq 0$.

Now consider a function field $L := k(\boldsymbol{x}_n)$ over a perfect field k. The following fact, proven in §A.2, is quite useful for our differential calculations.

Lemma 16 (Frobenius kernel)**.** *We have* $\ker\left(\mathrm{W}_{\ell+i}\,\Omega^r_L \xrightarrow{\mathrm{F}^i} \mathrm{W}_\ell\,\Omega^r_L\right) \subseteq \mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega^r_L$.

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 $A := k[\boldsymbol{x}] = k[\boldsymbol{x}_n]$. In [Ill79, §I.2] there is an explicit description of $\mathrm{W}_\bullet\,\Omega^{\cdot}_A$ in the case $k = \mathbb{F}_p$. We generalize this construction by invoking Lemma 12 (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 $C := \bigcup_{i\geq 0} K[\boldsymbol{x}^{p^{-i}}]$. For $r \geq 0$, we write $\Omega^r_B := \Omega^r_{B/\,\mathrm{W}(k)}$ and $\Omega^r_C := \Omega^r_{C/K}$. Since the universal derivation $d\colon C \to \Omega^1_C$ satisfies

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

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

$$\omega = \sum\nolimits_I c_I \cdot \bigwedge\nolimits_{j\in I} d\log x_j, \tag{3}$$

where the sum is over all $I \in \binom{[n]}{r}$, the $c_I \in C$ are divisible by $(\prod_{j\in I} x_j)^{p^{-s}}$ for some $s \geq 0$, and $d\log x_j := dx_j/x_j$. The c_I in (3) are called *coordinates* of ω. A form ω is called *integral* if all its coordinates have coefficients in $\mathrm{W}(k)$. We define

$$\mathrm{E}^r := \mathrm{E}^r_A := \{\omega \in \Omega^r_C \mid \text{both } \omega \text{ and } d\omega \text{ are integral}\}.$$

Then, $\mathrm{E} := \bigoplus_{r\geq 0} \mathrm{E}^r$ 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 (1) and sending $x_j^{p^{-i}}$ to $x_j^{p^{-i+1}}$. The map F extends to an automorphism $\mathrm{F}\colon \Omega^r_C \to \Omega^r_C$ of dga's by acting on the coordinates of the differential forms (keeping $d\log x_j$ fixed), and we define $\mathrm{V}\colon \Omega^r_C \to \Omega^r_C$ by $\mathrm{V} := p\,\mathrm{F}^{-1}$. We have $d\,\mathrm{F} = p\,\mathrm{F}\,d$ and $\mathrm{V}\,d = pd\,\mathrm{V}$, 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

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

and hence 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 17 (Explicit forms)**.** *The system* $\mathrm{E}_\bullet$ *is a VDR, isomorphic to* $\mathrm{W}_\bullet\,\Omega^{\cdot}_A$.

Proof. The case $k = \mathbb{F}_p$ follows from [Ill79, Théorème I.2.5]. Lemma 12 yields $\mathrm{W}_\bullet\,\Omega^{\cdot}_A \cong \mathrm{W}_\bullet(k) \otimes_{\mathrm{W}(\mathbb{F}_p)} \mathrm{W}_\bullet\,\Omega^{\cdot}_{\mathbb{F}_p[\boldsymbol{x}]}$ 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 18 ([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 $k[\boldsymbol{x}] = k[\boldsymbol{x}_n]$. In this section we characterize the zeroness of the Jacobian differential which, combined with Lemma 8, gives a criterion on the Jacobian matrix. The proofs for this section can be found in §A.3.

Theorem 19 (Jacobian criterion – abstract)**.** *Let* $\boldsymbol{f}_r \in k[\boldsymbol{x}]$ *be polynomials. Assume that* $k(\boldsymbol{x})$ *is a separable extension of* $k(\boldsymbol{f}_r)$. *Then,* $\boldsymbol{f}_r$ *are algebraically independent over* k *if and only if* $\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}_r) \neq 0$.

As a consequence of Theorem 4, the separability hypothesis of Theorem 19 is satisfied in sufficiently large characteristic.

Lemma 20. *Let $\boldsymbol{f}_m \in k[\boldsymbol{x}]$ have transcendence degree r and maximal degree δ, and assume $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > \delta^r$. Then the extension $k(\boldsymbol{x})/k(\boldsymbol{f}_m)$ is separable.*

4. The Witt-Jacobian criterion

This we prove in two steps. First, an abstract criterion (zeroness of a differential). Second, an explicit criterion (degeneracy of a p-adic polynomial).

4.1. **The Witt-Jacobian differential.**

Definition 21. Let A be an $\mathbb{F}_p$-algebra, $\boldsymbol{a}_r \in A$, and $\ell \geq 1$. We call $\mathrm{WJ}_{\ell,A}(\boldsymbol{a}_r) := d[a_1]_{\leq \ell} \wedge \cdots \wedge d[a_r]_{\leq \ell} \in \mathrm{W}_\ell\, \Omega^r_A$ the *(ℓ-th) Witt-Jacobian differential of $\boldsymbol{a}_r$ in $\mathrm{W}_\ell\, \Omega^r_A$.*

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

Lemma 22. *Let L/k be a finitely generated field extension and let $\ell \geq 1$. Then $\mathrm{W}_\ell\, \Omega^r_L = 0$ if and only if $r > \mathrm{trdeg}_k(L)$.*

Proof. Let $s := \mathrm{trdeg}_k(L)$. Since L is finitely generated over a perfect field, it has a separating transcendence basis $\{a_1, \dots, a_s\} \subset L$. This means that L is a finite separable extension of $K := k(\boldsymbol{a}_s)$. Since $A := k[\boldsymbol{a}_s]$ is isomorphic to a polynomial ring over k, we have $\mathrm{W}_\ell\, \Omega^r_A = 0$ iff $r \geq s+1$ by §2.6. Lemmas 13 and 14 imply $\mathrm{W}_\ell\, \Omega^r_A = 0$ iff $\mathrm{W}_\ell\, \Omega^r_K = 0$ iff $\mathrm{W}_\ell\, \Omega^r_L = 0$. □

Corollary 23. *For an affine k-domain A and $\ell \geq 1$, $\mathrm{W}_\ell\, \Omega^r_A = 0$ iff $r > \mathrm{trdeg}_k(A)$.*

Proof. Apply Lemma 22 to the quotient field of A and use Lemma 13. □

Now let $A := k[\boldsymbol{x}] = k[\boldsymbol{x}_n]$ be a polynomial ring over k.

Lemma 24 (Zeroness)**.** *If $\boldsymbol{f}_r \in A$ are algebraically dependent, then $\mathrm{WJ}_{\ell,A}(\boldsymbol{f}_r) = 0$ for all $\ell \geq 1$.*

Proof. Assume that $\boldsymbol{f}_r$ are algebraically dependent and set $R := k[\boldsymbol{f}_r]$. Corollary 23 implies $\mathrm{W}_\ell\, \Omega^r_R = 0$, thus $\mathrm{WJ}_{\ell,R}(\boldsymbol{f}_r) = 0$. The inclusion $R \subseteq A$ induces a homomorphism $\mathrm{W}_\ell\, \Omega^r_R \to \mathrm{W}_\ell\, \Omega^r_A$, hence $\mathrm{WJ}_{\ell,A}(\boldsymbol{f}_r) = 0$. □

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 25 (Non-zeroness)**.** *If $\boldsymbol{f}_r \in A$ are algebraically independent, then we have $\mathrm{WJ}_{\ell,A}(\boldsymbol{f}_r) \neq 0$ for all $\ell > \log_p [k(\boldsymbol{x}) : k(\boldsymbol{f}_r)]_{\mathrm{insep}}$.*

Proof. It suffices to consider the case $\ell = e+1$, where $e := \log_p [k(\boldsymbol{x}) : k(\boldsymbol{f}_r)]_{\mathrm{insep}}$. By definition of e, there exist $\boldsymbol{f}_{[r+1,n]} \in k(\boldsymbol{x})$ such that $L := k(\boldsymbol{x})$ is algebraic over $K = k(\boldsymbol{f}) := k(\boldsymbol{f}_n)$ with $[L:K]_{\mathrm{insep}} = p^e$. 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 18. Lemma 13 implies $p^e \cdot \mathrm{WJ}_{\ell,L}(\boldsymbol{x}) \neq 0$. We conclude

$$\mathrm{WJ}_{\ell,L}(x_1^{q_1}, \ldots, x_n^{q_n}) = p^e \cdot [x_1]^{q_1-1} \cdots [x_n]^{q_n-1} \cdot \mathrm{WJ}_{\ell,L}(\boldsymbol{x}) \neq 0, \tag{4}$$

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 want to show inductively for $j = 0, \ldots, n-1$ that the induced map $\Psi_j \colon \mathrm{W}_\ell \, \Omega^n_{K_j} \to \mathrm{W}_\ell \, \Omega^n_L$ satisfies

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

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 10, every element $\overline{\omega} \in \mathrm{W}_\ell \, \Omega^n_R$ is a $\mathbb{Z}$-linear combination of products of elements of the form $\mathrm{V}^i[c\boldsymbol{f}^\alpha]$ and $d\,\mathrm{V}^i[c\boldsymbol{f}^\alpha]$ for some $i \in [0, \ell-1]$, $c \in k$, and $\alpha \in \mathbb{N}^n$. Wlog., let $\overline{\omega} = \mathrm{V}^{i_0}[c_0\boldsymbol{f}^{\alpha_0}] \cdot d\,\mathrm{V}^{i_1}[c_1\boldsymbol{f}^{\alpha_1}] \wedge \cdots \wedge d\,\mathrm{V}^{i_n}[c_n\boldsymbol{f}^{\alpha_n}]$. Let $\omega \in \mathrm{W}_m \, \Omega^n_R$ be a lift of $\overline{\omega}$ for m sufficiently large (say $m = 2\ell$). Using $\mathrm{F}\,d\,\mathrm{V} = d$ and $\mathrm{F}\,d[w] = [w]^{p-1}d[w]$ for $w \in R$, we deduce $\mathrm{F}^\ell \omega = g \cdot d[c_1\boldsymbol{f}^{\alpha_1}] \wedge \cdots \wedge d[c_n\boldsymbol{f}^{\alpha_n}]$ for some $g \in \mathrm{W}_{m-\ell}(R)$. 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 $g' \in \mathrm{W}_{m-\ell}(R)$. Since $\mathrm{WJ}_{\ell,L}(\boldsymbol{f}) = 0$ by assumption, we obtain $\mathrm{F}^\ell \Psi(\omega) = \Psi(\mathrm{F}^\ell \omega) \in \mathrm{Fil}^\ell \mathrm{W}_{m-\ell} \, \Omega^n_L$, hence $\Psi(\omega) \in \mathrm{Fil}^\ell \mathrm{W}_m \, \Omega^n_L$ by Lemma 16. This shows $\Psi(\overline{\omega}) = 0$, so Ψ is zero. Lemmas 13 and 14 imply that the map Ψ_0 is zero, proving the claim 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 $a_{j+1}, \ldots, a_n \in K_j$. Since $K_j = K_{j-1}[x_j]$, we may assume by Lemma 10 that $\overline{\omega} = d[x_1^{q_1}] \wedge \cdots \wedge d[x_j^{q_j}] \wedge d\,\mathrm{V}^{i_{j+1}}[c_{j+1}x_j^{\alpha_{j+1}}] \wedge \cdots \wedge d\,\mathrm{V}^{i_n}[c_n x_j^{\alpha_n}]$ with $i_{j+1}, \ldots, i_n \in [0, \ell-1]$, $c_{j+1}, \ldots, c_n \in K_{j-1}$, and $\alpha_{j+1}, \ldots, \alpha_n \geq 0$. Let $\omega \in \mathrm{W}_m \, \Omega^n_{K_j}$ be a lift of $\overline{\omega}$ for m sufficiently large (say $m = 2\ell$). 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 $g \in \mathrm{W}_{m-\ell}(K_j)$, 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 $g' \in \mathrm{W}_{m-\ell}(K_j)$. Since $x_1^{q_1}, \ldots, x_j^{q_j}, c_{j+1}, \ldots, c_n \in K_{j-1}$, we obtain $\mathrm{F}^\ell \Psi_j(\omega) = \Psi_j(\mathrm{F}^\ell \omega) \in \mathrm{Fil}^\ell \mathrm{W}_{m-\ell} \, \Omega^n_L$ by induction, hence $\Psi_j(\omega) \in \mathrm{Fil}^\ell \mathrm{W}_m \, \Omega^n_L$ by Lemma 16. This shows $\Psi_j(\overline{\omega}) = 0$, finishing the proof of the claim.

For $j = n-1$ and $a_n = x_n^{q_n} \in K_{n-1}$ the claim implies $\mathrm{WJ}_{\ell,L}(x_1^{q_1}, \ldots, x_n^{q_n}) = 0$ which is contradicting (4). Therefore, $\mathrm{WJ}_{\ell,L}(\boldsymbol{f}_n) \neq 0$, hence $\mathrm{WJ}_{\ell,L}(\boldsymbol{f}_r) \neq 0$. Lemma 13 implies $\mathrm{WJ}_{\ell,A}(\boldsymbol{f}_r) \neq 0$. □

Remark 26. Lemma 25 is tight in the case $f_i := x_i^{p^{e_i}}$ for $i \in [r]$.

Theorem 27 (Witt-Jacobian criterion – abstract)**.** *Let $\boldsymbol{f}_r \in A$ be of degree at most $\delta \geq 1$ and fix $\ell > \lfloor r \log_p \delta \rfloor$. Then, $\boldsymbol{f}_r$ are algebraically independent over k if and only if $\mathrm{WJ}_{\ell,A}(\boldsymbol{f}_r) \neq 0$.*

Proof. Let $\boldsymbol{f}_{[r+1,n]} \subseteq \boldsymbol{x}$ be a transcendence basis of $k(\boldsymbol{x})/k(\boldsymbol{f}_r)$. Then $[k(\boldsymbol{x}) : k(\boldsymbol{f}_r)]_{\mathrm{insep}} \leq [k(\boldsymbol{x}) : k(\boldsymbol{f}_n)]_{\mathrm{insep}} \leq [k(\boldsymbol{x}) : k(\boldsymbol{f}_n)] \leq \delta^r$ by Theorem 4. The assertion follows from Lemmas 24 and 25. □

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, $A = k[\boldsymbol{x}] = k[\boldsymbol{x}_n]$, $B = \mathrm{W}(k)[\boldsymbol{x}]$, $K = Q(\mathrm{W}(k))$, and $C = \bigcup_{r \geq 0} K[\boldsymbol{x}^{p^{-r}}]$. Recall that $\mathrm{E} = \mathrm{E}_A$ is a subalgebra of $\Omega^\cdot_C$ containing $\Omega^\cdot_B$, 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 28 (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 17. Then we have $\tau([f]_{\leq \ell+1}) = (\mathrm{F}^{-\ell} g)^{p^\ell}$.*

Proof. Write $g = \sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i}$, where $c_i \in \mathrm{W}(k)$ and $\alpha_i \in \mathbb{N}^n$. By assumption, we have $[f] = \sum_{i=1}^{s} c_i[\boldsymbol{x}^{\alpha_i}]$ in $\mathrm{W}_1(A)$. By Lemma 37, we obtain

$$\mathrm{F}^\ell[f] = [f]^{p^\ell} = \left(\textstyle\sum_{i=1}^{s} c_i[\boldsymbol{x}^{\alpha_i}]\right)^{p^\ell} = \sum_{|\boldsymbol{i}|=p^\ell} \tbinom{p^\ell}{\boldsymbol{i}} \cdot \boldsymbol{c}^{\boldsymbol{i}}[\boldsymbol{x}^{\alpha_1}]^{i_1}\cdots[\boldsymbol{x}^{\alpha_s}]^{i_s} \quad \text{in } \mathrm{W}_{\ell+1}(A).$$

As in the proof of Lemma 10, this implies

$$[f] = \sum_{|\boldsymbol{i}|=p^\ell} p^{-\ell+v_p(\boldsymbol{i})}\tbinom{p^\ell}{\boldsymbol{i}} \cdot \mathrm{V}^{\ell-v_p(\boldsymbol{i})}\,\mathrm{F}^{-v_p(\boldsymbol{i})}\big(c_1^{i_1}[\boldsymbol{x}^{\alpha_1}]^{i_1}\cdots c_s^{i_s}[\boldsymbol{x}^{\alpha_s}]^{i_s}\big) \quad \text{in } \mathrm{W}_{\ell+1}(A).$$

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 $\tau\,\mathrm{V} = \mathrm{V}\,\tau$ and $\tau([x_i]) = x_i$, we conclude

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

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 $\beta \in G$ are of the form $c\boldsymbol{x}^\beta$ for some $c \in K$. This grading extends to Ω_C by defining $\omega \in \Omega^r_C$ to be homogeneous of degree $\beta \in G$ if its coordinates in (3) are. We denote the homogeneous part of ω of degree β by $(\omega)_\beta$.

Lemma 29 (Explicit filtration [Ill79, Proposition I.2.12])**.** *Let $\ell \geq 0$ and let $\beta \in G$. Define $\nu(\ell+1,\beta) := \min\big\{\max\{0, \ell+1+v_p(\beta)\}, \ell+1\big\} \in [0, \ell+1]$. Then $(\mathrm{Fil}^{\ell+1}\mathrm{E})_\beta = p^{\nu(\ell+1,\beta)}(\mathrm{E})_\beta$.*

The following lemma shows how degeneracy is naturally related to ν. A proof is given in §A.4.

Lemma 30. *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 $\boldsymbol{x}^\beta$ in $\mathrm{F}^{-\ell} f$ is divisible by $p^{\nu(\ell+1,\beta)}$ for all $\beta \in G$.*

Lemma 31 (Zeroness vs. degeneracy)**.** *Let $\ell \geq 0$, let $\boldsymbol{g}_r \in B \subset \mathrm{E}^0$ be polynomials, and define $\omega := d(\mathrm{F}^{-\ell} g_1)^{p^\ell} \wedge \cdots \wedge d(\mathrm{F}^{-\ell} g_r)^{p^\ell} \in \mathrm{E}^r$. Then $\omega \in \mathrm{Fil}^{\ell+1}\mathrm{E}^r$ if and only if $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{g}_r)$ is $(\ell+1)$-degenerate for all $I \in \binom{[n]}{r}$.*

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

$$dg_1 \wedge \cdots \wedge dg_r = \sum\nolimits_I \left(\textstyle\prod_{j\in I} x_j\right) \cdot \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{g}_r) \cdot \textstyle\bigwedge_{j\in I} d\log x_j,$$

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

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

By Lemma 29, we have $\mathrm{Fil}^{\ell+1}\mathrm{E}^r = \bigoplus_{\beta\in G}\big(\mathrm{Fil}^{\ell+1}\mathrm{E}^r\big)_\beta = \bigoplus_{\beta\in G} p^{\nu(\ell+1,\beta)}\big(\mathrm{E}^r\big)_\beta$, and we conclude

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

where we used Lemma 30. □

Proof of Theorem 1. Using Lemmas 28 and 31, this follows from Theorem 27. □

5. Independence testing: Proving Theorem 2

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].

For detailed proofs of the following two lemmas see §A.5.

Lemma 32 (Interpolation)**.** *Let $f \in G_{\ell+1,t}[z]$ be a polynomial of degree $D < p^t - 1$ and let $\xi \in G_{\ell+1,t}$ be a primitive (p^t-1)-th root of unity. Then*

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

This exponentially large sum can be evaluated using a #P-oracle [Val79].

Lemma 33 (#P-oracle)**.** *Given $G_{\ell+1,t}$, a primitive (p^t-1)-th root of unity $\xi \in G_{\ell+1,t}$, an arithmetic circuit C over $G_{\ell+1,t}[z]$ of degree $D < p^t-1$ and $d\in[0,D]$. The* $\mathrm{coeff}(z^d, C)$ *can be computed in* $\mathrm{FP}^{\#\mathrm{P}}$ *(with a single #P-oracle query).*

Proof of Theorem 2. We set up some notation. Let $s := \mathrm{size}(\boldsymbol{C}_r)$ be the size of the input circuits. Then $\delta := 2^{s^2}$ is an upper bound for their degrees. Set $\ell := \lfloor r\log_p \delta\rfloor$ and $D := r\delta^{r+1}+1$. The constants of $\boldsymbol{C}_r$ 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 $\boldsymbol{C}_r$.

(1) Using non-determinism, guess $I \in \binom{[n]}{r}$ and $\alpha\in[0,D-1]^n$.

(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 $x^{p^t-1}-1$, $\overline{h} := h \pmod p$ 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 $\xi := x + (f)$.
(3) By lifting the constants of $\boldsymbol{C}_r$ from k to $G_{\ell+1,t}$, compute circuits $\boldsymbol{C}'_r$ over $G_{\ell+1,t}[\boldsymbol{x}]$ such that $\boldsymbol{C}'_i \equiv \boldsymbol{C}_i \pmod p$. Furthermore, compute a circuit C for $\mathrm{WJP}_{\ell+1,I}(\boldsymbol{C}'_r)$ 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 $\boldsymbol{x}^\alpha$ is mapped to z^d, 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 $p^{\min\{v_p(\alpha),\ell\}+1}$, 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 the section. To obtain C in polynomial time, we use [BS83] and [Ber84] for computing partial derivatives and the determinant, and repeated squaring for the high power.

We have $\deg(C) \le r\delta(p^\ell-1) + r + r(\delta-1) \le r\delta^{r+1} < D$, 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 33. Altogether we get an $\mathrm{NP}^{\#\mathrm{P}}$-algorithm. □

6. Identity testing: Proving Theorem 3

The aim of this section is to construct an efficiently computable hitting-set for poly-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. We use some lemmas from §A.6.

As before, we consider a polynomial ring $A = k[\boldsymbol{x}]$ over an algebraic extension k of $\mathbb{F}_p$. Furthermore, 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 34 (Variable reduction)**.** *Let $\boldsymbol{f}_r \in A$ be polynomials of sparsity at most $s \ge 1$ and degree at most $\delta \ge 1$. Assume that $\boldsymbol{f}_r$, $\boldsymbol{x}_{[r+1,n]}$ are algebraically independent. Let $D := r\delta^{r+1}+1$ and let $S \subseteq k$ be of size $|S| = n^2(2\delta rs)^{4r^2s}\lceil \log_2 D\rceil^2 D$.*

Then there exist $c \in S$ and a prime $2 \le q \le n^2(2\delta rs)^{4r^2s}\lceil \log_2 D\rceil^2$ 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 $\boldsymbol{c} = \left(c^{\lfloor D^0 \rfloor_q}, c^{\lfloor D^1 \rfloor_q}, \dots, c^{\lfloor D^{n-r-1} \rfloor_q}\right) \in k^{n-r}$.

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

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

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

$$g' := (g_1 \cdots g_r)^{p^\ell-1}(x_1 \cdots x_r) \cdot \det \mathcal{J}_{\boldsymbol{x}_r}(\boldsymbol{g}_r) \in B.$$

Then $g = (x_{r+1}\cdots x_n)^{p^\ell} g'$, and g' is not $(\ell+1)$-degenerate by Lemma 44. Furthermore, we have $\deg(g') \le r\delta(p^\ell - 1) + r + r(\delta-1) \le r\delta^{r+1} < D$ and

$$\operatorname{sp}(g') \le \binom{s + (p^\ell - 1) - 1}{s-1}^r \cdot r! s^r \le \bigl(s + \delta^r\bigr)^{rs} \cdot (rs)^r \le (2\delta r s)^{2r^2 s}.$$

By Lemma 42, there exist $c \in S$ and a prime $q \le n^2 (2\delta r s)^{4r^2 s} \lceil \log_2 D\rceil^2$ such that $h := g'(\boldsymbol{x}_r, \boldsymbol{c}') \in R[\boldsymbol{x}_r]$ is not $(\ell+1)$-degenerate, where

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

and $\boldsymbol{c}' \in R^{n-r}$ is the componentwise lift of $\boldsymbol{c}$ to R. Since $h = \mathrm{WJP}_{\ell+1,[r]}\bigl(g_1(\boldsymbol{x}_r, \boldsymbol{c}'), \ldots, g_r(\boldsymbol{x}_r, \boldsymbol{c}')\bigr)$ 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 $f_1(\boldsymbol{x}_r, \boldsymbol{c}), \ldots, f_r(\boldsymbol{x}_r, \boldsymbol{c})$ are algebraically independent over k. $\square$

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 $\pi_I \colon k^n \to k^n$, $(a_1, \ldots, a_n) \mapsto (a_{i_1}, \ldots, a_{i_n})$. We now restate, in more detail, and prove Theorem 3.

Theorem 35 (Hitting-set)**.** *Let $\boldsymbol{f}_m \in A$ be s-sparse, of degree at most δ, having transcendence degree at most r, and assume $s, \delta, r \ge 1$. Let $C \in k[\boldsymbol{y}_m]$ such that the degree of $C(\boldsymbol{f}_m)$ is bounded by d. Define the subset*

$$\mathcal{H} := \Bigl\{ \pi_I\bigl(\boldsymbol{b}, c^{\lfloor D^0 \rfloor_q}, c^{\lfloor D^1 \rfloor_q}, \ldots, c^{\lfloor D^{n-r-1} \rfloor_q}\bigr) \bigm| I \in \tbinom{[n]}{r},\, \boldsymbol{b} \in S_1^r,\, c \in S_2,\, q \in [N] \Bigr\}$$

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

If $C(\boldsymbol{f}_m) \ne 0$ then there exists $\boldsymbol{a} \in \mathcal{H}$ such that $\bigl(C(\boldsymbol{f}_m)\bigr)(\boldsymbol{a}) \ne 0$. The set $\mathcal{H}$ can be constructed in $\operatorname{poly}\bigl((nd)^r, (\delta r s)^{r^2 s}\bigr)$*-time.*

Proof. We may assume that $\boldsymbol{f}_r$ are algebraically independent over k There exists $I = \{i_1 < \cdots < i_r\} \subseteq [n]$ with complement $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$ such that $\boldsymbol{f}_r$, $\boldsymbol{x}_{[n]\setminus I}$ are algebraically independent. By the definition of $\mathcal{H}$, we may assume that $I = [r]$. By Lemma 34, there exist $c \in S_2$ and a prime $q \in [N]$ such that $f_1(\boldsymbol{x}_r, \boldsymbol{c}), \ldots, f_r(\boldsymbol{x}_r, \boldsymbol{c}) \in k[\boldsymbol{x}_r]$ are algebraically independent, where $\boldsymbol{c} = \bigl(c^{\lfloor D^0 \rfloor_q}, c^{\lfloor D^1 \rfloor_q}, \ldots, c^{\lfloor D^{n-r-1} \rfloor_q}\bigr) \in k^{n-r}$. If $C(\boldsymbol{f}_m) \ne 0$, then Lemma 45 implies that $\bigl(C(\boldsymbol{f}_m)\bigr)(\boldsymbol{x}_r, \boldsymbol{c}) \ne 0$. From Lemma 46 we obtain $\boldsymbol{b} \in S_1$ such that $\bigl(C(\boldsymbol{f}_m)\bigr)(\boldsymbol{b}, \boldsymbol{c}) \ne 0$. Thus, $\boldsymbol{a} := (\boldsymbol{b}, \boldsymbol{c}) \in \mathcal{H}$ satisfies the first assertion. The last one is clear by construction. $\square$

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.

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)? (See an attempt in Theorem 36.)

Acknowledgements. We are grateful to the Hausdorff Center for Mathematics, Bonn, for its kind support. 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

[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/.

[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.

[BMS11] M. Beecken, J. Mittmann, and N. Saxena, *Algebraic Independence and Blackbox Identity Testing*, 38th International Colloquium on Automata, Languages and Programming (ICALP), vol. 6756, 2011, pp. 137–148.

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

[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).

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

[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.

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

[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.

[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.
[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.
[L'v84] M.S. L'vov, *Calculation of invariants of programs interpreted over an integrality domain*, Cybernetics and Systems Analysis **20** (1984), 492–499.
[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.
[Per27] O. Perron, *Algebra I (Die Grundlagen)*, W. de Gruyter, Berlin, 1927.
[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.
[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.

Appendix A. Missing theorems, lemmas and proofs

In this appendix we present statements and proofs that did not fit in the main part due to space constraints.

A.1. Degeneracy of the p-adic Jacobian.

Theorem 36 (Necessity)**.** *Let $\boldsymbol{f}_r \in A$ and $\boldsymbol{g}_r \in B$ such that $\forall i \in [r], f_i \equiv g_i \pmod{pB}$. If $\boldsymbol{f}_r$ are algebraically dependent, then for any r variables $\boldsymbol{x}_I$, $I \in \binom{[n]}{r}$, the p-adic polynomial $\hat{J}_{\boldsymbol{x}_I}(\boldsymbol{g}_r) := \left(\prod_{j\in I} x_j\right) \cdot \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{g}_r)$ is degenerate. The converse does not hold.*

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

Assume that $f_1, \ldots, f_r$ are algebraically dependent and set $R := k[f_1, \ldots, f_r]$. Corollary 23 implies $\mathrm{W}_{\ell+1}\,\Omega^r_R = 0$, thus γ vanishes in $\mathrm{W}_{\ell+1}\,\Omega^r_R$. The inclusion $R \subseteq A$ induces a homomorphism $\mathrm{W}_{\ell+1}\,\Omega^r_R \to \mathrm{W}_{\ell+1}\,\Omega^r_A$, hence γ vanishes in $\mathrm{W}_{\ell+1}\,\Omega^r_A$ itself.

As in the proof of Lemma 28, we first make $\mathrm{V}^\ell[f]_{\le \ell+1}$ explicit. Let $g \in B$ such that $f \equiv g \pmod{pB}$, and write $g = \sum_{i=1}^s c_i \boldsymbol{x}^{\alpha_i}$, where $c_i \in \mathrm{W}(k)$ and

$\alpha_i \in \mathbb{N}^n$ for $i \in [s]$. Note that $\mathrm{F}^\ell(\mathrm{V}^\ell[f]_{\leq \ell+1}) = p^\ell [f]_{\leq \ell+1}$. Also, for $w := \mathrm{V}^\ell(\sum_{i=1}^s c_i[\boldsymbol{x}^{\alpha_i}]) \in \mathrm{W}_{\ell+1}(A)$ we have $\mathrm{F}^\ell(w) = p^\ell \sum_{i=1}^s c_i[\boldsymbol{x}^{\alpha_i}]$. Since by assumption $([f] - \sum_{i=1}^s c_i[\boldsymbol{x}^{\alpha_i}]) \in \mathrm{V}\,\mathrm{W}(A)$, we get $p^\ell([f] - \sum_{i=1}^s c_i[\boldsymbol{x}^{\alpha_i}]) \in \mathrm{V}^{\ell+1}\,\mathrm{W}(A)$. This proves $\mathrm{F}^\ell(\mathrm{V}^\ell[f]_{\leq \ell+1}) = \mathrm{F}^\ell(w)$. The injectivity of F^ℓ implies $\mathrm{V}^\ell[f]_{\leq \ell+1} = w$. Finally, we can apply $\tau\colon\ \mathrm{W}_{\ell+1}(A) \to \mathrm{E}^0_{\ell+1}$ to get: $\tau(\mathrm{V}^\ell[f]_{\leq \ell+1}) = \tau(w) = \mathrm{V}^\ell(g)$.

Thus, we have the explicit condition $\gamma' := \tau(\gamma) = d\,\mathrm{V}^\ell(g_1) \wedge \cdots \wedge d\,\mathrm{V}^\ell(g_r) \in \mathrm{Fil}^{\ell+1}\,\mathrm{E}^r$. Now we continue to calculate γ' much like in Lemma 31. 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 $\mathrm{F}^\ell\,d(V^\ell g_i) = dg_i$, hence $\mathrm{F}^\ell\,\gamma' = dg_1 \wedge \cdots \wedge dg_r$. Furthermore,

$$dg_1 \wedge \cdots \wedge dg_r = \sum\nolimits_I \left(\prod\nolimits_{j \in I} x_j\right) \cdot \det \mathcal{J}_{\boldsymbol{x}_I}(\boldsymbol{g}_r) \cdot \bigwedge\nolimits_{j \in I} d \log x_j,$$

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

$$\gamma' = \sum\nolimits_I \mathrm{F}^{-\ell}\,\hat{J}_{\boldsymbol{x}_I}(\boldsymbol{g}_r) \cdot \bigwedge\nolimits_{j \in I} d \log x_j,$$

and this representation is unique.

As in the proof of Lemma 31 we conclude

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

where we used Lemma 30. Since our ℓ is large enough, this is finally equivalent to the degeneracy of $\hat{J}_{\boldsymbol{x}_I}(\boldsymbol{g}_r)$. 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 $\hat{J}_{\boldsymbol{x}_2}(x_1^p, x_2^p) = p^2 x_1^p x_2^p$. This is clearly degenerate, but f_1, f_2 are algebraically independent. □

A.2. **Proofs for Section 2.** For a polynomial f in some polynomial ring $k[\boldsymbol{x}_n]$ and a vector $\boldsymbol{w} \in \mathbb{N}^n$, the *weighted-degree* is defined as

$$\max\Big\{\sum_{i=1}^n w_i e_i \mid \boldsymbol{e} \in \mathbb{N}^n, \mathrm{coeff}(\boldsymbol{x}^{\boldsymbol{e}}, f) \neq 0\Big\}.$$

For the following proof we need to define a map $\mu_{\boldsymbol{w}} : k[\boldsymbol{x}] \to k[\boldsymbol{x}]$ that extracts the *highest weighted-degree part*. I.e. for $f \in k[\boldsymbol{x}]$ of weighted-degree δ, $\mu_{\boldsymbol{w}}(f)$ is the sum of the weighted-degree-δ terms in f. E.g. $\mu_{(1,3)}(2x_1^2 + 3x_2) = 3x_2$. Note that $\mu_{\boldsymbol{w}}(f) = 0$ iff $f = 0$.

Theorem 4 (restated). *Let k be a field, $\boldsymbol{f}_n \in k[\boldsymbol{x}]$ be algebraically independent, and set $\delta_i := \deg(f_i)$ for $i \in [n]$. Then $[k(\boldsymbol{x}_n) : k(\boldsymbol{f}_n)] \leq \delta_1 \cdots \delta_n$.*

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

Firstly, $z, \boldsymbol{g}_n$ are algebraically independent over k. Otherwise, there is an irreducible polynomial $H \in k[\boldsymbol{y}_{[0,n]}]$ such that $H(z, \boldsymbol{g}_n) = 0$. Evaluation at $z = 1$ yields $H(1, \boldsymbol{f}_n) = 0$. The algebraic independence of $\boldsymbol{f}_n$ implies $H(1, \boldsymbol{y}_n) = 0$, hence $(y_0 - 1) | H(\boldsymbol{y}_{[0,n]})$ by the Gauss Lemma. This contradicts the irreducibility of H.

Thus, $d' := [k(z, \boldsymbol{x}_n) : k(z, \boldsymbol{g}_n)]$ is finite. We will now compare it with $[k(\boldsymbol{x}_n) : k(\boldsymbol{f}_n)] =: d$. Denote the vector spaces $k(z, \boldsymbol{x}_n)$ over $k(z, \boldsymbol{g}_n)$ by $\mathbb{V}'$, and $k(\boldsymbol{x}_n)$ over $k(\boldsymbol{f}_n)$ by $\mathbb{V}$. Each of these vector spaces admits a finite basis consisting of monomials in $\boldsymbol{x}_n$ only.

Suppose $S = \{\boldsymbol{x}^\alpha | \alpha \in I\}$, for some $I \subset \mathbb{N}^n$, is a basis of $\mathbb{V}'$. Assume that

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

with some $h_\alpha \in k[\boldsymbol{y}_n]$. By *homogenizing* each term in this equation with respect to the same sufficiently large degree, we obtain $h'_\alpha \in k[\boldsymbol{y}_{[0,n]}]$ such that

$$\sum_{\alpha\in I} h'_\alpha(z, \boldsymbol{g}_n) \cdot \boldsymbol{x}^\alpha = 0.$$

Since the $\boldsymbol{x}^\alpha$ are linearly independent over $k(z, \boldsymbol{g}_n)$, we conclude $h'_\alpha(z, \boldsymbol{g}_n) = 0$, hence $h_\alpha(\boldsymbol{f}_n) = 0$ for all α. Thus, $d' \leq d$.

Suppose $S = \{\boldsymbol{x}^\alpha | \alpha \in I\}$, for $I \subset \mathbb{N}^n$, is a basis of $\mathbb{V}$. If they are linearly dependent in $\mathbb{V}'$, then there exist $h_\alpha \in k[\boldsymbol{y}_{[0,n]}]$ such that

$$\sum_{\alpha\in I} h_\alpha(z, \boldsymbol{g}_n) \cdot \boldsymbol{x}^\alpha = 0 \tag{5}$$

is a nontrivial equation. Let $\mathbf{1} := (1, \dots, 1) \in \mathbb{N}^{n+1}$, $\boldsymbol{w} := (1, \boldsymbol{\delta}_n)$ and $h'_\alpha := \mu_{\boldsymbol{w}}(h_\alpha) \in k[\boldsymbol{y}_{[0,n]}]$. Applying $\mu_{\mathbf{1}}$ on (5) we get for some nonempty $J \subseteq I$ a nontrivial equation:

$$\sum_{\alpha\in J} h'_\alpha(z, \boldsymbol{g}_n) \cdot \boldsymbol{x}^\alpha = 0.$$

Since $h'_\alpha(z, \boldsymbol{g}_n)$ is homogeneous and nonzero, it cannot be divisible by $(z-1)$. Thus, $h'_\alpha(1, \boldsymbol{f}_n) \neq 0$ and we get a nontrivial equation in $\mathbb{V}$:

$$\sum_{\alpha\in J} h'_\alpha(1, \boldsymbol{f}_n) \cdot \boldsymbol{x}^\alpha = 0.$$

This contradicts the choice of I. Hence, $d \leq d'$.

Finally, $d = d'$ and from [Kem96, Corollary 1.8] we know $d' \leq \delta_1 \cdots \delta_n$. □

Now we use the notation of §2.4.

Lemma 37 (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 $\ell \geq 0$.*

Proof. We use induction on ℓ, where the base case $\ell = 0$ holds by assumption. Now let $\ell \geq 1$. By 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 $a^{p^\ell} - b^{p^\ell} = \big(b^{p^{\ell-1}} + c\big)^p - b^{p^\ell} = c^p + \sum_{i=1}^{p-1} p^{-1}\binom{p}{i}\,\mathrm{V}\,\mathrm{F}\big(b^{p^{\ell-1}(p-i)}c^i\big) \in \mathrm{V}^{\ell+1}\,\mathrm{W}(A)$. □

Lemma 38 (Multinomials [Sin80, Theorem 32])**.** *Let $\ell, s \geq 1$ and let $\alpha \in \mathbb{N}^s$ such that $|\alpha| = p^\ell$. Then $p^{\ell - v_p(\alpha)}$ divides the multinomial coefficient $\binom{p^\ell}{\alpha} := \binom{p^\ell}{\alpha_1, \dots, \alpha_s}$.*

Now we use the notation of §2.5 and consider a function field $L := k(\boldsymbol{x}_n)$ over a perfect field k.

Lemma 16 (restated). *We have* $\ker\big(\mathrm{W}_{\ell+i}\,\Omega_L^r \xrightarrow{\mathrm{F}^i} \mathrm{W}_\ell\,\Omega_L^r\big) \subseteq \mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega_L^r$.

Proof. Let $\omega \in \mathrm{W}_{\ell+i}\,\Omega_L^r$ with $\mathrm{F}^i\,\omega = 0$. Applying $\mathrm{V}^i\colon \mathrm{W}_\ell\,\Omega_L^r \to \mathrm{W}_{\ell+i}\,\Omega_L^r$ 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 $\omega \in \mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega_L^r$. □

A.3. **Proofs for Section 3.**

Theorem 19 (restated). *Let $\boldsymbol{f}_r \in k[\boldsymbol{x}]$ be polynomials. Assume that $k(\boldsymbol{x})$ is a separable extension of $k(\boldsymbol{f}_r)$. Then, $\boldsymbol{f}_r$ are algebraically independent over k if and only if $\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}_r) \neq 0$.*

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

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

Remark 39. Note that without the separability hypothesis algebraic dependence of the $\boldsymbol{f}_r$ still implies $\mathrm{J}_{k[\boldsymbol{x}]/k}(\boldsymbol{f}_r) = 0$.

Lemma 20 (restated). *Let $\boldsymbol{f}_m \in k[\boldsymbol{x}]$ have transcendence degree r and maximal degree δ, and assume that $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > \delta^r$. Then the extension $k(\boldsymbol{x})/k(\boldsymbol{f}_m)$ 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 $k(\boldsymbol{x})/k(\boldsymbol{f}_m)$. A transcendence degree argument shows that they form a transcendence basis. Hence it suffices to show that x_i is separable over $K := k(\boldsymbol{f}_m, \boldsymbol{x}_{[r+1,n]})$ for all $i \in [r]$. By Theorem 4, we have $[k(\boldsymbol{x}) : K] \le [k(\boldsymbol{x}) : k(\boldsymbol{f}_r, \boldsymbol{x}_{[r+1,n]})] \le \delta^r < p$. Therefore, the degree of the minimal polynomial of x_i over K is $< p$, thus x_i is indeed separable for all $i \in [r]$. □

A.4. **Proofs for Section 4.** We use the notation of §4.2.

Lemma 30 (restated). *Let $\ell \ge 0$ and let $f \in B \subset \mathrm{E}^0$. Then f is $(\ell+1)$-degenerate if and only if the coefficient of $\boldsymbol{x}^\beta$ in $\mathrm{F}^{-\ell} f$ is divisible by $p^{\nu(\ell+1,\beta)}$ for all $\beta \in G$.*

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

A.5. **Proofs for Section 5.** We use the notation of §5.

Lemma 32 (restated). *Let $f \in G_{\ell+1,t}[z]$ be a polynomial of degree $D < p^t - 1$ and let $\xi \in G_{\ell+1,t}$ be a primitive $(p^t - 1)$-th root of unity. Then*

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

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

Lemma 33 (restated). *Given $G_{\ell+1,t}$, a primitive (p^t-1)-th root of unity $\xi \in G_{\ell+1,t}$, 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 $m := p^t - 1$. As in §5, we assume that $G_{\ell+1,t} = \mathbb{Z}/(p^{\ell+1})[x]/(h)$, where $\deg(h) = t$, and $\xi = x + (h)$. By Lemma 32, we have to compute a sum $S := \sum_{i=0}^{m-1} a_i$ with $a_i \in G_{\ell+1,t}$. Each summand a_i can be computed in polynomial time, because C can be efficiently evaluated. Since the number of summands in S is exponential, we need the help of a #P-oracle to compute it.

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

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

This bijection and its inverse are efficiently computable. Moreover, ι is compatible with the sum under consideration, i.e. $\iota(\boldsymbol{s}) = \sum_{i=0}^{m-1} \iota(c_i)$, 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 have to design a non-deterministic polynomial-time Turing machine that, given input as above, has exactly $\iota(\boldsymbol{s})$ accepting computation paths. This can be done as follows. First we branch over all integers $i \in [0, m-1]$. In each branch i, we (deterministically) compute the integer $\iota(c_i)$ and branch again into exactly $\iota(c_i)$ computation paths that all accept. This implies that the machine has altogether $\sum_{i=0}^{m-1} \iota(c_i) = \iota(\boldsymbol{s})$ accepting computation paths. □

We now state here the claims proved by Mengel [Men12]. Define the problem of *ℓ-Degen* as: Given a univariate arithmetic circuit computing $C(x) \in \mathbb{Q}_p[x]$, test whether $C(x)$ is ℓ-degenerate. Note that for $\ell = 1$ this is the same as the identity test $C(x) \equiv 0 \pmod{p}$, which can be done in randomized polynomial time (or ZPP). The situation drastically changes when $\ell > 1$.

Theorem 40. [Men12] *For $\ell > 1$, ℓ-Degen is* $\mathrm{C_{=}P}$*-hard under* ZPP*-reductions.*

Proof sketch. Denote by ZMC the problem: Given $m \in \mathbb{N}$ and a univariate arithmetic circuit computing $C(x) \in \mathbb{Q}[x]$, test whether $\operatorname{coeff}(x^m, C(x)) = 0$. By [FMM12] ZMC is $\mathrm{C_{=}P}$-hard. The idea is to reduce ZMC to 2-Degen. Randomly pick a sufficiently large prime p. Consider the circuit $C'(x) := px^{p-m} \cdot C(x)$. It can be shown that $C'(x)$ is 2-degenerate iff $\operatorname{coeff}(x^m, C(x)) = 0$. □

Corollary 41. [Men12] *Let $\ell > 1$. If ℓ-Degen is in* PH *then* PH *collapses.*

Proof sketch. Classically, we have

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

By the theorem it now 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 $\mathrm{PH} \subseteq \Sigma_{i+2}$. □

A.6. **Proofs for Section 6.** We use the notation of §6.

Lemma 42 (Using sparsity)**.** *Let $\ell \geq 0$ and let $g \in B$ be an s-sparse polynomial of degree less than $D \geq 2$ which is not $(\ell+1)$-degenerate. Let $S \subset R$ be a subset such that $|S \setminus pR| = (ns\lceil \log_2 D \rceil)^2 D$, and let $r \in [n]$.*

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

Proof. Write $g = \sum_{\beta \in \mathbb{N}^r} g_\beta \boldsymbol{x}_r^\beta$ with $g_\beta \in R[\boldsymbol{x}_{[r+1,n]}]$. Since g is not $(\ell+1)$-degenerate, there exists $\alpha \in \mathbb{N}^n$ such that the coefficient $c_\alpha \in R$ of $\boldsymbol{x}^\alpha$ in g is not divisible by $p^{\min\{v_p(\alpha), \ell\}+1}$. Write $\alpha = (\alpha', \alpha'') \in \mathbb{N}^r \times \mathbb{N}^{n-r}$. Since c_α is the coefficient of $\boldsymbol{x}_{[r+1,n]}^{\alpha''}$ in $g_{\alpha'}$, this polynomial cannot be divisible by $p^{\min\{v_p(\alpha), \ell\}+1}$. Our aim is to find $\boldsymbol{c} \in R^{n-r}$ such that $g_{\alpha'}(\boldsymbol{c})$ is not divisible by $p^{\min\{v_p(\alpha), \ell\}+1}$, since then it is neither by the possibly higher power $p^{\min\{v_p(\alpha''), \ell\}+1}$. In other words, if we write $g_{\alpha'} = p^e g'$, 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 $h' := g'\left(t^{D^0}, t^{D^1}, \ldots, t^{D^{n-r-1}}\right) \in R[t]$ in the new variable t. Since $\deg g' = \deg g_{\alpha'} \leq \deg g < D$, 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 be the polynomial obtained from h' by reducing every exponent modulo q. 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 $N \geq 2$ (this follows e.g. from [RS62, Corollary 1]), there is a prime $q \leq (ns\lceil \log_2 D \rceil)^2$ with $h_q \notin pR[t]$. Since $\deg(h_q) < qD \leq (ns\lceil \log_2 D \rceil)^2 D = |S \setminus pR|$, there exists $c \in S$ with $h_q(c) \notin pR$. □

Lemma 43 (p-adic triangle is isosceles)**.** *Let $\alpha, \beta \in \mathbb{Q}^s$. Then $v_p(\alpha+\beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$, with equality if $v_p(\alpha) \neq v_p(\beta)$.*

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

Now assume $v_p(\alpha) \neq v_p(\beta)$, say $v_p(\alpha) < v_p(\beta)$. Let $i \in [s]$ such that $v_p(\alpha) = v_p(\alpha_i)$. Then $v_p(\alpha_i) < v_p(\beta_i)$, therefore we obtain $v_p(\alpha+\beta) \leq v_p(\alpha_i+\beta_i) = \min\{v_p(\alpha_i), v_p(\beta_i)\} = v_p(\alpha_i) = v_p(\alpha) = \min\{v_p(\alpha), v_p(\beta)\} \leq v_p(\alpha+\beta)$. □

Lemma 44. *Let $\ell \geq 0$, let $g \in B$ and let $\alpha \in \mathbb{N}^n$ with $v_p(\alpha) \geq \ell$. Then g is $(\ell+1)$-degenerate if and only if $\boldsymbol{x}^\alpha \cdot g$ is $(\ell+1)$-degenerate.*

Proof. It suffices to show that $\min\{v_p(\beta), \ell\} = \min\{v_p(\alpha+\beta), \ell\}$ for all $\beta \in \mathbb{N}^n$. But the assumption implies that $\min\{v_p(\beta), \ell\} = \min\{v_p(\alpha), v_p(\beta), \ell\}$, which is $\leq \min\{v_p(\alpha+\beta), \ell\}$ by Lemma 43 with equality, if $v_p(\alpha) \neq v_p(\beta)$. If $v_p(\alpha) = v_p(\beta)$, then $\min\{v_p(\beta), \ell\} = \min\{v_p(\alpha), \ell\} = \ell \geq \min\{v_p(\alpha+\beta), \ell\}$. □

Let $\boldsymbol{f}_m \in A$ be polynomials and let $\varphi \colon k[\boldsymbol{x}] \to k[\boldsymbol{x}_r]$ be a k-algebra homomorphism. We say that φ is *faithful to* $\boldsymbol{f}_m$ if $\operatorname{trdeg}_k(\boldsymbol{f}_m) = \operatorname{trdeg}_k(\varphi(\boldsymbol{f}_m))$.

Lemma 45 (Faithful is useful [BMS11, Theorem 11])**.** *Let $\varphi \colon A \to k[\boldsymbol{x}_r]$ be a k-algebra homomorphism and $\boldsymbol{f}_m \in A$. Then, φ is faithful to $\boldsymbol{f}_m$ iff $\varphi|_{k[\boldsymbol{f}_m]}$ is injective.*

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

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

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

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

ECCC ISSN 1433-8092

http://eccc.hpi-web.de