Fields Institute Communications
Volume **00**, 0000

On the Decidability of the Existential Theory of $\mathbb{F}_p[[t]]$

Jan Denef
Department of Mathematics
Catholic University of Leuven
Celestijnenlaan 200B
B-3001 Leuven (Belgium)
Jan.Denef@wis.kuleuven.ac.be
http://www.wis.kuleuven.ac.be/wis/algebra/denef.html

Hans Schoutens
Department of Mathematics
Ohio State University
Columbus, OH 43210 (USA)
schoutens@math.ohio-state.edu
http://www.math.ohio-state.edu/~schoutens

Abstract. We show how Resolution of Singularities in characteristic p implies the decidability of the existential theory of $\mathbb{F}_p[[t]]$ in the language of discrete valuation rings, where t is a single variable and $\mathbb{F}_p$ the p-element field.

1 Introduction

The aim of this paper is to study the ring $\mathbb{F}_p[[t]]$, where t is a single variable and $\mathbb{F}_p$ the p-element field. Note that this is an equicharacteristic complete, whence Henselian, discrete valuation ring with maximal ideal generated by t and residue field $\mathbb{F}_p$. Hence, from an algebraic point of view this is a very well understood ring. However, from a model-theoretic point of view, it is poorly understood. This is in spite of the analogies, made evident by the work [3] of Ax en Kochen, between $\mathbb{F}_p[[t]]$ and the ring of p-adic integers. For instance, a complete recursive axiom system for the theory of $\mathbb{F}_p[[t]]$ is still unknown. For many purposes, it is an equivalent problem to understand the theory of the field $\mathbb{F}_p((t))$ as a valued field (where the valuation is the t-adic one). Indeed, in general, if (K, v) denotes a valued field, with which we mean a field K with a valuation v on it, and if R denotes its valuation ring, then R is obviously definable in K (in the language of valued fields), and, conversely, for $a, b \in R$, we have that $v(a) \leq v(b)$ if, and only if, there exists $c \in R$ with $b = ca$.

1991 *Mathematics Subject Classification.* 13L05, 12L05.

In [14] it is pointed out that the following "obvious" candidate for an axiom system for the field $K = \mathbb{F}_p((t))$ with its natural valuation v, derived by analogy from the axiom system for the p-adics, is not complete.

- The valued field (K, v) is Henselian and defectless.
- The characteristic of K is p.
- The value group of v is a $\mathbb{Z}$-group.
- The residue field is $\mathbb{F}_p$.

Note that the condition that K be defectless is superfluous for fields of characteristic zero, but in positive characteristic Henselian discretely valued fields *with defect* exist (that is to say, fields which admit a finite extension in which the fundamental equality fails). In [14], Kuhlmann proposes some additional axioms involving additive polynomials, but the resulting system is still not known to be complete.

As an immediate consequence of the existence of a complete recursive axiom system, we would get that the theory of $\mathbb{F}_p[[t]]$ is decidable. In this paper we will explain how the decidability of the *existential* theory of $\mathbb{F}_p[[t]]$ in the language of discrete valuation rings follows from Resolution of Singularities. More precisely, let $\mathcal{L}^{\mathrm{DVR}}$ be the language of rings with a single constant symbol $\boldsymbol{\pi}$ added. Let R be a discrete valuation ring with uniformizing parameter π (that is to say, the maximal ideal of R is πR). We view R as an $\mathcal{L}^{\mathrm{DVR}}$-structure by interpreting $\boldsymbol{\pi}$ as the uniformizing parameter π. Let R_0 be the subring of R generated by π, then every term in $\mathcal{L}^{\mathrm{DVR}}$ names an element of R_0 and conversely. For instance, in case $R = \mathbb{F}_p[[t]]$ (with uniformizing parameter t) then $R_0 = \mathbb{F}_p[t]$. Note that in the language $\mathcal{L}^{\mathrm{DVR}}$, both formulae $v(a) \leq v(b)$ and $v(a) < v(b)$ are existentially definable, by requiring that there exists $c \in R$ with $b = ca$, respectively $b = ca\pi$. Therefore, our results on the decidability of the existential theory of R, also hold when we add a symbol for the valuation to the language.

Our main result is that, assuming Resolution of Singularities, there exists an algorithm which decides, for an arbitrary system of equations $f_1(\xi) = \dots = f_m(\xi) = 0$ and an inequation $f_0(\xi) \neq 0$, with $f_i \in \mathbb{F}_p[t, \xi]$ and ξ a finite set of variables, whether this system has a solution in $\mathbb{F}_p[[t]]$. In fact, we will prove this for a larger class of discrete valuation rings; see Theorem 4.3. Unfortunately, Resolution of Singularities (in the form we need it; see Theorem 1 below for the precise content) is still conjectural in positive characteristic. The weaker version of De Jong, which uses finite-to-one maps instead of birational maps, appears to be not strong enough to carry out the present method of proof. What follows is a brief description of our method.

As an immediate corollary of a theorem of Greenberg in [10], a system of polynomial equations in a finite number of variables ξ over an excellent discrete valuation ring R has a solution, if it has a solution modulo arbitrary high powers of the maximal ideal. This was generalized by Artin in [2] to Henselian local rings of the form $R = \kappa[[t]]$ or $R = \kappa[[t]]^{\mathrm{alg}}$ (the ring of algebraic power series), where t is now a finite set of variables and κ is a field. Moreover, he obtains the following effective version for systems of equations with polynomial coefficients. If $f_i \in \kappa[t, \xi]$, then to find a solution of the system $f_1(\xi) = \dots = f_m(\xi) = 0$ over R, it suffices to find an approximate solution modulo the N-th power of the maximal ideal, where N depends only on the total degree d of the f_i and the number of variables t and ξ. This result is now commonly known as *Strong Artin Approximation*. Using non-standard methods, the first author et al., have shown in [4] that N depends even in a computable (recursive) way on d and the number of variables. For systems of equations with more general coefficients, see [6].

Moreover, Artin conjectured Strong Artin Approximation to be true for any excellent Henselian local ring. The status of this Conjecture has been unclear for a while, but now several proofs have been put forward, see for instance [22] or [18] (and the commentaries provided by Swan in an alas unpublished paper [23]). For our purposes (but not for the main case of interest, namely when $R = \mathbb{F}_p[[t]]$), we need a Strong Artin Approximation theorem which includes parameters (Theorem 3.1). This theorem follows from these general results together with some structure theorems for complete Noetherian local rings.

In this paper we exhibit an algorithm that verifies whether a system of equations together with some inequations over R_0 has a solution over an equicharacteristic Henselian discrete valuation ring R, at least relative to the residue field κ of R. (As before R_0 is the subring generated by some uniformizing parameter). Relative to the residue field means that this algorithm will use the theory of κ as an oracle. In fact, the algorithm will reduce the problem to finding a solution of some (effectively constructible) system of equations and inequations over the residue field κ. Since the theory of any finite or any algebraically closed field is decidable, this will yield the decidability of the existential theory of any equicharacteristic Henselian discrete valuation ring R with a finite or algebraically closed residue field. Unfortunately, this result depends on the validity of Resolution of Singularities. This is known in characteristic zero, but still conjectural for positive characteristic. In particular, we do get a positive result for instance for the rings $\mathbb{C}[[t]]$ and $\mathbb{C}[[t]]^{\mathrm{alg}}$, where t is a single variable, but only a conjectural result for the rings $\mathbf{F}_p[[t]]$. It should be noted, however, that the results over $\mathbb{C}$ also follow from the work of Ax-Kochen-Ershov ([3] and [7, 8, 9]).

Sketch of the Algorithm. What follows is a brief sketch of the strategy in the main case that $R = \mathbb{F}_p[[t]]$. Let there be given an open W in a closed subscheme X of $\mathbb{A}^n_R$, both defined over $R_0 = \mathbb{F}_p[t]$. We describe an algorithm that decides whether or not W admits an R-rational point (that is to say, a solution over R of the system of equations and inequations that define W; this will be explained in more detail in 2.1). To simplify the argument, let us moreover assume that X is irreducible and reduced. (In general, we will only be allowed to assume that the generic fibre $X_K =: X \times_{\operatorname{Spec} R} \operatorname{Spec} K$ is reduced, using Lemma 4.2.) If $W = X$, then using an effective version of Greenberg's result ([4, Theorem 3.2], or in the more general case, Theorem 3.1 below), we can reduce the problem of finding an R-rational point on X to a similar problem over $\mathbb{F}_p$, so that this particular instance is decidable, as already explained. Next we show that if the generic fibre of X has no singularities, then either X admits no R-rational points at all or the R-rational points are dense on X (see Theorem 2.4 below for an exact statement; the proof rests on some form of Néron Desingularization). Therefore, in the non-singular case, we reduced the problem of finding an R-rational point on W, to finding an R-rational point on X, and we know already how to deal with this. Finally, if the generic fibre X_K of X has singularities, and under the assumption that Resolution of Singularities for X_K holds, we can (effectively) find a proper, birational morphism $h\colon V \to X_K$ of schemes of finite type over K with V non-singular. We then 'clear denominators' to define a scheme Y over R with generic fibre equal to V and a proper birational morphism $f\colon Y \to X$ which specializes to h after base change. Outside a nowhere closed subset Z of X, the morphism f is an isomorphism (defined over R). Since f is proper, there is therefore a one-one correspondence between R-rational points on $f^{-1}(W) - f^{-1}(Z)$ and $W - Z$, by the Valuative Criterium for Properness. Since the generic fibre of Y is non-singular, we are back in the previous case. Finally, on Z we get by with an inductive argument on the dimension.

The above proof collapses for arbitrary (excellent) Henselian local rings R, since the Valuative Criterion for Properness fails for higher-dimensional local rings, so that R-rationality can no longer be preserved in the way we did above. However, for a W in *general position*, we can describe an algorithm which does not even rely on Resolution of Singularities. This is explained in the last section, where the precise definition of general position, in terms of the non-smooth locus of the generic fibre, can be found.

Acknowledgement. The main ideas in this paper, namely the results on the decidability of the existential theory of $\mathbb{F}_p[[t]]$ modulo Resolution of Singularities, are entirely due to the first author, who had made these observations already in 1983. The second author, while taking up the task of working out the details and preparing this manuscript for publication based on notes taken by F.-V. Kuhlmann during an Oberwolfach meeting in 1999, has further generalized these results to include arbitrary excellent Henselian discrete valuation rings.

2 Smooth Rational Points

2.1 Solutions and Rational Points. Let R be a ring and X a scheme over $\operatorname{Spec} R$. Let us denote the *structure morphism* by $s\colon X \to \operatorname{Spec} R$. With an *$R$-rational point* x on X, we mean a section $x\colon \operatorname{Spec} R \to X$ of the structure morphism s, that is to say, such that $s \circ x$ is the identity on $\operatorname{Spec} R$. If X is affine, say $X = \operatorname{Spec} A$ with A an R-algebra, then an R-rational point x corresponds to an R-algebra homomorphism $\phi\colon A \to R$. In particular, if A is moreover finitely generated as an algebra over R, say $A \cong R[\xi]/(f_1, \dots, f_t)$ with $\xi = (\xi_1, \dots, \xi_m)$ variables, then an R-rational point on $\operatorname{Spec} A$ is uniquely determined by an m-tuple $\mathbf{r} = (r_1, \dots, r_m) \in R^m$ such that $f_1(\mathbf{r}) = \dots = f_t(\mathbf{r}) = 0$. Namely, r_i is the image of (the class of) ξ_i under ϕ. In this terminology, we see that an R-rational point simply corresponds to a solution over R of the system of equations $f_1 = \dots = f_t = 0$.

If $f\colon Y \to X$ is a morphism of schemes over $\operatorname{Spec} R$, then we say that the R-rational point y on Y is a *lifting* of the R-rational point x on X, or that x *admits an R-rational lifting y*, if the following diagram commutes

$$\begin{tikzcd} & \operatorname{Spec} R \arrow[dl, "y"'] \arrow[dr, "x"] & \\ Y \arrow[rr, "f"'] & & X \end{tikzcd} \qquad (1)$$

The collection of all R-rational points y on Y lifting x is in one-one correspondence with the collection of all R-rational points on the fibre product $Y \times_X \operatorname{Spec} R$

given by the commutative diagram

$$\begin{tikzcd}
Y \times_X \operatorname{Spec} R \arrow[r] \arrow[d] & \operatorname{Spec} R \arrow[d, "x"] \\
Y \arrow[r, "f"'] & X
\end{tikzcd} \tag{2}$$

If f is a locally closed immersion defined over R (that is to say, if Y is an open inside a closed subscheme X' of X, where both X' and Y and the two inclusion morphisms are defined over R), then an R-rational point x on X has at most one lifting on Y, and if such a lifting exists, we simply say that x is an R-rational point on Y. Moreover, if R is local and w is the closed point of $\operatorname{Spec} R$ corresponding to the maximal ideal of R, then x is an R-rational point on an open $Y \subset X$ if, and only if, $x(w) \in Y$. Indeed, $x^{-1}(Y)$ is an open in $\operatorname{Spec} R$, since x is continuous. The only open of $\operatorname{Spec} R$ containing the closed point w is $\operatorname{Spec} R$ itself. Therefore, the image of x is entirely inside Y, showing that x is an R-rational point on Y. In particular, it follows that each R-rational point on X is already an R-rational point on an affine open subset of X, provided that R is local.

In spite of its name, an R-rational point on X is not a point *of* X. However, in case $R = K$ is a field, we can identify it with a point of X as follows. Let η be the unique point of $\operatorname{Spec} K$ (that is to say, the point corresponding to the prime ideal (0)). Let x be a K-rational point on X, that is to say, a morphism $x\colon \operatorname{Spec} K \to X$. We now may identify x with the point $x(\eta)$ of X. In fact $x(\eta)$ is a closed point of X with residue field K and each such point arises as the image of η under some K-rational point.

For R a domain, let η denote the point of $\operatorname{Spec} R$ corresponding to the prime ideal (0). We say that η is the *generic point* of $\operatorname{Spec} R$. Let x be an R-rational point on X. In particular, $x(\eta)$ is a point of X. If $X = \operatorname{Spec} A$ is affine (and by the remark above, we may always assume this provided R is moreover local), then x corresponds to an R-algebra homomorphism $\phi\colon A \to R$. Therefore $x(\eta)$ corresponds to the prime ideal $\mathfrak{p} =: \phi^{-1}(0)$, that is to say, to the kernel of ϕ. If R is not a field, then $\mathfrak{p}$ is no longer a maximal ideal, so that $x(\eta)$ is not a closed point of X. Let K denote the field of fractions of R and let $i\colon \operatorname{Spec} K \to \operatorname{Spec} R$ be the morphism corresponding to the inclusion $R \subset K$. We have a base change (or fibre product) diagram

$$\begin{tikzcd}
X_K \arrow[r, "j"] \arrow[d] & X \arrow[d, "s"] \\
\operatorname{Spec} K \arrow[r, "i"'] & \operatorname{Spec} R
\end{tikzcd} \tag{3}$$

where X_K denotes the fibre product $X \times_{\operatorname{Spec} R} \operatorname{Spec} K$. In the rest of this paper, we will always adopt the use of a subscript K to mean base change over i; this convention might be applied to schemes as well as to morphisms.

The scheme X_K is called the *generic fibre* of X, since it can be identified with $s^{-1}(\eta)$. In particular, since $s \circ x$ is by assumption the identity, we see that $x(\eta)$ lies in fact on $s^{-1}(\eta) \cong X_K$. We denote the corresponding K-rational point of X_K by x_K and call it the *underlying point* of x (on X_K). It is simply the base change of x over j, so that we have a commutative diagram

$$\begin{tikzcd}
\operatorname{Spec} K \arrow[r, "i"] \arrow[d, "x_K"'] & \operatorname{Spec} R \arrow[d, "x"] \\
X_K \arrow[r, "j"'] & X
\end{tikzcd} \tag{4}$$

Algebraically (that is to say, in case $X = \operatorname{Spec} A$ is affine), x_K corresponds to the kernel of the base change $A \otimes_R K \to K$, which is just $\mathfrak{p}(A \otimes_R K)$, since $R \subset K$ is flat. In conclusion, the underlying point of an R-rational point x on X, is a K-rational point x_K on X_K.

A note of caution: one would be tempted to identify x_K (or even $x(\eta)$) with the composition xi. However, $xi\colon \operatorname{Spec} K \to X$ is not even a K-rational point, since X is in general not a scheme over $\operatorname{Spec} K$ (which was a necessary condition in our definition).

2.2. Proposition *Let R be a discrete valuation ring with field of fractions K. Let $f\colon Y \to X$ be a proper morphism of Noetherian schemes over* Spec *R. Let x be an R-rational point on X. If the underlying point x_K of x admits a K-rational lifting on the generic fibre Y_K, then x admits an R-rational lifting on Y.*

More precisely, if w is a K-rational lifting of x_K on Y_K, then we can choose an R-rational lifting y of x on Y with underlying point equal to w.

Proof This is a direct application of the Valuative Criterium for Properness as follows. Namely, let w be a K-rational point on Y_K lifting x_K. This means that $w\colon \operatorname{Spec} K \to Y_K$ and $x_K = f_K \circ w$, where $f_K\colon Y_K \to X_K$ is the base change of f.

Let us denote by $y_0\colon \operatorname{Spec} K \to Y$ the composition of w with the base change morphism $Y_K \to Y$. We therefore have a commutative diagram

$$\begin{tikzcd}
\operatorname{Spec} K \arrow[r, "i"] \arrow[d, "y_0"'] & \operatorname{Spec} R \arrow[d, "x"] \\
Y \arrow[r, "f"'] & X
\end{tikzcd} \tag{5}$$

By [11, Chapter II, Theorem 4.7], there exists a morphism $y\colon \operatorname{Spec} R \to Y$, such that $fy = x$ and $y_0 = yi$, which therefore defines an R-rational lifting of x, with $y_K = w$. □

2.3. Definition Let R be a domain with field of fractions K. Let X be a scheme over Spec R and let x be an R-rational point on X. By abuse of terminology, we will say that x is *non-singular*, if the underlying point x_K of x is a non-singular point of X_K. Algebraically, in case $X = \operatorname{Spec} A$ is affine, this means that $A_{\mathfrak{p}} \otimes_R K$ is a regular local ring, where $\mathfrak{p}$ is the kernel of the homomorphism $A \to R$ corresponding to x.

The following theorem shows that non-singular R-rational points are locally dense. The proof uses some form of Néron Desingularization (Claim 2.5).

2.4. Theorem *Let $(R, \mathfrak{m})$ be an Henselian local domain with fraction field K. Let X be a scheme of finite type over* $\operatorname{Spec} R$. *If X admits a non-singular R-rational point x, then there exists an open X' of X, defined over R and admitting x as an R-rational point, with the following property. Every open W of X' which is defined over R, admits at least one R-rational point. (We'll simply say that the R-rational points are* dense in a neighbourhood *X' of the non-singular point x).*

Proof We may assume that $X = \operatorname{Spec} A$ is affine, since R is local (see the remark near the end of the second paragraph in 2.1). Let $\mathfrak{p}$ be the kernel of the R-algebra homomorphism $A \to R$ corresponding to x. Let $A_K = A \otimes_R K$, so that the generic fibre X_K of X is isomorphic to $\operatorname{Spec} A_K$. Hence $\mathfrak{p} A_K$ is the maximal ideal corresponding to the underlying point x_K of x and we will still write $\mathfrak{p}$ for its image in A_K.

Since by assumption $(A_K)_{\mathfrak{p}}$ is regular, we can find a regular system of parameters $(t_1, \dots, t_h)$ for $(A_K)_{\mathfrak{p}}$, with $t_i \in A$. Note that this simply means that $(t_1, \dots, t_h)(A_K)_{\mathfrak{p}} = \mathfrak{p}(A_K)_{\mathfrak{p}}$ where h is the dimension of $(A_K)_{\mathfrak{p}}$. Consider the K-algebra homomorphism

$$\psi \colon K[\xi] \to A_K \tag{6}$$

given by sending ξ_i to t_i, where $\xi = (\xi_1, \dots, \xi_h)$ are variables. Let $\mathfrak{n}$ denote the maximal ideal in $K[\xi]$ generated by the ξ_i, so that

$$(A_K)_{\mathfrak{p}} / \mathfrak{n}(A_K)_{\mathfrak{p}} = (A_K)_{\mathfrak{p}} / \mathfrak{p}(A_K)_{\mathfrak{p}} = K. \tag{7}$$

Note that $(\xi_1, \dots, \xi_h)$ is a regular sequence in $K[\xi]_{\mathfrak{n}}$ mapped bijectively by ψ onto the regular sequence $(t_1, \dots, t_h)$ in $(A_K)_{\mathfrak{p}}$. By the Local Flatness Criterion [16, Theorem 22.3], we get that $K[\xi]_{\mathfrak{n}} \to (A_K)_{\mathfrak{p}}$ is flat. Equation (7) shows that $K[\xi]_{\mathfrak{n}} \to (A_K)_{\mathfrak{p}}$ is also unramified (note that both local rings have residue field K). Therefore ψ is etale at $\mathfrak{p}$; see for instance [17, Chapter I.§3] or [19, Chapitre V] for definitions. In other words, ψ induces a morphism $f \colon X_K \to \mathbb{A}^h_K$ which is etale at x_K. Note that this implies in particular that X_K is smooth over K in the point x_K.

After a translation, since x is R-rational, we might as well have taken x so that x_K lies over the origin in $\mathbb{A}^h_K$ (identified with the n-tuple 0). By [17, Corollary 3.16], we can write A_K as

$$A_K \cong K[\xi, \zeta]/(f_1, \dots, f_N) \tag{8}$$

with $\xi = (\xi_1, \dots, \xi_h)$ and $\zeta = (\zeta_1, \dots, \zeta_N)$ variables, and where h is the dimension of X_K and $f_j \in R[\xi, \zeta]$ are polynomials without constant term, such that the *Jacobian Criterion* holds in the point $(0, 0)$ with respect to the ζ-variables. This means that the determinant d of

$$\frac{\partial(f_1, \dots, f_N)}{\partial(\zeta_1, \dots, \zeta_N)} =: \begin{pmatrix} \partial f_1/\partial\zeta_1 & \partial f_1/\partial\zeta_2 & \dots & \partial f_1/\partial\zeta_N \\ \partial f_2/\partial\zeta_1 & \partial f_2/\partial\zeta_2 & \dots & \partial f_2/\partial\zeta_N \\ \vdots & \vdots & \ddots & \vdots \\ \partial f_N/\partial\zeta_1 & \partial f_N/\partial\zeta_2 & \dots & \partial f_N/\partial\zeta_N \end{pmatrix} \tag{9}$$

is non-zero when evaluated at $(0,0)$. Let $d_0 = d(0,0)$ be this non-zero element. Note that $d_0 \in R$.

Set

$$B =: R[\xi,\zeta]/(f_1,\dots,f_N) \tag{10}$$

and let Y be the affine scheme $\operatorname{Spec} B$. By construction, $X_K = Y_K$, so that we can find an open W of X which is defined over R and admits x as an R-rational point, and an open V of Y, defined over R, such that $W \cong V$ (as schemes over $\operatorname{Spec} R$). Moreover, we can find an R-rational point y on V with underlying point equal to x_K. Therefore R-rational points are dense on X in a neighbourhood of x if, and only if, they are dense on Y in a neighbourhood of y (in the terminology introduced in the statement), so that we may as well assume that $Y = X$.

We define an R-algebra endomorphism σ on $R[\xi,\zeta]$ by letting

$$\begin{cases} \xi_j & \mapsto d_0^2\xi_j \\ \zeta_j & \mapsto d_0\zeta_j. \end{cases} \tag{11}$$

Let $f_i^\sigma(\xi,\zeta)$ denote the image of f_i under σ. If $\mathbf{r} = (s_1,\dots,s_h,t_1,\dots,t_N) \in R^{h+N}$ is an R-rational solution of $f^\sigma = 0$, then $(d_0^2 s_1,\dots,d_0^2 s_h, d_0 t_1,\dots,d_0 t_N)$ is an R-rational solution of $f = 0$. In particular, if the R-rational points are dense on the variety X^σ defined by f^σ, then so are the R-rational points on X.

2.5. Claim *There exist $g_i \in R[\xi,\zeta]$, for $i = 1,\dots,N$, such that the variety over R defined by the g_i is X^σ, and, moreover, the determinant of $\frac{\partial(g_1,\dots,g_N)}{\partial(\zeta_1,\dots,\zeta_N)}$ evaluated at $(0,0)$, equals 1, where $\frac{\partial(g_1,\dots,g_N)}{\partial(\zeta_1,\dots,\zeta_N)}$ is defined as in (9) with the g_i instead of the f_i.*

Assuming the claim, we therefore may assume upon replacing X by X^σ, that $d(0,0) = d_0 = 1$. Let $\mathfrak{m}$ denote the maximal ideal of R. Let W be a non-zero open subset of X, defined over R. We need to show that W admits an R-rational point. Without loss of generality, we may assume that W is the complement of the hypersurface defined by some $f_0 \in R[\xi,\zeta]$. Since W is non-empty, the ideal $(f_0,\dots,f_N)$ has height at least $N+1$ in $K[\xi,\zeta]$. By taking generic hyperplanes, we can find $a_i \in \mathfrak{m}$, for $i = 1,\dots,h-1$, such that the ideal

$$(f_0,\dots,f_N,\xi_1 - a_1,\dots,\xi_{h-1} - a_{h-1}) \tag{12}$$

has height $h+N$ in $K[\xi,\zeta]$, whence has only finitely many solutions (over the algebraic closure of K). Therefore, we can choose $a_h \in \mathfrak{m}$, so that

$$(f_0,\dots,f_N,\xi_1 - a_1,\dots,\xi_h - a_h)K[\xi,\zeta] \tag{13}$$

is the unit ideal of $K[\xi,\zeta]$.

Set $F_i(\zeta) = f_i(a_1,\dots,a_h,\zeta)$, for $i = 0,\dots,N$, so that $F_i \in R[\zeta]$. Write f for $(f_1,\dots,f_N)$ and F for $(F_1,\dots,F_N)$. Using (13), we get that

$$(F_0,\dots,F_N)K[\zeta] = (1) \tag{14}$$

Since $f(0,0) = 0$ and $a_i \in \mathfrak{m}$, we get that $F(0) \equiv 0 \mod \mathfrak{m}$. Moreover, since $d(0,0) = 1$, we get that the determinant of $\frac{\partial(F_1,\dots,F_N)}{\partial(\zeta_1,\dots,\zeta_N)}$ is a unit in R when evaluated at 0. Since R is Henselian, we can find $\mathbf{t} = (t_1,\dots,t_N) \in R^N$, such that $F(\mathbf{t}) = 0$. By (14), we must have that $F_0(\mathbf{t}) \neq 0$. In other words, if we let $\mathbf{r} = (a_1,\dots,a_h,\mathbf{t})$, then $\mathbf{r}$ defines an R-rational point on W, as required.

So remains to prove our Claim 2.5. Let us write J for $\frac{\partial(f_1,\ldots,f_N)}{\partial(\zeta_1,\ldots,\zeta_N)}$ as defined in (9). Taylor expansion at $(0,0)$ of f gives (in matrix notation)

$$f = \zeta J + p(\xi) + q(\xi,\zeta) \tag{15}$$

with p_i linear forms in the variables ξ and with $q_i \in (\xi,\zeta)^2 R[\xi,\zeta]$, where we have written $p = (p_1,\ldots,p_N)$ and $q = (q_1,\ldots,q_N)$.

Let H be the adjoint matrix of J, so that H has also its entries in R and, moreover, we have that

$$HJ = JH = d\mathbf{E}_N \tag{16}$$

where $\mathbf{E}_N$ denotes the $(N \times N)$-identity matrix. Applying H to equation (15) yields

$$fH = d\zeta + p'(\xi) + q'(\xi,\zeta) \tag{17}$$

with the linear forms p'_i in the ξ-variables and the polynomials $q'_i \in (\xi,\zeta)^2 R[\xi,\zeta]$ the respective entries of the N-tuples p' and q'. Let σ denote the change of variables (11). We will use in general a superscript σ to denote the image of an element or a matrix under σ. Hence applying σ to Equation (17) gives

$$f^\sigma H^\sigma = d^\sigma d_0 \zeta + d_0^2 p''(\xi) + d_0^2 q''(\xi,\zeta) \tag{18}$$

with the linear forms p''_i in the variables ξ and the polynomials $q''_i \in (\xi,\zeta)^2 R[\xi,\zeta]$ the entries of p'' and q'' respectively. Since $d^\sigma(0,0) = d(0,0) = d_0$, we have in fact that

$$f^\sigma H^\sigma = d_0^2\big[\zeta + p'''(\xi) + q'''(\xi,\zeta)\big] \tag{19}$$

with the linear forms p'''_i in the ξ-variables and the polynomials $q'''_i \in (\xi,\zeta)^2 R[\xi,\zeta]$ the entries of p''' and q''' respectively. Put

$$g = \zeta + p'''(\xi) + q'''(\xi,\zeta), \tag{20}$$

so that $f^\sigma H^\sigma = d_0^2 g$, by (19). In particular, g defines the same variety X^σ as f^σ. Moreover, the determinant of $\frac{\partial(g_1,\ldots,g_N)}{\partial(\zeta_1,\ldots,\zeta_N)}$ evaluated at $(0,0)$ is 1, as required. □

3 The Positive Existential Theory

The following theorem generalizes [4, Theorem 3.2] in that we allow now also parameters. Nonetheless, the (non-standard) method of proof is the same, in the main case that R is a power series ring over a field, but instead of using Artin's original result [2, Theorem 1.10], we need the general solution of the Artin Conjecture due to [22] or [18].

3.1. Theorem (Strong Artin Approximation with Parameters) *Let $(R,\mathfrak{m})$ be an equicharacteristic excellent Henselian local ring. Let $\mathbf{u}$ be a k-tuple (of parameters) over R. There exists a function $N_{R,\mathbf{u}}\colon \mathbb{N}^2 \to \mathbb{N}$, only depending on R and on $\mathbf{u}$, with the following property. Let $f_i(U,\xi)$, for $i = 1,\ldots,t$, be polynomials of degree at most d in the k variables U and the m variables ξ over $\mathbb{Z}$. If there exists an m-tuple $\mathbf{r} \in R^m$ such that all $f_i(\mathbf{u},\mathbf{r}) \equiv 0 \mod \mathfrak{m}^N$, with $N = N_{R,\mathbf{u}}(d,m)$, then there exists $\mathbf{s} \in R^m$, such that all $f_i(\mathbf{u},\mathbf{s}) = 0$.*

Proof Let $f_i \in \mathbb{Z}[U,\xi]$ be of degree at most $d \geq 2$, for $i = 1,\ldots,t$ with $U = (U_1,\ldots,U_k)$ and $\xi = (\xi_1,\ldots,\xi_m)$ variables, where the U will play the role of parameter variables and the ξ of indeterminates. We first reduce to the case that R is complete, as follows. Let R be arbitrary and assume the theorem proven for equicharacteristic complete Noetherian local rings. Let $\widehat{R}$ be the completion of R (with respect to the $\mathfrak{m}$-adic topology). By the result [22] or [18] (see also [23]), the pair $R \subset \widehat{R}$ has Artin Approximation. In model-theoretic terms, this simply means that R is existentially closed in $\widehat{R}$. Algebraically, this means that any polynomial system of equations over R is solvable over R, if it is already solvable over $\widehat{R}$. We claim that we can simply take $N_{\widehat{R},\mathbf{u}}$ for the function $N_{R,\mathbf{u}}$. Indeed, let $N = N_{\widehat{R},\mathbf{u}}(d,m)$ and suppose $\mathbf{r} \in R^m$ satisfies that all $f_i(\mathbf{u},\mathbf{r}) \equiv 0 \mod \mathfrak{m}^N$. Since this remains true in $\widehat{R}$, we get by assumption that there exists $\widehat{\mathbf{r}} \in \widehat{R}^m$, such that all $f_i(\mathbf{u},\widehat{\mathbf{r}}) = 0$. Using Artin Approximation to the system of equations $f_i(\mathbf{u},\xi) = 0$, we therefore can find $\tilde{\mathbf{r}} \in R^m$, with all $f_i(\mathbf{u},\tilde{\mathbf{r}}) = 0$.

Therefore, we may moreover assume that R is complete. Next we show that if the theorem holds for R, then it also holds for any homomorphic image of R. Indeed, assume that $N_{R,\mathbf{u}}$ has been shown to exist for R and all tuples $\mathbf{u}$. Let $\mathfrak{a} = (v_1,\dots,v_l)$ be an ideal of R. Set $\bar{R} = R/\mathfrak{a}$ and let $\mathbf{u}$ be a k-tuple over R. Let $\mathbf{r} \in R^m$ and assume that $f_i(\mathbf{u},\mathbf{r}) \equiv 0 \mod \mathfrak{m}^M\bar{R}$, for some $M \in \mathbb{N}$ (to be determined later). Hence there exists $a_{ij} \in R$, such that

$$f_i(\mathbf{u},\mathbf{r}) \equiv \sum_{j=1}^{l} a_{ij} v_j \mod \mathfrak{m}^M \tag{21}$$

in R, for all $i = 1,\dots,t$. Put

$$F_i(U,V,\xi,\zeta) = f_i(U,\xi) - \sum_{j=1}^{l} \zeta_{ij} V_j \tag{22}$$

for all $i = 1,\dots,t$, so that F_i is a polynomial over $\mathbb{Z}$ in the variables U, $V = (V_1,\dots,V_l)$, ξ and $\zeta = (\zeta_{ij})$. Note that F_i has again degree at most d. Set $\mathbf{a} = (a_{ij})$ and $\mathbf{v} = (v_1,\dots,v_l)$, so that $F_i(\mathbf{u},\mathbf{v},\mathbf{r},\mathbf{a}) \equiv 0 \mod \mathfrak{m}^M$ in R by (21). If we let M be at least $N_{R,(\mathbf{u},\mathbf{v})}(d, n+lt)$, then we can find a tuple $(\mathbf{s},\mathbf{b}) \in R^{n+lt}$, such that all $F_i(\mathbf{u},\mathbf{v},\mathbf{s},\mathbf{b}) = 0$. However, this simply means that all $f_i(\mathbf{u},\mathbf{s}) = 0$ in $\bar{R}$, as required.

Since any complete Noetherian local ring is a quotient of a complete regular local ring by [16, Theorem 29.4], we may moreover assume by the previous argument that R is an equicharacteristic complete regular local ring. Therefore, R is isomorphic to a power series ring over a field by Cohen's Structure Theorem [16, Theorem 28.3]. In other words, $R = \kappa[[T]]$, with $T = (T_1,\dots,T_d)$ a finite set of variables (where d is the dimension of R) and κ the residue field of R. We would like to apply [4, Theorem 3.2], where the existence of the required computable function is shown. However, (with notation from that paper), this result is only applicable if $u_i \in \kappa[T]$, by letting $F_i(T,\xi) = f_i(\mathbf{u},\xi)$ and taking $N_{R,\mathbf{u}}$ equal to the function $\beta(d,m,\delta,0)$, where δ is the total degree of the polynomials F_i.

For arbitrary $\mathbf{u}$, we cannot apply [4] as it stands. Instead we prove a more general result using the same (non-standard) method of proof; for more details on these non-standard techniques, we refer to [4]. Therefore, towards a contradiction, assume that no such bound as in the statement exists for the pair (d,m). This means that we can find for each $c \in \mathbb{N}$ a counterexample, ${f_i}^{[c]} \in \kappa[U,\xi]$ (we may as well take coefficients in κ) and $\mathbf{r}^{[c]} \in R^m$ as follows. The total degree of each ${f_i}^{[c]}$

is at most d and

$$f_i{}^{[c]}(\mathbf{u}, \mathbf{r}^{[c]}) \equiv 0 \mod \mathfrak{m}^c \tag{23}$$

but no solution over R to the system of equations $f_i{}^{[c]}(\mathbf{u}, \xi) = 0$ exists. Let $\mathcal{U}$ be some non-principal ultrafilter on $\mathbb{N}$ and let $R^{[\mathcal{U}]}$ and $\kappa^{[\mathcal{U}]}$ be the ultrapowers of R and κ respectively. It follows from [4, Lemma 3.4] that

$$R^{[\mathcal{U}]}/\mathfrak{m}^\infty R^{[\mathcal{U}]} \cong \kappa^{[\mathcal{U}]}[[T]], \tag{24}$$

where $\mathfrak{m}^\infty R^{[\mathcal{U}]}$ is the ideal of infinitesimals, that is to say, the intersection of all $\mathfrak{m}^n R^{[\mathcal{U}]}$. Let $\mathbf{r}^{[\mathcal{U}]}$ and $f_i{}^{[\mathcal{U}]}$ be the image of the sequences $(\mathbf{r}^{[c]})_c$ and $(f_i{}^{[c]})_c$ in $R^{[\mathcal{U}]}$ and $\kappa^{[\mathcal{U}]}[U, \xi]$ respectively. Just observe that since each $f_i{}^{[c]}$ has degree at most d, so does $f_i{}^{[\mathcal{U}]}$, whence it is in particular a polynomial. From (23), it follows that $f_i{}^{[\mathcal{U}]}(\mathbf{u}, \mathbf{r}^{[\mathcal{U}]}) \in \mathfrak{m}^\infty R^{[\mathcal{U}]}$, for all i. Therefore, by (24), each $f_i{}^{[\mathcal{U}]}(\mathbf{u}, \mathbf{r}^{[\mathcal{U}]}) = 0$ when viewed as an element in $\kappa^{[\mathcal{U}]}[[T]]$.

Let A denote the localization of $\kappa^{[\mathcal{U}]}[T, \mathbf{u}]$ (the $\kappa^{[\mathcal{U}]}$-subalgebra of $\kappa^{[\mathcal{U}]}[[T]]$ generated by $\mathbf{u}$ and T) at the maximal ideal $\mathfrak{m}\kappa^{[\mathcal{U}]}[[T]] \cap \kappa^{[\mathcal{U}]}[T, \mathbf{u}]$. Since A is locally of finite type over the field $\kappa^{[\mathcal{U}]}$, it is an excellent ring ([15, §34]). Note that $f_i{}^{[\mathcal{U}]}(\mathbf{u}, \xi) \in A[\xi]$. Since $\kappa^{[\mathcal{U}]}[T] \subset A$, the completion of A is $\kappa^{[\mathcal{U}]}[[T]]$. By Artin Approximation [22] or [18] applied to the Henselization $A^\sim$ of A, we can find already a solution $\mathbf{r}^\sim$ over $A^\sim$ to the system $f_i{}^{[\mathcal{U}]}(\mathbf{u}, \xi) = 0$, that is to say, so that $f_i{}^{[\mathcal{U}]}(\mathbf{u}, \mathbf{r}^\sim) = 0$. Since both $\mathbf{u}$ and $\kappa^{[\mathcal{U}]}[T]$ are contained in $R^{[\mathcal{U}]}$, so is A. By the universal property of Henselizations and the fact that $R^{[\mathcal{U}]}$ is again Henselian by Łos's Theorem [13, Theorem 9.5.1], there is a unique A-algebra homomorphism $\gamma \colon A^\sim \to R^{[\mathcal{U}]}$. Therefore, if we put $\mathbf{s} = \gamma(\mathbf{r}^\sim)$, then $f_i{}^{[\mathcal{U}]}(\mathbf{u}, \mathbf{s}) = 0$ in $R^{[\mathcal{U}]}$. However, choosing some tuples $\mathbf{s}^{[c]}$ over R so that the image $\mathbf{s}^{[\mathcal{U}]}$ of the sequence of these tuples in $R^{[\mathcal{U}]}$ is equal to $\mathbf{s}$, we see that for almost all c, we have that $f_i{}^{[c]}(\mathbf{u}, \mathbf{s}^{[c]}) = 0$, for all $i = 1, \dots, t$, contradicting our original assumptions. □

3.2. Remark The above proof in fact shows that we can prove a slightly more general result. Namely in the statement of the theorem, we may take the f_i to have coefficients over any subfield λ of R.

3.3. Remark Let $\mathcal{L}(\mathbf{u})$ denote the language of rings together with constant symbols denoting the entries of $\mathbf{u}$. Using a similar proof as in [4, Theorem 6.1], one can show that the function $N_{R,\mathbf{u}}$ in the above statement can be chosen to be computable modulo the $\mathcal{L}(\mathbf{u})$-diagram of R (see [13, p. 16] for the definition of diagram). In other words, when computing the function $N_{R,\mathbf{u}}$, we are allowed to use as oracles, all equations and inequations over $\mathbb{Z}$ among the entries of $\mathbf{u}$ which are true in R. In particular, if the the subring of R generated by $\mathbf{u}$ is *computable*, in the sense that it admits an enumeration of its elements for which addition and multiplication are computable functions, then $N_{R,\mathbf{u}}$ can be chosen to be computable.

3.4. Remark We will use this Strong Artin Approximation with Parameters below to prove certain decidability results for excellent equicharacteristic discrete valuation rings. In the main case of interest, that is, when $R = \mathbb{F}_p[[t]]$, we need the above result with $\mathbf{u}$ equal to t, so that we can apply [4, Theorem 3.2] without reserve. In particular, in this case, the proof does not rely on the general Artin Approximation Theorem [22] or [18], but only on Artin's result [2, Theorem 1.10].

In [21], the second author gives a proof of a mixed characteristic form of Strong Artin Approximation with Parameters, by essentially the same methods.

3.5. Proposition *Let R be an equicharacteristic excellent Henselian local domain with residue field κ. Let $\mathbf{u}$ be a k-tuple in R. Then the positive $\mathcal{L}(\mathbf{u})$-existential theory of R is decidable relative to the existential theory of κ and the $\mathcal{L}(\mathbf{u})$-diagram of R.*

More precisely, given a morphism of finite type $f\colon Y \to X$ of schemes of finite type over R, we can obtain (in a constructive way from the parameters used to describe X, Y and f) a morphism of finite type $\mathfrak{f}\colon \mathfrak{Y} \to \mathfrak{X}$ of schemes of finite type over κ, such that, for each R-rational point $x\colon \operatorname{Spec} R \to X$, we can construct a κ-rational point $\bar{x}$ of $\mathfrak{X}$ with the property that x admits an R-rational lifting on Y if, and only if, the fibre $\mathfrak{Y}_{\bar{x}} = \mathfrak{f}^{-1}(\bar{x})$ admits a κ-rational point.

Proof Let φ be a positive $\mathcal{L}(\mathbf{u})$-existential formula, so that it is a disjunction of statements of the form

$$(\exists \xi) f_1(\mathbf{u}, \xi) = f_2(\mathbf{u}, \xi) = \cdots = f_t(\mathbf{u}, \xi) = 0 \tag{25}$$

with $f_i \in \mathbf{Z}[U, \xi]$ and $U = (U_1, \dots, U_k)$ and $\xi = (\xi_1, \dots, \xi_m)$ tuples of variables. Without loss of generality we may assume that φ is one such disjunct (25). Using Strong Artin Approximation with Parameters (Theorem 3.1), we can find some N, such that φ holds if, and only if, there exists $\mathbf{r} \in R^m$ such that

$$f_1(\mathbf{u}, \mathbf{r}) \equiv f_2(\mathbf{u}, \mathbf{r}) \equiv \cdots \equiv f_t(\mathbf{u}, \mathbf{r}) \equiv 0 \mod \mathfrak{m}^N. \tag{26}$$

Moreover, N depends in a computable way only on the $\mathcal{L}(\mathbf{u})$-diagram of R, on m and on the total degrees of the f_i. In other words, we reduced the problem, modulo the $\mathcal{L}(\mathbf{u})$-diagram of R, to the decidability of the existential theory of $R/\mathfrak{m}^N$. As $R/\mathfrak{m}^N$ is a finite dimensional vector space over κ, we even reduced the problem to the decidability of the existential theory of κ.

The last statement is just a translation into a more geometric language of the above algorithm. Indeed, since the problem is local, we may assume that both X and Y are affine. Since X is a closed subscheme of some affine space $\mathbb{A}^k_R$, we may as well assume that X is the affine space $\mathbb{A}^k_R = \operatorname{Spec} R[U]$, with $U = (U_1, \dots, U_k)$ some variables. If B is the coordinate ring of Y, then $B = R[U, \xi]/(f_1, \dots, f_t)$, for some polynomials f_i and some variables $\xi = (\xi_1, \dots, \xi_m)$. Suppose $f_i = g_i(\mathbf{u}', U, \xi)$ with g_i defined over $\mathbb{Z}$ and $\mathbf{u}'$ a k'-tuple over R. Set $C = \mathbb{Z}[U', U, \xi]/(g_1, \dots, g_t)$, with $U' = (U'_1, \dots, U'_{k'})$ variables. Let x be an R-rational point on $\mathbb{A}^k_R$ given by the k-tuple $\mathbf{u}$. The tuple $(\mathbf{u}', \mathbf{u})$ then defines an R-rational point on $\mathbb{A}^{k'+k}_R$. Moreover, these rational points induce an equality of fibre products

$$\operatorname{Spec} C \times_{\mathbb{A}^{k'+k}_R} \operatorname{Spec} R = Y \times_{\mathbb{A}^k_R} \operatorname{Spec} R. \tag{27}$$

Since a lifting of an R-rational point on $\mathbb{A}^{k'+k}_R$ or $\mathbb{A}^k_R$ corresponds to an R-rational point on these respective fibre products, we may assume, after enlarging the tuple of variables U, that the f_i have already coefficients over $\mathbb{Z}$.

Let $e_1, \dots, e_\tau$ be a basis of $R/\mathfrak{m}^N$ over κ. Write the image of $\mathbf{u}$ in $R/\mathfrak{m}^N$ as $\mathbf{l}_1 e_1 + \cdots + \mathbf{l}_\tau e_\tau$ with $\mathbf{l}_i$ tuples over κ and set $\mathbf{l}$ equal to the tuple of all $\mathbf{l}_i$. Let ζ_j and λ be tuples of variables with ζ equal to the tuple of all ζ_j and write

$$\bar{f}_i(\mathbf{u}, \zeta_1 e_1 + \dots \zeta_\tau e_\tau) = g_{i1}(\mathbf{l}, \zeta) e_1 + \cdots + g_{i\tau}(\mathbf{l}, \zeta) e_\tau \tag{28}$$

for $i = 1, \dots, t$, with $g_{ij} \in \kappa[\lambda, \zeta]$ and where $\bar{f}_i$ denotes the reduction of f_i modulo $\mathfrak{m}$. Then the equivalence (26) has a solution if, and only if, the system of equations $g_{ij}(\mathbf{l}, \zeta) = 0$ has a solution in κ. Therefore, we proved the last statement by setting $\mathfrak{Y} = \operatorname{Spec} \kappa[\lambda, \zeta]/(g_{ij})$ and $\mathfrak{X} = \mathbb{A}^{t\tau}_{\kappa}$. □

3.6. Remark In particular, if the subring generated by $\mathbf{u}$ is computable (see Remark 3.3) and if κ is either a finite field or an algebraically closed field, then the positive $\mathcal{L}(\mathbf{u})$-existential theory of R is decidable. This is because in either case κ is decidable. In fact, if κ is finite, then we do not need to assume that R is equicharacteristic, provided we have the equivalent statement for mixed characteristic in Theorem 3.1, for then $R/\mathfrak{m}^N$ will also be finite whence decidable.

4 The Existential Theory of $\mathbb{F}_p[[t]]$.

We will assume the truth of the following Conjecture.

Conjecture 1 (Resolution of Singularities) *Let X be a reduced scheme of finite type over a field K. Then there exists a morphism $f\colon \tilde{X} \to X$ of schemes of finite type over K, such that*

- *f is a blowing up in a nowhere dense centre defined over K;*
- *$\tilde{X}$ is non-singular.*

Note that a blowing up in a nowhere dense centre is a proper, birational morphism by [11, Chapter II Proposition 7.16]. In fact, one expects that if the conjecture is true then we can take f to be a composition of finitely many blowing ups with smooth centres.

The Conjecture is known in the following cases.

- If K has characteristic zero, by a theorem of Hironaka in [12]; see also [5].
- If X has dimension at most two, by a theorem of Abhyankar in [1].

4.1. Remark If the Conjecture holds for the scheme X, then we can in fact calculate the desingularization f in an effective way as follows. Firstly, without loss of generality, we may assume that $X = \operatorname{Spec} A$ is affine. Let K_0 be a finitely generated (whence countable) field over which X is already defined, so that $X = \operatorname{Spec} A_0 \times_{K_0} K$, where A_0 is some finitely generated K_0-algebra. Let $\mathfrak{a}_1, \mathfrak{a}_2, \dots$ be an enumeration of all ideals of A_0 defining a nowhere dense closed subset of $\operatorname{Spec} A_0$. For each $i = 1, 2, \dots$, let $f_i\colon X_i \to \operatorname{Spec} A_0$ be the blowing up with respect to $\mathfrak{a}_i$. To check whether X_i is non-singular, we can use the Jacobian Criterion [16, Theorem 30.3], which amounts in checking whether certain determinants vanish or not. This establishes an effective procedure to find a desingularization for X, since after checking a finite number of ideals, we must arrive, according to Resolution of Singularities, at a situation where the blowing up is non-singular. This algorithm does rely though on the fact that we can verify identities holding in K_0 (or K). In particular, if X is already defined over the prime field or a transcendental extension of the prime field (or, for that matter, over any computable subfield), then the desingularization is computable.

4.2. Lemma *Let R be a domain with field of fractions K. Let X be a scheme of finite type over $\operatorname{Spec} R$. There exists a closed subscheme Y of X, such that Y_K is equal to the reduced closed subscheme of X_K (that is to say, Y_K and X_K have the same underlying set and Y_K is reduced), and such that any R-rational point on*

X lies already on Y. Moreover, there exists an algorithm which calculates Y from X.

Proof We may assume that $X = \operatorname{Spec} A$ is affine, with A a finitely generated R-algebra. Suppose $A = R[\xi]/(f_1, \dots, f_t)$, with $\xi = (\xi_1, \dots, \xi_m)$ variables. Therefore, $K[\xi]/(f_1, \dots, f_t)K[\xi]$ is the affine algebra of X_K. Let $g_1, \dots, g_s \in R[\xi]$, so that the radical of $(f_1, \dots, f_t)K[\xi]$ equals $(g_1, \dots, g_s)K[\xi]$. By [20, Theorem 2.10], there exists a uniform bound on the degrees of the g_i, depending in a computable way, only on the degrees of the f_i. This latter fact implies that there is an algorithm which effectively calculates these g_i at least over K, after which we just need to clear denominators to obtain polynomials over R.

Let $B = R[\xi]/(f_1, \dots, f_t, g_1, \dots, g_s)$ and set $Y = \operatorname{Spec} B$, so that Y is a closed subscheme of X. By construction Y_K equals the reduced closed subscheme with the same underlying set as X_K. Suppose that x is an R-rational point on X. To x there corresponds an R-tuple $\mathbf{r} \in R^m$ such that $f_1(\mathbf{r}) = \dots = f_t(\mathbf{r}) = 0$, as explained above in 2.1. Since the g_i belong to the radical of $(f_1, \dots, f_t)K[\xi]$, it follows that also $g_1(\mathbf{r}) = \dots = g_s(\mathbf{r}) = 0$. Using once more the correspondence between R-rational points and solutions over R, we see that x is an R-rational point on Y, as required. □

We can now prove the main theorem of this paper.

4.3. Theorem *Let us assume the validity of Conjecture 1. Let R be an excellent equicharacteristic Henselian discrete valuation ring with residue field κ. Then the existential theory of R in the language $\mathcal{L}^{DVR}$ is decidable relative to the existential theory of κ and the $\mathcal{L}^{DVR}$-diagram of R.*

In particular, the $\mathcal{L}^{DVR}$-existential theory of $\mathbb{F}_p[[t]]$ is decidable, where t is a single variable.

Proof The last statement follows immediately from the first statement, as a finite field is definable. Hence remains to show the first statement. Let $\mathfrak{m} = \pi R$ be the maximal ideal of R. Let K denote the field of fractions of R and let R_0 be the subring of R generated by the uniformizing parameter π. Let φ be an existential sentence in the language $\mathcal{L}^{\mathrm{DVR}}$. The theorem states that there is an algorithm deciding whether φ holds in R, where the algorithm is allowed to use the existential theory of κ as an oracle, that is to say, we may assume that we know how to decide whether an existential sentence is true over κ.

The sentence φ is a disjunction of sentences of the form

$$(\exists \xi) f_1(\pi, \xi) = f_2(\pi, \xi) = \dots = f_t(\pi, \xi) = 0 \wedge f_0(\pi, \xi) \neq 0 \tag{29}$$

with $f_i \in \mathbf{Z}[U, \xi]$, for $i = 0, \dots, t$ and where U and $\xi = (\xi_1, \dots, \xi_m)$ are variables. We may assume that φ is just one such disjunct (29). Let X denote the closed subscheme of $\mathbf{A}^m_R$ defined by the ideal $(f_1(\pi, \xi), \dots, f_t(\pi, \xi))$, that is to say,

$$X = \operatorname{Spec}(R[\xi]/(f_1(\pi, \xi), \dots, f_t(\pi, \xi)). \tag{30}$$

Let W be the Zariski open subset of X defined by the extra condition $f_0(\pi, \xi) \neq 0$. We have to exhibit an algorithm which verifies whether or not W admits an R-rational point. Using Lemma 4.2, we may even assume that X_K is reduced, where as always

$$X_K \cong \operatorname{Spec}(K[\xi]/(f_1(\pi, \xi), \dots, f_t(\pi, \xi)) \tag{31}$$

is the generic fibre of X.

Apply Conjecture 1 to the reduced scheme X_K to obtain a morphism $h\colon V \to X_K$ of schemes of finite type over K, such that h is a blowing up defined over K, and V is non-singular. Moreover, by Remark 4.1, there is a computable function that calculates this desingularization h, since X_K is defined over the field of fractions of R_0. By clearing denominators in the defining equations of the centre, we can find a scheme Y of finite type over $\operatorname{Spec} R$ (in fact, over R_0) and a blowing up $f\colon Y \to X$ with nowhere dense centre Z defined over R, such that $Y_K \cong V$ and the base change f_K of f coincides with h.

The algorithm now works as follows, by induction on the dimension of X. Check first whether $W \cap Z$ admits an R-rational point, using the induction hypothesis on the lower dimensional scheme Z. If a solution exists, we are done. So assume no such solution exists. We then check whether Y admits an R-rational point using Proposition 3.5. Suppose we found an R-rational point on Y. Since V is non-singular, the underlying point of an arbitrary R-rational point on Y is non-singular. Therefore, using Theorem 2.4, it follows that also the non-empty open subset $f^{-1}(W) - f^{-1}(Z)$ admits an R-rational point y. Since f is defined over R, it follows that $f \circ y$ is an R-rational point on W and we are done.

Finally, suppose neither does there exist an R-rational point on Y. I claim that in that case W does not admit an R-rational point. Indeed, assume that x is an R-rational point on W. By our first assumption, x must be an R-rational point on the open $X - Z$. Therefore, the underlying point x_K of x does not belong to Z_K. Since f is an isomorphism outside Z, so is $h = f_K$ outside Z_K. Hence there exists exactly one (K-rational) point w on Y_K with $h(w) = x_K$. By Proposition 2.2 and the fact that f is proper ([11, Chapter II Proposition 7.16]), there exists therefore an R-rational point on Y (lifting x), contradiction. □

4.4. Remark The restriction on R to be equicharacteristic comes from the same restriction in Proposition 3.5. However, using the remark following that Proposition, we can extend the above Theorem to the case that R has mixed characteristic with finite residue field, provided the mixed characteristic analogue of Theorem 3.1 holds. A similar remark applies to Theorem 5.2 below.

5 General Existential Sentences

5.1. Definition Let X be a reduced scheme of finite type over a field K. The *smooth stratification* of X is the chain of closed subsets

$$\emptyset = X_0 \subset X_1 \subset X_2 \subset \cdots \subset X_h \subset X_{h+1} = X \qquad (32)$$

where each X_i is the non-smooth locus of X_{i+1}, for $i = 1, \dots, h$. Note that using the Jacobian Criterion for smoothness [16, Theorem 30.3], the non-smooth locus is closed. Moreover, given defining equations for X, one calculates the smooth stratification of X using this Jacobian Criterion.

We define the *bad locus* Σ of X as the union of all smooth connected components of some X_i, where i ranges from 1 to h. Note that this union is in fact a disjoint union. Indeed, let F be a smooth connected component of X_i, for some $i = 1, \dots, h$, and let F' be another smooth connected component of $X_{i'}$, for some $i' = 1, \dots, h$. If $i = i'$ but $F \neq F'$, then clearly F and F' are disjoint, so we may assume $i' < i$. Since F is smooth, it is disjoint from X_{i-1} whence from $X_{i'}$, so that $F \cap F' = \emptyset$, proving our claim. In particular, the bad locus is itself a smooth scheme and its connected components are irreducible. The latter is a consequence of the fact that a smooth and connected scheme is irreducible.

For example, if the non-smooth locus of X consists of three lines forming a triangle together with a fourth line disjoint from these three, then the bad locus consists of the three vertices of the triangle together with the fourth line.

In this paper, we will say that an open subset W of X *lies in general position*, if its intersection with the bad locus is everywhere dense in the bad locus. Note that this means that the complement $X - W$ of W does not contain any irreducible component of the bad locus. For instance, for the example in the previous paragraph, W will be in general position if it contains the three vertices and intersects the fourth line.

Let R be a domain with field of fractions K. Let $f_i \in R[\xi]$, for $i = 0, \dots, t$, with $\xi = (\xi_1, \dots, \xi_m)$ variables. Let X be the closed subscheme of $\mathbb{A}^m_R$ defined by the ideal $(f_1, \dots, f_t)$. In other words, X has affine coordinate ring $R[\xi]/(f_1, \dots, f_t)$. Let W be the open in X given by the extra condition $f_0 \neq 0$. We will say that the existential sentence

$$(\exists \xi) f_1(\xi) = f_2(\xi) = \cdots = f_t(\xi) = 0 \wedge f_0(\xi) \neq 0 \tag{33}$$

is *general*, if W_K lies in general position on the reduction of X_K, where as always a subscript K indicates the generic fibre of a scheme, that is to say, the base change over K. We call an arbitrary existential sentence *general*, if it is a disjunction of general sentences of the form (33).

5.2. Theorem *Let R be an excellent equicharacteristic Henselian local domain. Let $\mathbf{u}$ be a k-tuple in R. There is an algorithm relative to the residue field of R and the $\mathcal{L}(\mathbf{u})$-diagram of R, which decides whether a general existential sentence with parameters $\mathbf{u}$, holds in R.*

Proof Let κ be the residue field of R and $\mathfrak{m}$ its maximal ideal. Let K denote the field of fractions of R. Let $U = (U_1, \dots, U_k)$ be a k-tuple of variables. Let φ be a general existential sentence with parameters $\mathbf{u}$. The theorem then states that there is an algorithm deciding whether φ holds in R, where the algorithm is allowed to use the existential theory of κ and the equational theory of the subring generated by $\mathbf{u}$ as oracles, that is to say, we may assume that we know how to decide whether an (arbitrary) existential sentence is true over κ and whether a polynomial $h(U)$ with integer coefficients vanishes on $\mathbf{u}$ in R.

Let φ be an arbitrary general existential sentence. In other words, φ is a disjunction of general sentences of the form

$$(\exists \xi) f_1(\mathbf{u}, \xi) = f_2(\mathbf{u}, \xi) = \cdots = f_t(\mathbf{u}, \xi) = 0 \wedge f_0(\mathbf{u}, \xi) \neq 0 \tag{34}$$

with $f_i \in \mathbb{Z}[U, \xi]$, for $i = 0, \dots, t$ and where $\xi = (\xi_1, \dots, \xi_m)$ is a tuple of variables. In order to prove the theorem, we may assume that φ is just one such disjunct (34). Let X denote the closed subscheme of $\mathbf{A}^m_R$ defined by the ideal $(f_1(\mathbf{u}, \xi), \dots, f_t(\mathbf{u}, \xi))$ and let W be the Zariski open subset of X defined by the extra condition $f_0(\mathbf{u}, \xi) \neq 0$. By definition, W_K lies in general position on the reduction of X_K. Using Lemma 4.2, we may assume that X_K is actually reduced (the sentence corresponding to this new X is equivalent over R with the original φ).

Choose an increasing sequence of closed subschemes

$$\emptyset = X_0 \subset X_1 \subset X_2 \subset \cdots \subset X_h \subset X_{h+1} = X \tag{35}$$

so that their generic fibers form the smooth stratification of X_K. Recall that this means that $(X_1)_K$ and all the open subsets $(X_{i+1})_K - (X_i)_K$, for $i = 1, \dots, h$ are smooth over K. Moreover, using the Jacobian Criterion for smoothness [16, Theorem 30.3], such a sequence can effectively be constructed from the f_i, modulo the $\mathcal{L}(\mathbf{u})$-diagram of R.

We next describe the algorithm that will verify whether or not W admits an R-rational point. First check whether X_1 has an R-rational point using Proposition 3.5. If there is an R-rational point on X_1, we stop and let the output of our algorithm be **yes**. If not, we check, using Proposition 3.5 again, whether X_2 has an R-rational point. If it does, we stop and let the output be **yes**, otherwise we continue. At each stage, we check for the existence of an R-rational point on X_i using Proposition 3.5, stop when such a point exists and give the output **yes**, or continue otherwise. If we exhausted all the X_i (including the final $X_{h+1} = X$) and still have not found an R-rational point, we conclude that W has no R-rational point, so we stop and give the output **no**.

Let us verify the correctness of this algorithm. Obviously, if an R-rational point on W exists, then the algorithm will give output **yes**. Conversely, if the output is **yes**, then at some stage $i \in \{1, \dots, h+1\}$, we found an R-rational point x in X_i, but no R-rational point was found in X_{i-1}. Therefore x lies in $X_i - X_{i-1}$. Hence its underlying point x_K lies in $(X_i)_K - (X_{i-1})_K$ whence is a smooth point of $(X_i)_K$. By Theorem 2.4, the R-rational points are therefore dense on X_i in a neighbourhood of x. More precisely, there is an open V of X_i which is defined over R and admits x as an R-rational point, such that if $W \cap V$ is non-empty (in the scheme-theoretic sense), then $W \cap V$ admits also an R-rational point. Therefore we established the validity of the algorithm, provided we can show that $W \cap V$ is non-empty.

To this end, let F be an irreducible component of X_i. By construction of the bad locus, we can find an irreducible component Z of the bad locus of X_K with $Z \subset F_K$. Our general position assumption implies that $Z \cap W_K$ is non-empty. Therefore, $F_K \cap W_K$ whence $F \cap W$ is non-empty and therefore $F \cap W$ is dense in F. Since this holds for every irreducible component of X_i, it follows that $W \cap X_i$ is dense in X_i, so that $W \cap V$ is non-empty, as required. □

References

1. S. Abhyankar, *Resolution of singularities of embedded algebraic surfaces*, Pure and Applied Math., vol. 24, Academic Press, New York, 1966.
2. M. Artin, *Algebraic approximation of structures over complete local rings*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 23–58.
3. J. Ax and S. Kochen, *Diophantine problems over local fields I, II*, Amer. J. Math. **87** (1965), 605–630, 631–648.
4. J. Becker, J. Denef, L. van den Dries, and L. Lipshitz, *Ultraproducts and approximation in local rings I*, Invent. Math. **51** (1979), 189–203.
5. E. Bierstone and P.D. Milman, *Canonical desingularization in characteristic zero by blowing up the maximal strata of a local invariant*, Invent. Math. **128** (1997), 207–302.
6. J. Denef and L. Lipshitz, *Ultraproducts and approximation in local rings II*, Math. Ann. **253** (1980), 1–28.
7. Y. Eršhov, *On the elementary theory of maximal normed fields I*, Algebra i Logica **4** (1965), 31–69.
8. ______, *On the elementary theory of maximal normed fields II*, Algebra i Logica **5** (1966), 8–40.

9. ———, *On the elementary theory of maximal normed fields III*, Algebra i Logica **6** (1967), 31–37.
10. M. J. Greenberg, *Rational points in henselian discrete valuation rings*, Inst. Hautes Études Sci. Publ. Math. **31** (1966), 59–64.
11. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977.
12. H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Ann. of Math. **79** (1964), 109–326.
13. W. Hodges, *Model theory*, Cambridge University Press, Cambridge, 1993.
14. F.-V. Kuhlmann, *Elementary properties of power series fields over finite fields*, Fields Institute Preprint Series, 1998.
15. H. Matsumura, *Commutative algebra*, W.A. Benjamin, 1970.
16. ———, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986.
17. J. Milne, *Etale cohomology*, 33, Princeton Math., 1980.
18. D. Popescu, *General Néron desingularization and approximation*, Nagoya Math. J. **104** (1986), 85–115.
19. M. Raynaud, *Anneaux locaux henséliens*, Lect. Notes in Math., Springer-Verlag, 1970.
20. K. Schmidt and L. van den Dries, *Bounds in the theory of polynomial rings over fields. A non-standard approach*, Invent. Math. **76** (1984), 77–91.
21. H. Schoutens, *Reduction modulo p of power series with integer coefficients*, preprint available on URL address http://www.math.ohio-state.edu/~schoutens/Postscript/IntegerPowerSeries.ps, 2001.
22. M. Spivakovsky, *Smoothing of ring homomorphisms, approximation theorems, and the Bass-Quillen conjecture*, preprint.
23. R. Swan, *Néron-Popescu desingularization*, expanded notes from a Univ. of Chicago series of lectures, Spring 1995.