Annals of Pure and Applied Logic ••• (••••) •••–•••

Contents lists available at ScienceDirect

Annals of Pure and Applied Logic

www.elsevier.com/locate/apal

Direct twisted Galois stratification

Ivan Tomašić

School of Mathematical Sciences, Queen Mary University of London, London, E1 4NS, United Kingdom

ARTICLE INFO

Article history:
Received 9 May 2017
Accepted 16 July 2017
Available online xxxx

MSC:
primary 03C10, 12H10
secondary 11G25, 14G15

Keywords:
Difference scheme
Galois stratification
Galois formula
Frobenius automorphism
ACFA

ABSTRACT

The theory ACFA admits a primitive recursive quantifier elimination procedure. It is therefore primitive recursively decidable.

1. Introduction

1.1. Background

The role of our work in Model Theory of fields with powers of Frobenius and existentially closed difference fields is analogous to the role that Galois stratification of Fried, Haran, Jarden and Sacerdote ([7,5,6]), played in Model Theory of finite and pseudofinite fields, providing a more precise form, as well as the effectivity of quantifier elimination. In this light, our work will have an impact in the study of exceptional difference polynomials, difference version of Davenport's problem, graphs definable in fields with Frobenii and existentially closed difference fields, and many other areas inspired by applications of the classical Galois stratification over finite and pseudofinite fields.

In papers [18] and [17], we developed a theory of twisted Galois stratification for generalised difference schemes, and we established a rather *fine quantifier elimination* result, stating that every first-order formula in the language of difference rings is equivalent to a *Galois formula* modulo the theory ACFA of existentially

E-mail address: i.tomasic@qmul.ac.uk.

http://dx.doi.org/10.1016/j.apal.2017.07.002
0168-0072/

closed difference fields, where the latter formulae are associated with *finite* Galois covers of difference schemes. We argued that the elimination procedure was *effective* in the sense that it was primitive recursive reducible to a few natural operations in difference algebra (the status of which is unknown at the moment).

In this paper, we develop *direct twisted Galois stratification* in the context of direct presentations of difference schemes, which approximates the difference scheme framework to a sufficient order. We show a slightly coarser quantifier elimination result, Theorem 5.9, which (informally) states that

> every first-order formula is equivalent to a *direct Galois formula* modulo ACFA, or over the fields with Frobenii,

where the latter formulae are associated with direct Galois covers. Even though the class of direct Galois formulae is coarser than that of Galois formulae, direct Galois formulae are equivalent (4.16) to the $\exists_1$-formulae that appear after the known *logic quantifier elimination* for ACFA from [12] and [3].

Our main result (Theorems 6.7 and 6.10) is that

> the quantifier elimination procedure for ACFA and for fields with Frobenii is *primitive recursive*.

Given that working with direct presentations essentially reduces to working with algebraic varieties and correspondences between them, this follows by applying methods of classical effective/constructive algebraic geometry in our framework. Consequently, ACFA and the first-order theory of fields with Frobenii are decidable by a primitive recursive procedure, see Corollaries 6.8 and 6.12.

The present paper is not a variant of [18] and [17] since the whole machinery of direct Galois covers had to be developed from first principles, which is significantly more intricate than previous considerations involving difference schemes. There is no direct interaction with the methods of the previous papers, they only provide ideological guidance to identify the main conceptual steppingstones in the stratification procedure.

1.2. Direct presentations of difference schemes

Let (k, ς) be a difference field, let X be an algebraic variety over k, let X_ς denote the base change of X via $\varsigma : k \to k$, and let $W \subseteq X \times X_\varsigma$ be a closed subvariety. Let (F, φ) be any difference field extending (k, ς). The intuitive idea that sets of the form

$$\{x \in X(F) : (x, x\varphi) \in W\}$$

should correspond to sets of (F, φ)-points of a 'difference variety' has been around from the beginning of research on difference algebra, and it was particularly useful in the model-theoretic study of difference fields, as in [12] and [3].

Although the above data determines a 'directly presented difference scheme' defined in [10], we choose to minimise the use of the framework of difference schemes, and remain in the context of their *direct presentations*, using the classical language of algebraic schemes and correspondences (we only use difference schemes to control parameters, since the alternative leads to rather cumbersome notation). The benefit of this approach is that we can profit from the methods of effective algebraic geometry in order to prove that our constructions are primitive recursive.

1.3. Generalised difference schemes

The logic quantifier elimination mentioned above states that a first-order formula in the language of difference rings is equivalent to an existential formula modulo ACFA. Intuitively, such a formula chooses

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

one of the finitely many possible behaviours of the difference operator on some finite difference ring extension. We encode such an extension through the notion of a *Galois cover* of direct presentations

$$(X, \Sigma) \to (Y, \sigma),$$

where Σ is the set of all possible lifts of the difference operator σ from Y to the 'finite' cover X. The choice of a lift $\tilde{\sigma} \in \Sigma$ 'up to isomorphism', i.e., up to the action of the associated Galois group G amounts to the choice of a G-conjugacy class C in Σ. Hence the data

$$\langle (X, \Sigma)/(Y, \sigma), C \rangle$$

constitutes the basic building blocks of our Galois formulae.

In order to afford the existence of Galois covers and to provide a notational device for discussing several possible lifts of the difference operator, we must make our framework flexible enough to include presentations of *generalised difference schemes*, developed in [16]. Having that in mind, the real difficulty of this project is to isolate a robust enough notion of a Galois cover which will perpetuate through a number of operations and constructions (cf. Subsection 3.4).

1.4. Organisation of the paper

In Section 2 we define (generalised) direct presentations of difference schemes and their morphisms, and consider their structure and basic properties.

In Section 3, we define direct Galois covers of direct presentations, consider their basic properties, and show their permanence properties under the constructions needed in the sequel.

In Section 4, we define direct Galois stratifications and their associated formulae, and give a preliminary comparison of Galois formulae to first-order formulae over existentially closed difference fields (and asymptotically over fields with powers of Frobenius).

This work is completed in Section 5, where we prove a direct image theorem (Corollary 5.8), stating that the direct image of a Galois formula by a morphism of direct presentations is equivalent modulo ACFA (or fields with Frobenius) to a Galois formula. Given that existential quantification can be thought of as taking direct images via projections, this immediately implies a quantifier elimination result for the class of Galois formulae, and shows that it coincides with the class of first-order formulae (5.9). We compute direct images along arbitrary morphisms, rather than just projections, in order to benefit from general decompositions of morphisms which allow us to reduce the computation to manageable cases 5.3 and 5.4/5.5.

In Section 6, we review the preceding sections with our 'effective goggles' on and argue that the quantifier elimination procedure reduces to the known constructions in effective algebraic geometry and is therefore primitive recursive (6.7). We show how to draw consequences in effective/constructive difference algebra by proving that the *perfect ideal membership problem* is primitive recursive (6.13).

Finally, Appendix A gives a comparison of the framework of direct presentations and that of directly presented difference schemes.

2. Directly presented difference schemes

In view of the explanation from the Introduction that we shall be working with direct presentations rather than the associated difference schemes, the title of this section is symbolic and hints at the fact that we borrowed the adjective 'direct' from Hrushovski, and that our framework ties in nicely with that of directly presented schemes, as discussed in the Appendix.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

In the sequel, all rings are commutative with identity. By an *algebraic variety* over a ring R, we will mean a reduced separated scheme of finite presentation over $\mathrm{Spec}(R)$, and morphisms of varieties are assumed to be locally of finite presentation.

2.1. Difference rings

A *difference ring* is a pair

$$(R, \varsigma)$$

consisting of a ring R and an endomorphism $\varsigma : R \to R$.

A difference ring homomorphism

$$f : (R, \varsigma) \to (R', \varsigma')$$

is a ring homomorphism $f : R \to R'$ satisfying

$$\varsigma' f = f \varsigma.$$

Definition 2.1. A difference ring (R, ς) is called:

(1) *inversive*, if ς is bijective;
(2) a *transformal domain*, if R is a domain and ς is injective;
(3) a *difference field*, if R is a field.

Fact 2.2 *([4, Chapter 2, Theorem II]). Every difference ring (R, ς) with ς injective has an* inversive closure $(R^{\mathrm{inv}}, \varsigma^{\mathrm{inv}})$ *with the following universal property. There is an embedding $(R, \varsigma) \hookrightarrow (R^{\mathrm{inv}}, \varsigma^{\mathrm{inv}})$ such that every morphism $(R, \varsigma) \to (S, \tau)$ to an inversive difference ring factors through R^{inv}.*

Notation 2.3. Let (R, ς) be a transformal domain. We write

$$R_{-n} = (\varsigma^{\mathrm{inv}})^{-n}(R),$$

considered as a difference subring of R^{inv}.

Remark 2.4. Let (R, ς) be a difference ring, and let $S \subseteq R$ be a multiplicatively closed subset with $\varsigma(S) \subseteq S$. Then the localisation

$$S^{-1}R$$

has a natural structure of a difference ring.

Definition 2.5. Let (R, ς) be a transformal domain.

(1) A (finite) ς-localisation of R with respect to $f \in R \setminus \{0\}$ is the difference ring $S^{-1}R$, where S is the multiplicative set generated by $\{\varsigma^i(f) : i \in \mathbb{N}\}$.
(2) By convention, whenever we mention a *ς-localisation of R*, we shall mean a finite ς-localisation with respect to some f as above.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Definition 2.6. The *affine difference scheme* associated to a difference ring (R, ς) is

$$\mathrm{Spec}^{\varsigma}(R) = \{\mathfrak{p} \in \mathrm{Spec}(R) : \varsigma^{-1}(\mathfrak{p}) = \mathfrak{p}\},$$

together with the *Zariski topology*, as well as the structure sheaf, induced from $\mathrm{Spec}(R)$. It is the fixed point set of

$$\mathrm{Spec}(R, \varsigma) = (\mathrm{Spec}(R), {}^{a}\varsigma).$$

Write $\mathcal{S} = \mathrm{Spec}^{\varsigma}(R)$.

(1) For a point $s \in \mathcal{S}$, we write $\mathfrak{j}_s$ for the associated ς-prime ideal in R.
(2) The *local ring at* $s \in \mathcal{S}$ is just the (difference) localisation $R_{\mathfrak{j}_s}$, and its residue field $\mathbf{k}(s)$ is naturally a difference field, equipped with the induced endomorphism ς^s.
(3) A point $s \in \mathcal{S}$ is *closed*, if it is closed in the Zariski topology, i.e., if $\mathfrak{j}_s$ is maximal among the ς-prime ideals in R.

2.2. Direct presentations

Notation 2.7. Let (R, ς) be a difference ring, let $S = \mathrm{Spec}(R)$ and, by a slight abuse of notation, write ς for the scheme morphism ${}^{a}\varsigma : S \to S$ induced by ς. We write

$$(-)_{\varsigma} : \mathrm{Sch}_{/S} \to \mathrm{Sch}_{/S}$$

for the *base change functor via* ς. For an S-scheme Y, its ς-twist is

$$Y_{\varsigma} = Y \times_S S$$

as shown in the cartesian diagram

$$\begin{array}{ccc} Y_{\varsigma} & \to & Y \\ \downarrow & & \downarrow \\ S & \xrightarrow{\varsigma} & S \end{array}$$

and we extend the definition to morphisms in a natural way.

Definition 2.8. Let (R, ς) be a transformal domain, and write $S = \mathrm{Spec}(R)$. We define the category of *almost direct presentations* $\mathscr{D}^{\mathrm{a}} = \mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ as follows.

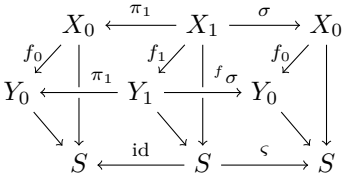
(1) An object (X, Σ) consists of S-schemes X_0 and X_1 and a collection of commutative diagrams of scheme morphisms

$$\begin{array}{ccccc} X_0 & \xleftarrow{\pi_1} & X_1 & \xrightarrow{\sigma} & X_0 \\ \downarrow & & \downarrow & & \downarrow \\ S & \xleftarrow{\mathrm{id}} & S & \xrightarrow{\varsigma} & S \end{array}$$

indexed by $\sigma \in \Sigma$. Note that π_1 is a morphism of S-schemes, while each σ is only a ς-linear scheme morphism.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

(2) A morphism $f : (X, \Sigma) \to (Y, T)$ consists of a map ${}^f() : \Sigma \to T$ and S-morphisms $f_0 : X_0 \to Y_0$, $f_1 : X_1 \to Y_1$, making the diagram



commutative for every $\sigma \in \Sigma$.

The category of *direct presentations* is the full subcategory $\mathscr{D}$ of $\mathscr{D}^{\mathrm{a}}$ consisting of those objects (X, Σ) for which the diagram in (1) induces a closed immersion $X_1 \hookrightarrow X_0 \times_S X_0$ for every $\sigma \in \Sigma$.

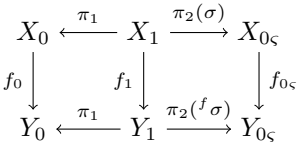
Definition 2.9. Let (R, ς) be a transformal domain, and write $S = \mathrm{Spec}(R)$. We define the category $\mathscr{D}^{\mathrm{av}} = \mathscr{D}^{\mathrm{av}}_{(R,\varsigma)}$ as follows.

(1) An object (X, Σ) consists of S-schemes X_0 and X_1 and a diagram of S-morphisms

$$X_0 \xleftarrow{\pi_1} X_1 \xrightarrow{\pi_2(\sigma)} X_{0\varsigma}$$

for every $\sigma \in \Sigma$.

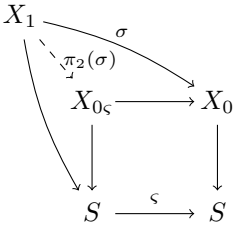
(2) A morphism $f : (X, \Sigma) \to (Y, T)$ consists of a map ${}^f() : \Sigma \to T$ and S-morphisms $f_0 : X_0 \to Y_0$, $f_1 : X_1 \to Y_1$, making the diagram



commutative for every $\sigma \in \Sigma$.

The category $\mathscr{D}^{\mathrm{v}}$ is the full subcategory of $\mathscr{D}^{\mathrm{av}}$ consisting of those objects (X, Σ) for which the diagram in (1) induces a closed immersion $X_1 \hookrightarrow X_0 \times_S X_{0,\varsigma}$ for every $\sigma \in \Sigma$.

Remark 2.10. The commutative diagram



yields an equivalence of categories between $\mathscr{D}^{\mathrm{a}}$ and $\mathscr{D}^{\mathrm{av}}$, as well as $\mathscr{D}$ and $\mathscr{D}^{\mathrm{v}}$. While the reader used to working with varieties might prefer to work in $\mathscr{D}^{\mathrm{av}}$, certain formalisms become tedious in that context. We

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

therefore work with $\mathscr{D}^{\mathrm{a}}$ and $\mathscr{D}^{\mathrm{av}}$ interchangeably, bearing in mind that the type of an object automatically reveals the category it belongs to.

2.3. Points, realisations, fibres

Notation 2.11. Let (R,ς) be a difference ring, and let (F,φ) be an (R,ς)-algebra (furnished with a morphism $(R,\varsigma)\to(F,\varphi)$). When needed, we consider $\mathrm{Spec}(F,\varphi)$ as the object

$$\mathrm{Spec}(F)\xleftarrow{\mathrm{id}}\mathrm{Spec}(F)\xrightarrow{\varphi}\mathrm{Spec}(F)$$

of $\mathscr{D}^{\mathrm{a}}$.

Definition 2.12. Let (X,Σ) be an object of $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ and let (F,φ) be an (R,ς)-algebra.

(1) The set of (F,φ)-*points* of (X,Σ) is

$$\begin{aligned}(X,\Sigma)(F,\varphi)&=\mathrm{Hom}_{\mathscr{D}^{\mathrm{a}}}(\mathrm{Spec}(F,\varphi),(X,\Sigma))\\&\simeq\{x_1\in X_1(F):\sigma x_1=\pi_1x_1\varphi,\text{ for some }\sigma\in\Sigma\},\end{aligned}$$

(2) The set of (F,φ)-*realisations* of an object (X,Σ) is

$$\begin{aligned}(X,\Sigma)^\sharp(F,\varphi)&=\{x_0\in X_0(F):x\in(X,\Sigma)(F,\varphi)\}\\&\simeq\pi_1\{x_1:x_1\in X_1(F),\ \sigma x_1=\pi_1x_1\varphi,\text{ for some }\sigma\in\Sigma\}.\end{aligned}$$

Remark 2.13. The category $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ has products. Indeed, if (X,Σ) and (X',Σ') are objects of $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$, then, writing $S=\mathrm{Spec}(R)$,

$$(X_0\times_S X_0',X_1\times_S X_1',\Sigma\times\Sigma')$$

is their product in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$.

Definition 2.14. Let (X,Σ) be an object of $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ and let $s\in\mathrm{Spec}^\varsigma(R)$. Then we consider $\mathrm{Spec}(\mathbf{k}(s),\varsigma^s)$ as an object in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$, and we define the *fibre* (X_s,Σ_s) as the product

$$(X,\Sigma)\times_{\mathrm{Spec}(R,\varsigma)}\mathrm{Spec}(\mathbf{k}(s),\varsigma^s),$$

considered as an object of $\mathscr{D}^{\mathrm{a}}_{(\mathbf{k}(s),\varsigma^s)}$.

Remark 2.15. It is often beneficial to view an object (X,Σ) of $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ as a family of objects (X_s,Σ_s) parametrised by points $s\in\mathcal{S}=\mathrm{Spec}^\varsigma(R)$.

If $x\in(X,\Sigma)(F,\varphi)$ as in 2.12 with F a field, then it implicitly determines a homomorphism $(R,\varsigma)\to(F,\varphi)$, whose kernel is a ς-prime ideal corresponding to some $s\in\mathcal{S}$ and (F,φ) extends $(\mathbf{k}(s),\varphi^s)$, so in fact we could write $x\in X_s(F,\varphi)$. Later on, when we become more mindful about the role of parameters, we may choose a parameter $s\in\mathcal{S}$ first, and then a field (F,φ) extending $(\mathbf{k}(s),\varsigma^s)$.

Remark 2.16. For a direct presentation (X,σ), we have a bijection

$$(X,\sigma)^\sharp(F,\varphi)\simeq(X,\sigma)(F,\varphi).$$

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Intuitively speaking, the set of (F,φ)-points of a 'directly presented difference scheme' associated with a direct presentation (X,σ) coincides with those in the above Remark (the precise statement is A.8). This justifies somewhat our habit to refer to the objects of $\mathscr{D}^{\mathrm{a}}$ as '(almost) directly presented difference schemes'.

2.4. Functors of points and realisations

Remark 2.17. Let (X,Σ) be an object of $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$. Items (1) and (2) from 2.12 define the functors

$$(X,\Sigma)^{\flat} \quad \text{and} \quad (X,\Sigma)^{\sharp}$$

from the category of (R,ς)-algebras to the category of sets. We shall write X in place of $X^{\flat}$ whenever it is clear from the context that we wish to refer to the functor of points.

We extend the above notation to a context suitable for our intended arithmetical applications.

Definition 2.18. Let (R,ς) be a transformal domain. We consider a category consisting of pairs

$$(s,(F,\varphi)),$$

where s ranges in a subset of $\mathrm{Spec}^{\varsigma}(R)$ and (F,φ) belongs to a chosen class of difference fields extending $(\mathbf{k}(s),\sigma^s)$. A morphism between $(s,(F,\varphi))$ and $(s',(F',\varphi'))$ exists only when s is a specialisation of s', and it is then given by a diagram

$$\begin{array}{ccc} F & \longrightarrow & F' \\ \uparrow & & \uparrow \\ \mathbf{k}(s) & \longrightarrow & \mathbf{k}(s') \end{array}$$

of difference field extensions.

The *points functor* $X^{\flat}$ and the *realisation functor* $X^{\sharp}$ associated to an object (X,σ) of $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ are set-valued functors on the above category defined by

(1) $X^{\flat}(s,(F,\varphi)) = X_s(F,\varphi)$;
(2) $X^{\sharp}(s,(F,\varphi)) = X^{\sharp}_s(F,\varphi)$,

so that we have the relation

$$X^{\sharp}_s(F,\varphi) = \pi_{1,s}\{x_1 : x \in X_s(F,\varphi)\} = \{x_0 : x \in X_s(F,\varphi)\}.$$

An (R,ς)-*subassignment* of $X^{\sharp}$ is any subfunctor $\mathcal{F}$ of $X^{\sharp}$. Namely, for any $(s,(F,\varphi))$ as above,

$$\mathcal{F}(s,(F,\varphi)) \subseteq X^{\sharp}_s(F,\varphi),$$

and for any $u : (s,(F,\varphi)) \to (s',(F',\varphi'))$, $\mathcal{F}(u)$ is the restriction of $X^{\sharp}(u)$ to $\mathcal{F}(s,(F,\varphi))$. Similarly we define subassignments of $X^{\flat}$.

Note that, in view of 2.15, the functors from 2.18 are just restrictions of those from 2.17 to appropriate subcategories of the category of (R,ς)-algebras.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

2.5. Properties of directly presented schemes

Definition 2.19. Let $f : (X, \sigma) \to (Y, \sigma)$ be a morphism in $\mathscr{D}^{\mathrm{av}}_{(R,\varsigma)}$, let P be a property of R-schemes, and let P' be a property of morphisms of R-schemes. We say that X is *directly* P, if X_0, X_1 and $X_{0\varsigma}$ have the property P. Similarly, we say that f is *directly* P', if the morphisms $f_0 : X_0 \to Y_0$, $f_1 : X_1 \to Y_1$ and $f_{0\varsigma} : X_{0\varsigma} \to Y_{0\varsigma}$ all have property P'.

In particular, an object (X, σ) od $\mathscr{D}^{\mathrm{av}}_{(R,\varsigma)}$ is called a *direct variety* if X_0 and X_1 are R-varieties.

Definition 2.20. A direct variety (X, σ) is *H-direct*, if it is directly integral and the projections $\pi_1 : X_1 \to X_0$ and $\pi_2(\sigma) : X_1 \to X_{0\varsigma}$ are both dominant.

2.6. Decomposition into direct components

The following 'direct decomposition' algorithm is so natural that variants of it already appeared in numerous sources, for example as [4, Solution to Problem I*, Chapter 8, No. 14], [9, Proposition 2.2.1] and [14, Lemma 3.6].

Proposition 2.21. *Let (X, σ) be a direct variety in $\mathscr{D}^{\mathrm{av}}_{(R,\varsigma)}$, where (R, ς) is a transformal domain. Let η be the generic point of* $\mathrm{Spec}^{\varsigma}(R)$ *and write X_η for the generic fibre of X over R. We can find a finite number of H-direct directly closed subschemes (Y_i, σ) defined over a ς-localisation R' of $R_{-\dim(X_{0,\eta})}$ such that, for every difference field (F, φ) over (R', ς),*

$$X^\sharp(F, \varphi) = \cup_i Y_i^\sharp(F, \varphi).$$

Proof. Suppose (X, σ) is given by a correspondence $X_0 \xleftarrow{\pi_1} W \xrightarrow{\pi_2} X_{0\varsigma}$. By decomposing W_η into irreducible components and ς-localising R, we may assume W is irreducible. Let X_1 be the Zariski closure of $\pi_1(W)$ in X_0, and let X_2 be the Zariski closure of $\pi_2(W)$ in $X_{0\varsigma}$. It follows that X_1 and X_2 are irreducible. If $X_{1\varsigma} = X_2$ the construction ends with the H-direct $X_1 \xleftarrow{\pi_1} W \xrightarrow{\pi_2} X_{1\varsigma}$.

Otherwise, we consider the presentation (X', σ) determined by $X'_0 \leftarrow W' \to X'_{0\varsigma}$, where $X'_0 = X_1 \cap X_{2\varsigma^{-1}}$ and $W' = (X'_0 \times X'_{0\varsigma}) \times_{X_0 \times X_{0\varsigma}} W$ are both defined over R_{-1}. It is straightforward to verify that $(X, \sigma)^\sharp(F, \varphi) = (X', \sigma)^\sharp(F, \varphi)$ for any suitable (F, φ). Moreover, denoting by η' the generic point of $\mathrm{Spec}^{\varsigma}(R_{-1})$, since $\dim(X'_{0,\eta'}) < \dim(X_{0,\eta'}) = \dim(X_{0,\eta})$, we can continue by induction on dimension which clearly ends in at most $\dim(X_{0,\eta})$ steps.

2.7. Local properties of directly presented schemes

In this subsection we work over a transformal domain (R, ς), and we implicitly allow a ς-localisation of R in every step that requires it.

Proposition 2.22. *Let $f : (X, \sigma) \to (Y, \sigma)$ be a morphism of direct varieties in $\mathscr{D}^{\mathrm{a}}$, and let P be a local property of morphisms of algebraic schemes (varieties) which is stable under base change.*

(1) *If P is generic in the target, then the property of being directly P is directly generic in the target.*
(2) *If P is generic in the source, then the property of being directly P is directly generic in the source.*

Proof. For (1), by genericity in the target, let $V_i \subseteq Y_i$ be open such that $f_i \restriction_{f_i^{-1}(V_i)}$ has property P, for $i = 0, 1$. By base change, $V_{0\varsigma}$ works for $f_{0\varsigma}$. Let $V = \pi_1^{-1}(V_0) \cap \pi_2^{-1}(V_{0\varsigma}) \cap V_1$. Then

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

$$\begin{array}{ccccc} f_0^{-1}(V_0) & \leftarrow & f_1^{-1}(V) & \rightarrow & f_{0\varsigma}^{-1}(V_{0\varsigma}) \\ \downarrow & & \downarrow & & \downarrow \\ V_0 & \longleftarrow & V & \longrightarrow & V_{0\varsigma} \end{array}$$

is directly P.

In the case (2) of genericity in the source, let $V_i \subseteq Y_i$, $U_i \subseteq X_i$ be open such that $f_i \restriction_{U_i \cap f_i^{-1}(V_i)}$ has property P, for $i = 0, 1$. By base change, $V_{0\varsigma}$ and $U_{0\varsigma}$ work for $f_{0\varsigma}$. Let $V = (\pi_1^Y)^{-1}(V_0) \cap (\pi_2^Y)^{-1}(V_{0\varsigma}) \cap V_1$ and $U = (\pi_1^X)^{-1}(U_0) \cap (\pi_2^X)^{-1}(U_{0\varsigma}) \cap U_1$. Then

$$\begin{array}{ccccc} U_0 \cap f_0^{-1}(V_0) & \leftarrow & U \cap f_1^{-1}(V) & \rightarrow & U_{0\varsigma} \cap f_{0\varsigma}^{-1}(V_{0\varsigma}) \\ \downarrow & & \downarrow & & \downarrow \\ V_0 & \longleftarrow & V & \longrightarrow & V_{0\varsigma} \end{array}$$

is directly P.

Corollary 2.23. *Let $f : (X, \sigma) \to (Y, \sigma)$ be a morphism of direct varieties in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$.*

(1) *If f is a map of directly integral schemes which has directly generically integral fibres, there is a direct localisation of (Y, σ) over which f is directly universally submersive (cf. 3.9, 3.10) with geometrically integral fibres.*
(2) *If f is directly generically étale, there is a direct localisation of (Y, σ) over which f is directly finite étale.*
(3) *If f is directly generically smooth, there is a direct localisation X' of X and Y' of Y such that $f \restriction_{X' \cap f^{-1}(Y')}$ is directly smooth.*
(4) *If (X, σ) is directly generically smooth (over (R, ς)), there is a direct localisation of X which is directly normal.*

Proposition 2.24. *Let $f : (X, \sigma) \to (Y, \sigma)$ be a morphism of direct varieties in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ and let P be a property of morphisms of algebraic schemes which is generic in the source (or target). There exist stratifications of (X, σ) and (Y, σ) into finitely many directly integral locally closed sub-objects (X_i, σ), (Y_j, σ) (defined over a ς-localisation of some R_{-n}) such that each restriction $f_i : (X_i, \sigma) \to (Y_{f(i)}, \sigma)$ of f is directly P.*

Proof. By 2.21 we may assume that X and Y are directly integral, and by 2.22, we find localisations (U, σ) of X and (V, σ) of Y so that $f \restriction_U : U \to V$ is directly P. In the remaining complement

$$\begin{array}{ccccc} X_0 & \longleftarrow & X_1 \setminus U_1 & \longrightarrow & X_{0\varsigma} \\ \downarrow & & \downarrow & & \downarrow \\ Y_0 & \longleftarrow & \overline{f_1(X_1 \setminus U_1)} & \longrightarrow & Y_{0\varsigma} \end{array}$$

the dimension of $X_1 \setminus U_1$ is strictly lower than the dimension of X_1, and we continue by devissage.

3. Direct Galois covers

3.1. Classical Galois covers

We recall Grothendieck's theory of the étale fundamental group and extract some of the basic properties of Galois covers.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

All schemes in this subsection are assumed to be locally noetherian. A finite étale morphism $X \to Y$ is called an *étale cover*. If X and X' are two étale covers of Y, we say that X *dominates* X', if there exists a Y-morphism $X \to X'$.

Definition 3.1. Let S be a scheme, and let $\bar{s} \in S(\Omega)$ be a geometric point of S (where Ω is an algebraically closed field). Let $F = F_{\bar{s}} : \text{Ét}(S) \to \text{Set}$ be the *fibre functor* from the category of étale covers of S to the category of sets given by

$$F_{\bar{s}}(X) = X_s = X \times_S \text{Spec}(\Omega).$$

The *étale fundamental group* of S (with base point $\bar{s}$) is defined as the profinite group

$$\pi_1(S, \bar{s}) = \text{Aut}(F_{\bar{s}}).$$

Fact 3.2 *([8]). With the above notation, the fibre functor $F_{\bar{s}}$ defines an equivalence of categories between $\text{Ét}(S)$ and the category of $\pi_1(S, \bar{s})$-sets.*

If $f : S \to S'$ is a morphism, the base change along f functor $\text{Ét}(S') \to \text{Ét}(S)$ gives rise to a homomorphism

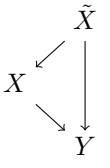
$$\pi_1(f) : \pi_1(S, \bar{s}) \to \pi_1(S', f(\bar{s})).$$

Definition 3.3. Let $X \to Y$ be a connected étale cover. Let $\bar{y}$ be a geometric point of Y, and let $F_{\bar{y}}(X) = X_{\bar{y}}$ be the geometric fibre of X over $\bar{y}$. We say that X is a *Galois cover* of Y if $\text{Aut}(X/Y)$ acts simply transitively on $F_{\bar{y}}(X)$.

Fact 3.4.

(1) *In the correspondence of 3.2, $X \to Y$ is a Galois cover if and only if $F_{\bar{y}}(X)$ is a transitive $\pi_1(Y, \bar{y})$-set.*
(2) *If X is a Galois cover of Y with group G, then $Y \simeq X/G$.*

Fact 3.5. *If $X \to Y$ is a connected étale cover, then there exists a least Galois cover $\tilde{X} \to Y$ which dominates X as in the diagram*



in the sense that any other Galois cover Z of Y that dominates X also dominates $\tilde{X}$. Such an $\tilde{X}$ is unique up to isomorphism and we call it the Galois closure of X over Y.

Fact 3.6 *([2, V §2.2, Corollaire à Th. 2]). Suppose G is a finite group acting on a ring A. Let f_1 and f_2 be two homomorphisms from A to a field L with the same restriction to A^G. Then there exists a $g \in G$ such that $f_2 = f_1 g$.*

Corollary 3.7. *Let $p : X \to Y$ be a Galois cover with group G, and $\phi_1, \phi_2 : Z \to X$ two morphisms from an integral scheme Z satisfying $p\phi_1 = p\phi_2$. Then there exists a $g \in G$ such that $\phi_2 = g\phi_1$.*

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Proof. We may assume that $X = \mathrm{Spec}(A)$, and that ϕ_i is associated to $f_i : A \to A$, $i = 1, 2$. Denote by j the inclusion of A in its fraction field. The previous Fact applied to jf_1 and jf_2 yields a $g \in G$ such that $jf_2 = jf_1 g$. Since j is injective, we deduce that $f_2 = f_1 g$, as required.

Corollary 3.8. *Suppose we have a commutative diagram*

$$\begin{array}{ccc} X & \xrightarrow{f} & X' \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ Y & \xrightarrow{h} & Y' \end{array}$$

where p and p' are Galois covers with groups G and G'. Then we have a homomorphism ${}^f(\,) : G \to G'$ such that, for $g \in G$,

$$ {}^f g\, f = f\, g.$$

Proof. For $g \in G$, we have that $p'fg = hpg = hp = p'f$. Thus, by 3.7, there is a unique element $g' \in G'$ such that $g'f = fg$. It is readily verified that the assignment $g \mapsto {}^f g = g'$ is a homomorphism.

Definition 3.9 *([8, IX.2.1]).* A morphism $f : S' \to S$ is *submersive* if it is surjective and makes S into a quotient topological space of S', i.e., a subset U of S is open if and only if $f^{-1}(U)$ is open in S'. A morphism is *universally submersive* if every base change of it remains submersive.

We will exploit the fact, proved in [8], that a faithfully flat quasi-compact morphism is universally submersive through the following.

Lemma 3.10. *Let $f : X \to Y$ be a dominant morphism of finite type of integral schemes whose generic fibre is geometrically integral. Then there is an open dense subset U of Y such that $f^{-1}(U) \to U$ is faithfully flat (so universally submersive) with geometrically integral fibres.*

Proof. Let U_1 be on open dense subset of Y such that f is flat over U_1 by generic flatness. Since f is dominant, there exists an open dense set U_2 such that f is surjective above U_2. By the constructibility of the property of being geometrically integral [1, Tag 0553, Tag 0574], we can find an open dense set U_3 such that over U_3, f has geometrically integral fibres. Then let $U = U_1 \cap U_2 \cap U_3$.

Lemma 3.11. *Let $f : X \to Y$ be an universally submersive morphism with geometrically connected fibres and assume Y is connected (whence it follows that X is connected). The base change functor $f^* : V \mapsto V \times_Y X$ from the category of étale covers of Y to the category of étale covers of X is fully faithful and it has a left adjoint f_*, i.e., for every étale cover $Z \to X$ we have a morphism $Z \to f_*Z$ inducing the natural isomorphism*

$$\mathrm{Hom}_Y(f_*Z, V) = \mathrm{Hom}_X(Z, f^*V),$$

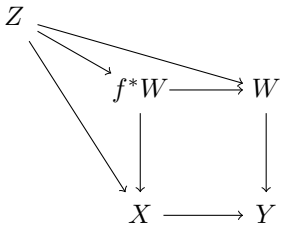
for every étale cover $V \to Y$.

Moreover, f^* and f_* take Galois covers to Galois covers and every Galois cover $Z \to X$ yields an exact sequence

$$1 \to \mathrm{Gal}(Z/f^*f_*Z) \to \mathrm{Gal}(Z/X) \to \mathrm{Gal}(f_*Z/Y) \to 1.$$

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Let $Z \to X$ be an étale cover as above. Note that the required f_*Z is the solution to the following universal problem. We need to show that there exists an étale cover $W \to Y$ completing the diagram



which is maximal in the sense that for any other étale cover $V \to Y$ which fits into an analogous diagram (i.e., $Z \to X$ dominates f^*V), $W \to X$ dominates $V \to X$. It will then follow that W is unique up to isomorphism and we will denote it by f_*Z.

Proof. The base change functor from étale covers of Y to étale covers of X induced by f is fully faithful by [8, IX.3.4].

If we choose a geometric point $\bar{x}$ in X mapping onto $\bar{y}$ in Y, it was proved in [8, IX.5.6] that the homomorphism

$$\pi_1(f) : \pi_1(X, \bar{x}) \to \pi_1(Y, \bar{y})$$

of étale fundamental groups is surjective.

Let us introduce some abstract notation associated with profinite group actions on finite sets. Given an epimorphism $\phi : \pi \to \pi'$ of profinite groups with kernel K, a π-set E and a π'-set E', we write

(1) ϕ^*E' for the set E' endowed with a π-action via ϕ;
(2) ϕ_*E for the set E/K endowed with a natural π'-action.

There is an obvious natural bijection

$$\mathrm{Hom}_{\pi'}(\phi_*E, E') \simeq \mathrm{Hom}_{\pi}(E, \phi^*E'). \qquad (\dagger)$$

Using this notation, given an étale cover $Z \to X$, we define f_*Z to be the étale cover of Y which corresponds via 3.2 to the $\pi_1(Y, \bar{y})$-set $\pi_1(f)_*F_{\bar{x}}(Z)$, i.e., to be the cover satisfying the property

$$F_{\bar{y}}(f_*Z) \simeq \pi_1(f)_*F_{\bar{x}}(Z).$$

On the other hand, if $V \to Y$ is an étale cover, we have that $F_{\bar{x}}(f^*V) \simeq F_{\bar{y}}(V)$ and f^*V clearly corresponds to the $\pi_1(X, \bar{x})$-set $\pi_1(f)^*F_{\bar{y}}(V)$, so the required adjunction is a formal consequence of (†) and 3.2.

If $V \to Y$ is Galois, if follows that f^*V is Galois since it is connected. If $Z \to X$ is Galois, then $\pi_1(X, \bar{x})$ acts transitively on $F_{\bar{x}}(Z)$, hence $\pi_1(Y, \bar{y})$ acts transitively on $\pi_1(f)_*F_{\bar{x}}(Z) = F_{\bar{y}}(f_*Z)$ and $f_*Z \to Y$ is Galois.

Note that the full faithfulness of f^* yields that for every Galois cover $V \to Y$, $\mathrm{Gal}(f^*V/X) \simeq \mathrm{Gal}(V/Y)$. The exact sequence follows from the particular case $V = f_*Z$.

Given the rather indirect flavour of the above proof making use of the theory the étale fundamental group and descent, let us give a direct construction of W under the additional hypothesis that X, Y and Z are normal and $X \to Y$ faithfully flat. The assumptions imply that $\mathbf{k}(X)$ is a regular extension of $\mathbf{k}(Y)$, and

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

we let W be the normalisation of Y in the relative algebraic closure L of $\mathbf{k}(Y)$ in $\mathbf{k}(Z)$, which is verifiably Galois. Then $X \times_Y W$ is the normalisation of X in $\mathbf{k}(X)L$, and it suffices to check that $X \times_Y W \to X$ is étale, which will subsequently imply that $W \to Y$ is finite étale Galois by faithfully flat descent, as required.

This is in fact a consequence of a more general principle stating that, given a tower $Z \to X' \to X$ of finite morphisms between normal connected schemes with $Z \to X$ étale and $Z \to X'$ surjective, the morphism $X' \to X$ is necessarily étale. Indeed, let us replace Z with its Galois closure over X and perform a base change of the whole situation via $Z \to X$. Exploiting the fact that $Z \times_X Z \simeq Z \times G$, and restricting attention to its components, we can reduce to the situation where $Z \to X$ is an isomorphism. It follows that $X' \to X$ is a bijective finite morphism of normal schemes and thus an isomorphism.

3.2. Definition and basic properties of direct Galois covers

Definition 3.12. An *almost direct Galois cover* is a $\mathscr{D}^{\mathrm{a}}$-morphism $p : (X, \Sigma) \to (Y, T)$ such that:

(1) X_i/Y_i is a Galois cover with group G_i, $i = 0, 1$;
(2) G_0 acts on Σ on the left so that $T \simeq G_0 \backslash \Sigma$ via ${}^{p}()$.

Remark 3.13. Using 3.8, we see that for the above data

(1) there exists a homomorphism ${}^{\pi_1}() : G_1 \to G_0$ such that, for $g_1 \in G_1$,

$$\pi_1 g_1 = {}^{\pi_1} g_1 \, \pi_1;$$

(2) for every $\sigma \in \Sigma$, there exists a homomorphism ${}^{\sigma}() : G_1 \to G_0$ such that, for $g_1 \in G_1$,

$$\sigma g_1 = {}^{\sigma} g_1 \, \sigma.$$

If $(X, \Sigma)/(Y, \sigma)$ is an almost direct Galois cover, the *almost direct Galois group* comprises the collection of data

$$(G_1, G_0, {}^{\pi_1}(), \tilde{\Sigma}),$$

where $\tilde{\Sigma} = \{{}^{\sigma}() : \sigma \in \Sigma\}$. On the other hand, the following lemma shows that it is reasonable to informally say that the almost direct Galois group is simply $(G_1, \tilde{\Sigma})$.

Lemma 3.14. *Let $p : (X, \Sigma) \to (Y, T)$ be an almost direct Galois cover. Then*

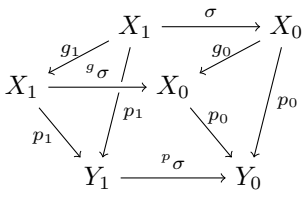
(1) $\mathrm{Aut}_{\mathscr{D}^{\mathrm{a}}}((X, \Sigma)/(Y, T)) \simeq G_1$, *and*
(2) *geometric fibres of p are G_1-orbits.*

Proof. For (1), we need to show that every $g_1 \in G_1$ induces a $\mathscr{D}^{\mathrm{a}}$-automorphism of (X, Σ). Writing $g_0 = {}^{\pi_1} g_1$, the condition $\pi_1 g_1 = g_0 \pi_1$ already gives the first half of the relevant diagram. Now, for each $\sigma \in \Sigma$ and $g = (g_0, g_1)$, we define

$${}^{g}\sigma = g_0 \sigma g_1^{-1} \overset{3.13(2)}{=} g_0 \, {}^{\sigma}(g_1^{-1}) \sigma \in \Sigma.$$

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

By the commutativity of the diagram



each ${}^g()$ defines a map $\Sigma \to \Sigma$ and for every $\sigma \in \Sigma$,

$$ {}^g\sigma\, g_1 = g_0\sigma,$$

so g_0 and g_1 give rise to an automorphism g of (X, Σ).

To show (2), let $y \in (Y, T)(F, \varphi)$ be a point with values in an algebraically closed difference field (F, φ). Writing $\pi_1 y_1 = y_0$ we have that $\tau y_1 = y_0\varphi$ for some $\tau \in T$. Since X_1/Y_1 is finite (Galois), there exists a point $x_1 \in X_1(F)$ such that $p_1(x_1) = y_1$. Let $x_0 = \pi_1(x_1)$ so that $p_0(x_0) = y_0$. Let $\sigma \in \Sigma$ be such that ${}^p\sigma = \tau$ and consider the ς-linear points σx_1 and $x_0\varphi$ of X_0. Since X_0/Y_0 is Galois, and

$$ p_0\sigma x_1 = \tau p_1 x_1 = \tau y_1 = y_0\varphi = p_0 x_0\varphi,$$

there exists a $g_0 \in G_0$ with $g_0\sigma x_1 = x_0\varphi$ and we conclude that $x \in X(F, \varphi)$.

Clearly for every $g \in G$, gx also maps to y, so by part (1) we conclude that fibres of $X(F, \varphi) \to Y(F, \varphi)$ are G_1-orbits. Moreover, the fibres of $X^\sharp(F, \varphi) \to Y^\sharp(F, \varphi)$ are ${}^{\pi_1}(G_1)$-orbits.

We refer the reader interested in the comparison of direct Galois covers with Galois covers of difference schemes defined in [16] to Remark A.9.

Remark 3.15. Suppose we have a $\mathscr{D}^{\mathrm{a}}$-morphism $(X, \tilde{\sigma}) \to (Y, \sigma)$ such that X_i/Y_i is a Galois cover with group G_i, $i = 0, 1$. Let $\Sigma = G_0\tilde{\sigma}$. Then $(X, \Sigma) \to (Y, \sigma)$ is an almost direct Galois cover.

3.3. Local substitutions

Definition 3.16. An object (X, Σ) of $\mathscr{D}^{\mathrm{a}}$ is *faithful* if Σ acts faithfully on geometric points of X in the sense that, for every algebraically closed difference field (F, φ), $\bar{x} \in X(F, \varphi)$, $\sigma, \sigma' \in \Sigma$, $\sigma\bar{x}_1 = \sigma'\bar{x}_1$ implies $\sigma = \sigma'$.

Lemma 3.17. *Suppose (Y, T) is faithful, and that $p : (X, \Sigma) \to (Y, T)$ is a directly étale almost direct Galois cover. Then (X, Σ) is also faithful.*

Proof. Let $\bar{x}$ be a geometric point on X with $p(\bar{x}) = \bar{y}$ and suppose $\sigma\bar{x}_1 = \sigma'\bar{x}_1$. Then ${}^p\sigma\bar{y}_1 = {}^p\sigma'\bar{y}_1$, so the faithfulness of Y implies that ${}^p\sigma = {}^p\sigma'$ and there is a $g_0 \in G_0$ such that $\sigma' = g_0\sigma$, so the original relation can be rewritten as $g_0\sigma\bar{x}_1 = \sigma\bar{x}_1$. Since X_0/Y_0 is étale, it follows that $g_0 = 1$.

Remark 3.18. Using the previous lemma, if $(X, \Sigma) \to (Y, \sigma)$ is a directly étale Galois cover, then (X, Σ) is automatically faithful.

Definition 3.19. Let $(X, \Sigma)/(Y, T)$ be a directly étale Galois cover with group $(G, \tilde{\Sigma})$ and (Y, T) faithful. Let (F, φ) be an algebraically closed difference field and let $x, x' \in X(F, \varphi)$, $y \in Y(F, \varphi)$ with $x, x' \mapsto y$. The *local φ-substitution at x* is the unique (by 3.17) $\varphi_x \in \Sigma$ such that $\varphi_x x_1 = x_0\varphi$ (i.e., $\varphi_x = \varphi^x$). Since X_1/Y_1 is Galois, there exists a $g \in G$ such that $x' = gx$ and

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

$$ {}^{g}\varphi_x\, x_1' = {}^{g}\varphi_x\, g_1 x_1 = g_0 \varphi_x x_1 = g_0 x_0 \varphi = x_0' \varphi, $$

so we conclude that $\varphi_{x'} = {}^{g}\varphi_x$ and we can define the *local φ-substitution at y* as the G-conjugacy class φ_y of any φ_x in Σ with $x \mapsto y$.

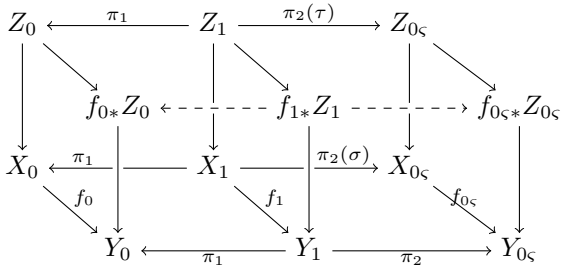
Remark 3.20. Suppose $(X, \Sigma) \to (Y, \sigma)$ is a directly étale almost direct Galois cover and let us fix a $\tilde{\sigma} \in \Sigma$ so that $\Sigma = G_0 \tilde{\sigma}$. Given $x \in X(F, \varphi)$, we can consider the unique $\dot{\varphi}_x \in G_0$ such that $\varphi_x = \dot{\varphi}_x \tilde{\sigma}$, i.e., $\dot{\varphi}_x \tilde{\sigma} x_1 = x_0 \varphi$. If $x, x' \mapsto y$, there is a $g \in G$ such that $x' = gx$ and

$$ \varphi_{x'} = {}^{g}\varphi_x = {}^{g}(\dot{\varphi}_x \tilde{\sigma}) = g_0 \dot{\varphi}_x \tilde{\sigma} g_1^{-1} = g_0 \dot{\varphi}_x {}^{\tilde{\sigma}}(g_1^{-1}) \tilde{\sigma}, $$

so we conclude that $\dot{\varphi}_{x'} = {}^{\pi_1 g_1 \dot{\varphi}_x \tilde{\sigma}}(g_1^{-1})$, a ${}^{\tilde{\sigma}}()$-conjugate of $\dot{\varphi}_x$. It is therefore meaningful to define $\dot{\varphi}_y$ as the $(G, {}^{\tilde{\sigma}}())$-conjugacy class in G_0 of any $\dot{\varphi}_x$ with $x \mapsto y$.

3.4. Constructions of direct Galois covers

Proposition 3.21 *(Pushforward of a direct Galois cover). Let $f : (X, \sigma) \to (Y, \sigma)$ be a morphism of directly integral almost direct presentations which is directly universally submersive with geometrically connected fibres, and let $(Z, \Sigma) \to (X, \sigma)$ be an almost direct Galois cover. For every $\tau \in \Sigma$, there is a diagram*



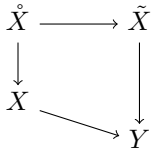
which makes $f_* Z = (f_{0*} Z_0, f_{1*} Z_1, f_{0\varsigma *} Z_{0\varsigma})$ into an almost direct Galois cover of Y.

Proof. While the solid arrows in the diagram come out directly from the assumptions, the dashed arrows are constructed using the universal property of direct images of Galois covers from 3.11.

Indeed, let V_1 be (a component of) $f_{0*} Z_0 \times_{Y_0} Y_1$, so that there is a morphism $Z_1 \to V_1$. Since V_1 is an étale cover of Y_1, by maximality of $f_{1*} Z_1$, there is a morphism $f_{1*} Z_1 \to V_1$, and we take the composite with the natural morphism $V_1 \to f_{0*} Z_0$.

Similarly, for each $\tau \in \Sigma$ we obtain a morphism $f_{1*} Z_1 \to f_{0\varsigma *} Z_{0\varsigma}$, as required.

Proposition 3.22 *(Direct Galois closure). Let $(X, \sigma) \to (Y, \sigma)$ be a directly finite étale morphism in $\mathscr{D}^{\mathrm{a}}$ between directly integral objects. There exists an object $(\tilde{X}, \tilde{\Sigma})$ in $\mathscr{D}^{\mathrm{a}}$, an inclusion $\iota : \mathring{\Sigma} \hookrightarrow \tilde{\Sigma}$ inducing a morphism $\mathring{X} = (\tilde{X}, \mathring{\Sigma}) \to (\tilde{X}, \tilde{\Sigma})$ as in the diagram*



where the vertical arrows are almost direct Galois covers, which is minimal in the sense that any other almost direct Galois cover that fits into an analogous diagram directly dominates $\tilde{X}$.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

The above diagram is called the *almost direct Galois closure* of $(X,\sigma) \to (Y,\sigma)$. Note that this is consistent with the notion of Galois closure in difference algebraic geometry [18].

Proof. Let $\tilde{X}_0$ be the Galois closure of X_0 over Y_0. The fibre product

$$\bar{X}_1 = X_1 \times_{Y_0 \times Y_0} \tilde{X}_0 \times \tilde{X}_0$$

is an étale cover of Y_1 with a transitive action of $\mathrm{Gal}(\tilde{X}_0/Y_0) \times \mathrm{Gal}(\tilde{X}_0/Y_0)$ on its connected components $C_1, \dots, C_r$.

We let $\tilde{X}_1$ be the Galois closure of C_1 over Y_1, so we obtain a correspondence $\tilde{X}_0 \overset{\pi_1}{\leftarrow} \tilde{X}_1 \overset{\tilde{\sigma}}{\to} \tilde{X}_0$ and a $\mathscr{D}^{\mathrm{a}}$-morphism $(\tilde{X},\tilde{\sigma}) \to (X,\sigma)$.

Writing $\mathring{\Sigma} = \mathrm{Gal}(\tilde{X}_0/X_0)\tilde{\sigma}$ and $\tilde{\Sigma} = \mathrm{Gal}(\tilde{X}_0/Y_0)\tilde{\sigma}$, Remark 3.15 shows that $(\tilde{X},\mathring{\Sigma}) \to (X,\sigma)$ and $(\tilde{X},\tilde{\Sigma}) \to (Y,\sigma)$ are almost direct Galois covers.

Suppose (Z,Σ_Z) is an almost direct Galois cover of (Y,σ) such that for some $\tilde{\sigma} \in \Sigma_Z$, we have a morphism $(Z,\tilde{\sigma}) \to (X,\sigma)$. Since $\tilde{X}_0$ is a Galois closure of X_0 over Y_0, we have a morphism $Z_0 \to \tilde{X}_0$ and, by the universal property of fibre products, we get a morphism $Z_1 \to \bar{X}_1$, where Z_1 actually lands onto a component C_j of $\bar{X}_1$. By transitivity of the Galois action on the components, there is a morphism $g_j : C_j \to C_1$, so we get a composite étale cover $Z_1 \to C_j \to C_1$, whence a morphism $Z_1 \to \tilde{X}_1$. We leave the verification that everything commutes to the reader.

4. Galois formulae and first-order formulae

4.1. Direct Galois stratifications and direct Galois formulae

Definition 4.1. Let (R,ς) be a difference domain, and let (X,σ) be a direct variety in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$. A *normal almost direct Galois stratification*

$$\mathcal{A} = \langle X, Z_i/X_i, C_i \,|\, i \in I \rangle$$

of (X,σ) over (R,ς) is a partition of (X,σ) into a finite set of directly integral normal locally closed subvarieties (X_i,σ) of (X,σ), each equipped with a directly connected almost direct Galois covering $(Z_i,\Sigma_i)/(X_i,\sigma)$ with group $(G_i,\tilde{\Sigma}_i)$, and C_i is a G_i-conjugacy domain in Σ_i.

Definition 4.2. Let $\mathcal{A}$ be an almost direct Galois stratification on (X,σ) over (R,ς). Then $\mathcal{A}$ defines a 'point set' subassignment $\mathcal{A}^\flat$ of $X^\flat$ as follows. For a point $s \in \mathrm{Spec}^{\varsigma}(R)$ and an algebraically closed difference field (F,φ) extending $(\mathbf{k}(s),\sigma^s)$,

$$\mathcal{A}^\flat(s,(F,\varphi)) = \mathcal{A}_s(F,\varphi) = \bigcup_i \{x \in X_{i,s}(F,\varphi) \mid \varphi_x^{Z_i/X_i} \subseteq C_i\},$$

where $\varphi_x^{Z_i/X_i}$ denotes the local φ-substitution at x, as defined in 3.19.

The *almost direct Galois formula* over (R,ς) associated with $\mathcal{A}$ is defined as the 'realisation' subassignment $\mathcal{A}^\sharp$ of $X^\sharp$ by the rule

$$\mathcal{A}^\sharp(s,(F,\varphi)) = \mathcal{A}^\sharp_s(F,\varphi) = \{x_0 \in X^\sharp(F,\varphi) : x \in \mathcal{A}_s(F,\varphi)\},$$

so that we can think of $\mathcal{A}^\sharp_s(F,\varphi)$ as the projection along π_1 of $\mathcal{A}_s(F,\varphi)$.

Notation 4.3. In informal discussion we may omit the word 'almost' from the above terms and refer simply to *direct Galois stratifications* and *direct Galois formulae*.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Remark 4.4. If we fix a lift $\sigma_i \in \Sigma_i$ of σ for each i, the above data is equivalent to fixing for each i a ${}^{\sigma_i}()$-conjugacy domain $\dot{C}_i$ in G_i, i.e., a union of ${}^{\sigma_i}()$-conjugacy classes in G_i. Clearly,

$$\mathcal{A}^\sharp_s(F,\varphi) = \bigcup_i \{x_0 \in X^\sharp_{i,s}(F,\varphi) \mid \dot{\varphi}_x^{Z_i/X_i} \subseteq \dot{C}_i\}.$$

Definition 4.5. Let (X,σ) be a direct variety in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ and let $\mathcal{A} = \langle X, Z_i/X_i, C_i\rangle$ be an almost direct Galois stratification on X.

(1) Suppose that for each i we have an almost direct covering $(Z_i',\Sigma_i')/(X_i,\sigma)$ which dominates $(Z_i,\Sigma_i)/(X_i,\sigma)$. Let $\pi_i : \Sigma_i' \to \Sigma_i$ denote the associated surjective map. The *inflation* of $\mathcal{A}$ is defined as

$$\mathcal{A}' = \langle X, Z_i'/X_i, \pi_i^{-1}(C_i)\rangle.$$

It has the property that for every $s \in S$, and every algebraically closed (F,φ) extending $(\mathbf{k}(s),\sigma^s)$,

$$\mathcal{A}'_s(F,\varphi) = \mathcal{A}_s(F,\varphi).$$

(2) Suppose that we have a further stratification of X_i into finitely many directly integral normal locally closed subschemes X_{ij}. For each i, j, let Z_{ij} be a direct component of $Z_i \times_{X_i} X_{ij}$, and let

$$D(Z_{ij,1}) = \{g \in \mathrm{Aut}(X_{ij,1} \times_{X_{i,1}} Z_{i,1}/X_{ij,1}) \simeq \mathrm{Gal}(Z_{i,1}/X_{i,1}) : g(Z_{ij,1}) = g(Z_{ij,1})\}$$

be the decomposition group of $Z_{ij,1}$. Since $\pi_1(Z_{ij,1}) \subseteq Z_{ij,0}$, it follows that ${}^{\pi_1}()$ takes $D(Z_{ij,1})$ into $D(Z_{ij,0})$. Consider $\Sigma_{ij} = \{\tau \in \Sigma_i : \tau(Z_{ij,1}) \subseteq Z_{ij,0}\}$ (which is non-empty since Z_i/X_i is Galois) and the inclusion $\iota_{ij} : \Sigma_{ij} \hookrightarrow \Sigma_i$. It can be verified, by 3.15 for example, that each $(Z_{ij},\Sigma_{ij})/(X_{ij},\sigma)$ is a Galois cover with group $D(Z_{ij,1})$.
The *refinement* of $\mathcal{A}$ associated to the above data is defined as

$$\mathcal{A}' = \langle X, Z_{ij}/X_{ij}, \iota_{ij}^{-1}(C_i)\rangle.$$

It has the property that for every $s \in S$, and every algebraically closed (F,φ) extending $(\mathbf{k}(s),\sigma^s)$,

$$\mathcal{A}'_s(F,\varphi) = \mathcal{A}_s(F,\varphi).$$

Definition 4.6. Let (X,σ) be a direct variety in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$. The class of (R,ς)-Galois formulae on X has a *Boolean algebra* structure as follows.

(1) $\bot_X = \langle X, X/X, \emptyset\rangle$, $\top_X = \langle X, X/X, \{\sigma\}\rangle$.

For Galois formulae on X given by $\mathcal{A}$ and $\mathcal{B}$, upon a refinement and an inflation we may assume that $\mathcal{A} = \langle X, Z_i/X_i, C_i\rangle$ and $\mathcal{B} = \langle X, Z_i/X_i, D_i\rangle$, with $C_i, D_i \subseteq \Sigma_i$.

(2) $\mathcal{A} \wedge \mathcal{B} = \langle X, Z_i/X_i, C_i \cap D_i\rangle$.
(3) $\mathcal{A} \vee \mathcal{B} = \langle X, Z_i/X_i, C_i \cup D_i\rangle$.
(4) $\neg\mathcal{A} = \langle X, Z_i/X_i, \Sigma_i \setminus C_i\rangle$.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

4.2. First-order formulae

Definition 4.7. Let (R, ς) be a transformal domain.

(1) A *first-order formula over* (R, ς) is a first-order formula $\theta(x_1, \ldots, x_n; a_1, \ldots, a_m)$ in the language of difference rings with free variables $x_1, \ldots, x_n$ and parameters $a_1, \ldots, a_m$ from R.
(2) An (R, ς)-formula $\theta(x_1, \ldots, x_n; a_1, \ldots, a_m)$ gives rise to a subassignment $\theta^\sharp$ of $\mathbb{A}^{n\sharp}_{(R,\varsigma)}$ by the following procedure. For any $s \in \mathrm{Spec}^\varsigma(R)$ and any difference field (F, φ) extending $(\mathbf{k}(s), \varsigma^s)$, writing $\bar{s}$ for the composite $(R, \varsigma) \to (\mathbf{k}(s), \varsigma^s) \to (F, \varphi)$, the value of

$$\theta^\sharp(s, (F, \varphi)) = \theta_s(F, \varphi)$$

is the set of realisations of the formula $\theta(x_1, \ldots, x_n, \bar{s}(a_1), \ldots, \bar{s}(a_m))$ in (F, φ).
(3) An (R, ς)-subassignment $\mathcal{F}$ of $\mathbb{A}^n_R$ is called *definable* if there is a first-order formula $\theta(x_1, \ldots, x_n)$ over (R, σ) such that $\mathcal{F} = \theta^\sharp$.

4.3. Existentially closed difference fields

It is known ([12,3]) that the first-order theory of difference fields has a model-companion called ACFA, which axiomatises existentially closed difference fields.

An axiom scheme for ACFA is obtained by a first-order transliteration of the following statement (the crucial statement is known as 'axiom H').

Fact 4.8. *An algebraically closed inversive difference field (F, φ) is existentially closed if and only if every H-direct (X, σ) in $\mathscr{D}_{(F,\varphi)}$ satisfies $X^\sharp(F, \varphi) \neq \emptyset$.*

The following is a uniform variant, obtained by using 2.23 to make all fibres geometrically H-direct, and subsequently applying axiom H.

Corollary 4.9. *Let (R, ς) be a transformal domain, and let (X, σ) be a direct variety in $\mathscr{D}_{(R,\varsigma)}$ whose generic fibre over R is geometrically H-direct. Then there exists a ς-localisation R' of R such that, for every $s \in \mathrm{Spec}^\varsigma(R')$ and every existentially closed (F, φ) extending $(\mathbf{k}(s), \varphi^s)$,*

$$X^\sharp_s(F, \varphi) \neq \emptyset.$$

4.4. Fields with powers of Frobenius

Notation 4.10. In the sequel, p denotes a rational prime, and q is a power of p.

If $q = p^n$, the map

$$\varphi_q : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p, \quad \varphi_q(\alpha) = \alpha^q$$

is the n-th power of the Frobenius automorphism on the algebraic closure of $\mathbb{F}_p$.

If k is a finite field, we may also write

$$\varphi_k = \varphi_{|k|} : \bar{k} \to \bar{k}.$$

In [10], Hrushovski proves that ACFA is in fact the elementary theory of difference fields $(\bar{\mathbb{F}}_p, \varphi_q)$. The crucial ingredient is the following consequence of his twisted Lang–Weil estimate.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Fact 4.11 *([10]). Let (R,ς) be a transformal domain of finite ς-type over $\mathbb{Z}$, and let (X,σ) be a direct variety in $\mathscr{D}_{(R,\varsigma)}$ whose generic fibre over R is geometrically H-direct. Then there exists a ς-localisation R' of R and an integer $N>0$ such that for every $s\in \mathrm{Spec}^{\varsigma}(R')$ and every field $(\bar{\mathbb{F}}_p,\varphi_q)$ extending $(\mathbf{k}(s),\varphi^s)$ with $q\geq N$,*

$$X_s^{\sharp}(\bar{\mathbb{F}}_p,\varphi_q)\neq\emptyset.$$

4.5. Equivalent subassignments and theories

Definition 4.12. Let (R,ς) be a transformal domain and let (X,σ) be an object of $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$. Let $\mathcal{F}$ and $\mathcal{F}'$ be (R,ς)-subassignments of X or $X^{\sharp}$.

(1) We shall say that $\mathcal{F}$ and $\mathcal{F}'$ are *equivalent* over (R,ς) and write

$$\mathcal{F}\equiv_{(R,\varsigma)}\mathcal{F}',$$

if for every closed $s\in\mathrm{Spec}^{\varsigma}(R)$, every algebraically closed difference field (F,φ) extending $(\mathbf{k}(s),\sigma^s)$,

$$\mathcal{F}(s,(F,\varphi))=\mathcal{F}'(s,(F,\varphi)).$$

(2) We shall write

$$\mathcal{F}\equiv^{\mathrm{ACFA}}_{(R,\varsigma)}\mathcal{F}',$$

if the above holds when (F,φ) ranges over suitable existentially closed difference fields. Additionally, we write

$$\mathcal{F}\equiv^{\mathrm{ACFA}}_{(R,\varsigma),\mathrm{gen}}\mathcal{F}',$$

if $\mathcal{F}\equiv^{\mathrm{ACFA}}_{(R',\varsigma)}\mathcal{F}'$ for some finite ς-localisation R' of R.

(3) When (R,ς) is of finite ς-type over $\mathbb{Z}$, and N a positive integer, we shall write

$$\mathcal{F}\equiv^{\textsc{Frob},N}_{(R,\varsigma)}\mathcal{F}',$$

if for every closed $s\in\mathrm{Spec}^{\varsigma}(R)$, every finite field k with $(\bar{k},\varphi_k)$ extending $(\mathbf{k}(s),\sigma^s)$ and $|k|>N$,

$$\mathcal{F}(s,(\bar{k},\varphi_k))=\mathcal{F}'(s,(\bar{k},\varphi_k)).$$

(4) If (R,ς) is of finite ς-type over $\mathbb{Z}$, we write

$$\mathcal{F}\equiv^{\textsc{Frob},\infty}_{(R,\varsigma)}\mathcal{F}',$$

if there is an $N>0$ such that $\mathcal{F}\equiv^{\textsc{Frob},N}_{(R,\varsigma)}\mathcal{F}'$. We write

$$\mathcal{F}\equiv^{\textsc{Frob},\infty}_{(R,\varsigma),\mathrm{gen}}\mathcal{F}',$$

if $\mathcal{F}\equiv^{\textsc{Frob},\infty}_{(R',\varsigma)}\mathcal{F}'$, for some finite ς-localisation R' of R.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Definition 4.13. Let (R, ς) be a transformal domain.

(1) The theory

$$\mathrm{ACFA}_{(R,\varsigma)}$$

is the set of first-order sentences θ over (R, ς) such that for any $s \in \mathrm{Spec}^{\varsigma}(R)$ and any existentially closed difference field (F, φ) extending $(\mathbf{k}(s), \varsigma^s)$, we have $(F, \varphi) \models \theta_s$. We write

$$\mathrm{ACFA}_{(R,\varsigma),\mathrm{gen}}$$

for the union of theories $\mathrm{ACFA}_{(R',\varsigma)}$, where (R', ς) ranges over all finite ς-localisations of R.

(2) If (R, ς) is of finite ς-type over $\mathbb{Z}$, the theory

$$T^{\infty}_{(R,\varsigma)} = T^{\mathrm{Frob},\infty}_{(R,\varsigma)}$$

is the set of first-order sentences θ over (R, ς) such that there exists a positive integer N such that for every closed $s \in \mathrm{Spec}^{\varsigma}(R)$, every finite field k with $(\bar{k}, \varphi_k)$ extending $(\mathbf{k}(s), \varsigma^s)$ and $|k| > N$, we have $(\bar{k}, \varphi_k) \models \theta_s$. We write

$$T^{\infty}_{(R,\varsigma),\mathrm{gen}}$$

for the union of theories $T^{\infty}_{(R',\varsigma)}$, where R' ranges over all finite ς-localisations of R.

Notation 4.14. We write

(1) $\mathrm{ACFA}_0 = \mathrm{ACFA}_{(\mathbb{Q},\mathrm{id})}$ for the theory of existentially closed fields of characteristic zero;
(2) $\mathrm{ACFA}_p = \mathrm{ACFA}_{(\mathbb{F}_p,\mathrm{id})}$ for the theory of existentially closed fields of positive characteristic p;
(3) $T^{\infty}_0 = T^{\infty}_{(\mathbb{Z},\mathrm{id}),\mathrm{gen}}$ for the set of sentences true in fields $(\bar{\mathbb{F}}_p, \varphi_q)$ for all but finitely many p and all sufficiently large q;
(4) $T^{\infty}_p = T^{\infty}_{(\mathbb{F}_p,\mathrm{id})}$ for the set of sentences true in $(\bar{F}_p, \varphi_q)$ for all large enough q.

4.6. Logic quantifier elimination

Fact 4.15 *([3, 1.6]). Every formula $\psi(x)$ in the variables $x = (x_1, \ldots, x_n)$ is equivalent modulo ACFA to a disjunction of formulae of the form $\exists y \theta(x, y)$ where y is a single variable, θ is quantifier-free, and in every model (F, φ), for every $a \in F$, $\theta(a, b)$ implies that b is algebraic over the subfield generated by $a, \varphi(a), \ldots, \varphi^m(a)$ for some m.*

In the above terminology, let (k, ς) be a prime field (either $(\mathbb{Q}, id)$ or $(\mathbb{F}_p, id)$). Then

$$\psi(x)^{\sharp} \equiv^{\mathrm{ACFA}}_{(k,\varsigma)} (\bigvee_i \exists y \theta_i(x, y))^{\sharp}$$

for θ_i as above.

4.7. First-order formulae associated with Galois formulae

Remark 4.16. Let (X, σ) be an almost direct presentation. The previously studied subassignments of X and $X^{\sharp}$ fit in the hierarchy of definable subassignments as follows.

(1) The subassignment X itself corresponds to a (positive) difference quantifier-free definable subset of the algebraic variety X_1.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

(2) The subassignment $X^\sharp$ itself corresponds to an existentially definable subset of the algebraic variety X_0, since it is a projection of X via π_1, see 2.12.
(3) An almost direct Galois formula on X is $\equiv$-equivalent to a definable set of the form that appears upon the logic quantifier elimination 4.15 down to $\exists_1$-formulae.
Indeed, suppose $(Z,\Sigma)/(X,\sigma)$ is an almost direct Galois cover with group $(G,\tilde{\Sigma})$, fix a $\tilde{\sigma}\in\Sigma$ and a $(G,{}^{\tilde{\sigma}}())$-conjugacy domain $\dot{C}$. Then

$$\langle (Z,\Sigma)/(X,\sigma),\dot{C}\rangle^\sharp(F,\varphi)=\{x_0\in X_0(F)\mid \exists z\in Z_1(F)\ \ \pi_1(z)\mapsto x_0\ \wedge \bigvee_{g_0\in\dot{C}} z\in (Z,g_0\tilde{\sigma})(F,\varphi)\},$$

so, in view of the fact that the conditions in the above disjunction are quantifier-free, it is clear that a basic direct Galois formula is equivalent to an existential first-order formula of a particular shape.
On the other hand, a general direct Galois formula is just a positive Boolean combination of basic ones so the result follows.
In case Z and X are direct, the associated first-order formula can be made even more explicit. The data yields a closed immersion

$$\begin{array}{ccccc} & & Z_1 & & \\ & \overset{\pi_1}{\swarrow} & \downarrow & \overset{\tilde{\sigma}}{\searrow} & \\ Z_0 & \longleftarrow & Z_0\times Z_0 & \longrightarrow & Z_0 \end{array}$$

whence

$$\langle (Z,\Sigma)/(X,\sigma),\dot{C}\rangle^\sharp(F,\varphi)=\{x_0\in X_0(F)\mid \exists z_0\in Z_0(F),\quad z_0\mapsto x_0\ \wedge \bigvee_{g_0\in\dot{C}} (z_0,g_0^{-1}z_0\varphi)\in Z_1\}.$$

The goal of subsequent sections is to show that existentially closed difference fields (and, asymptotically, fields with powers of Frobenius) allow quantifier elimination for Galois formulae and every first order formula is equivalent to a Galois formula over such fields.

5. Direct image theorems

5.1. Direct images of Galois formulae

Definition 5.1. Let $f:(X,\sigma)\to(Y,\sigma)$ be a morphism in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ and let $\mathcal{A}$ be an almost direct Galois stratification on X. We define a subassignment $f_\exists\mathcal{A}$ of Y and a subassignment $f^\sharp_\exists\mathcal{A}$ of $Y^\sharp$ by the following rule. For $s\in S$ and (F,φ) an algebraically closed difference field extending $(\mathbf{k}(s),\sigma^s)$,

(1) $f_\exists\mathcal{A}(s,(F,\varphi))=(f_\exists\mathcal{A})_s(F,\varphi)=f_s(\mathcal{A}_s(F,\varphi))\subseteq Y_s(F,\varphi)$;
(2) $f^\sharp_\exists\mathcal{A}(s,(F,\varphi))=(f^\sharp_\exists\mathcal{A})_s(F,\varphi)=f_{0,s}(\mathcal{A}^\sharp_s(F,\varphi))\subseteq Y^\sharp_s(F,\varphi)$.

Lemma 5.2. *Suppose that a diagram*

$$\begin{array}{ccc} (Z,\mathring{\Sigma}) & \longrightarrow & (Z,\Sigma) \\ \downarrow & & \\ (X,\sigma) & \overset{f}{\searrow} & \downarrow \\ & & (Y,\sigma) \end{array}$$

consists of almost direct Galois covers $(Z,\mathring{\Sigma})/(X,\sigma)$ *and* $(Z,\Sigma)/(Y,\sigma)$*, where the top horizontal arrow is induced by an inclusion* $\iota:\mathring{\Sigma}\hookrightarrow\Sigma$ *and* f *is directly finite étale. Let* $C\subseteq\mathring{\Sigma}$ *be a* $\mathrm{Gal}(Z/X)$*-conjugacy domain, and let* $\iota_*C\subseteq\Sigma$ *be the* $\mathrm{Gal}(Z/Y)$*-conjugacy domain induced by* C*. Then*

$$f_\exists^\sharp\langle Z/X,C\rangle\equiv\langle Z/Y,\iota_*C\rangle^\sharp.$$

Proof. We will show more, that $f_\exists\langle Z/X,C_0\rangle=\langle Z/Y,C\rangle^\flat$. For the left-to-right inclusion, let $y\in Y(F,\varphi)$ be such that there exists an $x\in\langle Z/X,C\rangle(F,\varphi)$ with $f(x)=y$. Thus, there exists a $z\in(Z,\mathring{\Sigma})(F,\varphi)$ with $z\mapsto x$ and $\varphi_z\in C$, so that its $\mathrm{Gal}(Z/X)$-conjugacy class $\varphi_x\subseteq C$. But φ_y is the $\mathrm{Gal}(Z/Y)$-conjugacy class of φ_z so it is clearly contained in ι_*C.

For the other inclusion, suppose $y\in\langle Z/Y,C\rangle(F,\varphi)$ for an algebraically closed difference field (F,φ). There exists a $z\in(Z,\Sigma)(F,\varphi)$ such that $z\mapsto y$ and

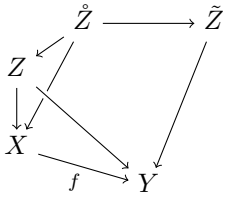
$$\varphi_z\in\iota_*C=\bigcup_{g\in\mathrm{Gal}(Z/Y)}{}^gC,$$

so let $\varphi_z\in{}^gC$ for some $g\in\mathrm{Gal}(Z/Y)$. Then $\varphi_{g^{-1}z}\in C$, so the image x of $g^{-1}z$ in X witnesses $f(x)=y$ and $x\in\langle Z/X,C\rangle(F,\varphi)$.

Proposition 5.3. *Let* $f:(X,\sigma)\to(Y,\sigma)$ *be a directly finite étale morphism in* $\mathscr{D}^{\mathrm{a}}$*, let* $(Z,\Sigma)/(X,\sigma)$ *be an almost direct Galois cover, and let* $C\subseteq\Sigma$ *be a conjugacy domain. Let* $(\tilde{Z},\tilde{\Sigma})$*,* $(\tilde{Z},\tilde{\Sigma})$*,* $\iota:\mathring{\Sigma}\hookrightarrow\tilde{\Sigma}$ *be the data associated with the direct Galois closure of* Z *over* Y*. Let* $\mathring{C}$ *be the preimage of* C *under the surjection* $\mathring{\Sigma}\to\Sigma$*, and let* $\iota_*\mathring{C}$ *be the least conjugacy domain in* $\tilde{\Sigma}$ *containing* $\iota(\mathring{C})$*. Then*

$$f_\exists^\sharp\langle Z/X,C\rangle\equiv\langle\tilde{Z}/Y,\iota_*\mathring{C}\rangle^\sharp.$$

Proof. As in the previous proof, let us show that $f_\exists\langle Z/X,C\rangle\equiv\langle\tilde{Z}/Y,\iota_*\mathring{C}\rangle^\flat$ already. The diagram



shows the situation described in the statement, where we wrote $\mathring{Z}$ for $(\tilde{Z},\mathring{\Sigma})$.

We have

$$f_\exists\langle Z/X,C\rangle\overset{\text{(inflation)}}{\equiv}f_\exists\langle\mathring{Z}/X,\mathring{C}\rangle\overset{(5.2)}{\equiv}\langle Z/Y,\iota_*\mathring{C}\rangle^\flat.$$

Proposition 5.4. *Let* $f:(X,\sigma)\to(Y,\sigma)$ *be a morphism of directly integral varieties in* $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$ *which is directly universally submersive with geometrically connected fibres, and let* $(Z,\Sigma)\to(X,\sigma)$ *be an almost direct Galois cover and let* $C\subseteq\Sigma$ *be a conjugacy domain. Let* f_*Z *be the almost direct Galois cover of* Y *obtained in 3.21. Then there is a finite* ς*-localisation* R' *of* R *such that*

$$f_\exists^\sharp\langle Z/X,C\rangle\underset{(R',\varsigma)}{=\!\!=^{\mathrm{ACFA}}}\langle f_*Z/Y,f_*C\rangle^\sharp,$$

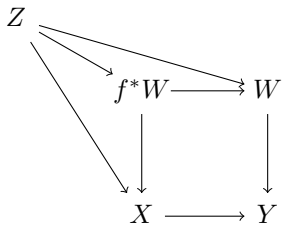
where f_*C *denotes the image of* C *under the surjective map* $\Sigma\to\Sigma_{f_*Z}$*.*

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Proposition 5.5. *When (R, ς) is of finite ς-type over $\mathbb{Z}$, there exists a positive integer N and a finite ς-localisation R' of R such that we have the analogous statement of 5.4 with*

$$f_{\exists}^{\sharp}\langle Z/X, C\rangle \equiv_{(R',\varsigma)}^{\text{Frob},N} \langle f_* Z/Y, f_* C\rangle^{\sharp}.$$

Proof of 5.4. Writing $W = f_* Z$, the diagram



resulting from 3.21 shows (by inflation, 4.5) that $\langle Z/X, f^* f_* C\rangle = \langle f^* W/X, f_* C\rangle$, and so $f_{\exists}\langle Z/X, C\rangle = f_{\exists}\langle Z/X, f^* f_* C\rangle = f_{\exists}\langle f^* W/X, f_* C\rangle$. Thus, it is sufficient to prove that, for any conjugacy domain $D \subseteq \Sigma_W$,

$$f_{\exists}\langle f^* W/X, D\rangle \equiv \langle W/Y, D\rangle.$$

Indeed, let $y \in Y(F, \varphi)$ with $\varphi_y \in D$. There exists an $y' \in W(F, \varphi)$ with $y' \mapsto y$ and $\varphi_{y'} \in D$, i.e., there exists a $\tau \in D$ such that $y' \in W^{\tau}(F, \varphi)$, $\tau y'_1 = y'_0 \varphi$. By construction, the fibre $(f^* W_{y'}, \tau)$ is directly geometrically integral, so by Axiom H (4.8), there exists an $x' \in (f^* W_{y'}, \tau)(F, \varphi)$ such that its image $x \in X(F, \varphi)$ witnesses $\varphi_x \subseteq D$, $f(x) = y$.

The proof of 5.5 is completely analogous, one simply replaces the use of Axiom H by the use of the twisted Lang–Weil estimate 4.11.

Theorem 5.6. *Let $f : (X, \sigma) \to (Y, \sigma)$ be a morphism of direct varieties in $\mathscr{D}^{\mathrm{a}}_{(R,\varsigma)}$, with (R, ς) a transformal domain. Let $\mathcal{A}$ be an almost direct Galois stratification on (X, σ). Then there exists an integer n, a localisation (R', ς) of R_{-n} and an almost direct Galois stratification $\mathcal{B}$ on (Y, σ) defined over R' such that*

$$f_{\exists}^{\sharp}\mathcal{A} \equiv_{(R',\varsigma)}^{\text{ACFA}} \mathcal{B}^{\sharp}.$$

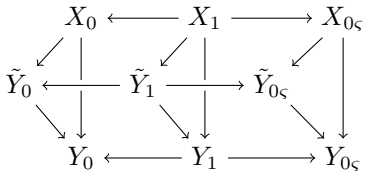
Theorem 5.7. *When (R, ς) is of finite ς-type over $\mathbb{Z}$, there exists a positive integer N such that we have the analogous statement of 5.6 with*

$$f_{\exists}^{\sharp}\mathcal{A} \equiv_{(R',\varsigma)}^{\text{Frob},N} \mathcal{B}^{\sharp}.$$

Proof of 5.6 and 5.7. Upon a direct irreducible decomposition and a localisation, we may assume that f is a morphism of H-direct normal objects, and that $\mathcal{A}$ is given as $\langle (Z, \Sigma)/(X, \sigma), C\rangle$ for an almost direct Galois cover Z/X.

We begin by performing a direct 'baby' Stein factorisation as follows. Let L_i be the relative algebraic closure of $\mathbf{k}(Y_i)$ in $\mathbf{k}(X_i)$ for $i = 0, 1$, so that $L_{0\varsigma}$ is the relative algebraic closure of $\mathbf{k}(Y_{0\varsigma})$ in $\mathbf{k}(X_{0\varsigma})$. Clearly $L_0 \hookrightarrow L_1 \hookleftarrow L_{0\varsigma}$, and let $\tilde{Y}_i$ be the normalisation of Y_i in L_i for $i = 0, 1$, so that $\tilde{Y}_{0\varsigma}$ is the normalisation of $Y_{0\varsigma}$ in $L_{0\varsigma}$. The resulting diagram

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002



gives the required factorisation of f, allowing us to reduce the consideration to the following two cases.

By localising, we may assume that the morphism $(X, \sigma) \to (\tilde{Y}, \sigma)$ is directly universally submersive with geometrically integral fibres, so we reduce to the known case 5.4. The complement is lower dimensional, so we proceed by devissage.

By localising, we may assume that the morphism $(\tilde{Y}, \sigma) \to (Y, \sigma)$ is directly finite étale, so we finish by 5.3. The complement is lower dimensional, so we proceed by devissage.

We end up with an almost direct Galois stratification on Y.

Corollary 5.8. *In addition to assumptions of 5.6, let (R, ς) be the inversive closure of a transformal domain of finite ς-type over a difference field or over $\mathbb{Z}$. Then we have the following.*

(1) *There exist a finite ς-localisation R' of R and an almost direct Galois stratification $\mathcal{B}$ on Y over R' such that*

$$f_{\exists}^{\sharp}\mathcal{A} \equiv^{\mathrm{ACFA}}_{(R',\varsigma)} \mathcal{B}^{\sharp}.$$

(2) *If (R, ς) is over $\mathbb{Z}$, there exist a finite ς-localisation R' of R, an almost direct Galois stratification $\mathcal{B}$ on Y over R' and a positive integer N such that*

$$f_{\exists}^{\sharp}\mathcal{A} \equiv^{\mathrm{Frob},N}_{(R',\varsigma)} \mathcal{B}^{\sharp}.$$

5.2. Quantifier elimination for direct Galois formulae

Theorem 5.9. *Let (R, ς) be the inversive closure of a transformal domain of finite ς-type over a difference field or $\mathbb{Z}$. Let $\theta(x) = \theta(x; a)$ be a first order formula in the language of difference rings in variables $x = x_1, \ldots, x_n$ with parameters a from (R, ς). Then we have the following.*

(1) *There exists a direct Galois stratification $\mathcal{A}$ of the difference affine n-space over a finite ς-localisation (R', ς) of R such that*

$$\theta^{\sharp} \equiv^{\mathrm{ACFA}}_{(R',\varsigma)} \mathcal{A}^{\sharp}.$$

(2) *If R is over $\mathbb{Z}$, there exists a direct Galois stratification $\mathcal{A}$ of the difference affine n-space over a finite ς-localisation R' of R and a positive integer N such that*

$$\theta^{\sharp} \equiv^{\mathrm{Frob},N}_{(R',\varsigma)} \mathcal{A}^{\sharp}.$$

Proof. The proof of the theorem is purely formal from 5.8 (where the difficult work was done) by induction on the complexity of $\theta(x)$. The crucial step is the elimination of the existential quantifier, where we apply 5.8 to a projection morphism. It is analogous to the derivation of 3.26 from 3.23 in [17] so we omit it.

Remark 5.10. The following is a logician's way of interpreting the statements of 5.9.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

(1) The class of definable (R,ς)-subassignments is $\equiv^{\mathrm{ACFA}}_{(R,\sigma),\mathrm{gen}}$-equivalent to the class of direct Galois formulae over (R,ς).
(2) The class of definable (R,ς)-subassignments is $\equiv^{\mathrm{Frob},\infty}_{(R,\sigma),\mathrm{gen}}$-equivalent to the class of direct Galois formulae over (R,ς).

Remark 5.11. It is possible to stratify $\mathrm{Spec}^{\varsigma}(R)$ into locally closed pieces so that the conclusions of 5.8 and 5.9 hold over each piece. In other words, a Galois-type formula can match a first-order formula over *every* point of $\mathrm{Spec}^{\varsigma}(R)$.

Indeed, the assumptions on (R,ς) ensure that it is Ritt, i.e., that $\mathrm{Spec}^{\varsigma}(R)$ is a noetherian topological space with Zariski topology induced from $\mathrm{Spec}(R)$. Theorems 5.6 and 5.7 ensure that a suitable $\mathcal{B}$ can be found on an open dense subset of $\mathrm{Spec}^{\varsigma}(R)$, so we can proceed by noetherian induction on the closed complement.

5.3. Sentences

Remark 5.12. Let θ be a first-order sentence over an inversive difference field (k,ς). Let S denote the (trivial) direct presentation associated with $\mathrm{Spec}(k,\varsigma)$. By 5.9, there exists a direct Galois stratification $\mathcal{A}$ on S so that θ is equivalent to the Galois formula $\mathcal{A}^{\sharp}$. Since $\mathrm{Spec}(k)$ is a point, $\mathcal{A}$ consists of a single direct Galois cover,

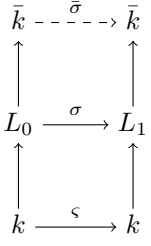
$$\mathcal{A} = \langle S, (Z,\Sigma)/(S,\varsigma), C\rangle.$$

(1) If $C \neq \emptyset$, there exists an existentially closed difference field (F,φ) extending (k,φ) with $(F,\varphi) \models \theta$, or, equivalently,

$$\mathcal{A}^{\sharp}(F,\varphi) \neq \emptyset.$$

(2) The sentence θ belongs to the theory $\mathrm{ACFA}_{(k,\varsigma)}$ if and only if $C = \Sigma$.

Proof. Note that $Z = (Z_0, Z_1) = (\mathrm{Spec}(L_0), \mathrm{Spec}(L_1))$, where L_0 and L_1 are finite Galois extensions of k with $L_0 \to L_1$. If $\sigma \in \Sigma$, the solid arrows in the diagram



show the given data upon fixing embeddings $L_0 \subseteq L_1 \subseteq \bar{k}$ into the algebraic closure of k. Using the classical extension theorem [11, Theorem V.2.8], we can lift σ to a dashed arrow $\bar{\sigma}$ on $\bar{k}$, and then we can embed $(\bar{k},\bar{\sigma})$ into an existentially closed difference field (F,φ). Thus, if $\sigma \in C$, $\mathcal{A}^{\sharp}(F,\varphi) \neq \emptyset$, as claimed in (1).

For (2), if $C \neq \Sigma$, then (1) gives an existentially closed difference field (F,φ) extending (k,ς) such that $(F,\varphi) \models \neg\theta \equiv \langle Z/S, \Sigma \setminus C\rangle^{\sharp}$.

Remark 5.13. Let (R,ς) be either $(\mathbb{Z}[1/n], \mathrm{id})$ for some non-zero integer n, or $(\mathbb{F}_q, \varphi_r)$ for some powers q and r of a prime p. Let θ be a first-order sentence over (R,ς).

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

By 5.9, there is a finite localisation R' of R, an integer $N > 0$ and a basic Galois stratification on $S' = \mathrm{Spec}(R', \varsigma)$ as an object in $\mathscr{D}^{\mathrm{a}}$

$$\mathcal{A} = \langle S', (Z, \Sigma)/(S', \varsigma), C \rangle,$$

such that

$$\theta^\sharp \equiv^{\mathrm{Frob},N}_{(R',\varsigma)} \mathcal{A}^\sharp.$$

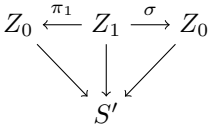
(1) If $C \neq \emptyset$ then for every ς-localisation R'' of R' there exists a closed point $s \in \mathrm{Spec}^\sigma(R'')$ such that for infinitely many finite fields k with $(\bar{k}, \varphi_k)$ extending $(\mathbf{k}(s), \varsigma^s)$ and $|k| > N$, we have

$$(\bar{k}, \varphi_k) \models \theta_s.$$

(2) The sentence θ belongs to the theory $T^\infty_{(R,\varsigma),\mathrm{gen}}$ if and only if $C = \Sigma$.

Proof. When $(R, \varsigma) = (\mathbb{F}_q, \varphi_r)$, then $R' = R$ and we argue as in 5.12 for $(k, \varsigma) = (\mathbb{F}_q, \varphi_r)$. Since L_0 and L_1 are finite, it follows that σ is a power of Frobenius on L_0, and the relevant diagram in 5.12 can be completed by the infinitely many powers of Frobenius $\bar{\sigma}$ which restrict to σ on L_0.

In the case $(R, \varsigma) = (\mathbb{Z}[1/n], \mathrm{id})$, it follows that $R' = \mathbb{Z}[1/n']$ where n divides n'. Given that the difference operator on S' is the identity, the Galois cover $(Z, \Sigma)/(S', \mathrm{id})$ is associated with particularly simple diagrams indexed by $\sigma \in \Sigma$



where Z_0/S and Z_1/S are Galois covers with groups G_0 and G_1. Since Z_1 dominates Z_0, the map ${}^{\pi_1}() : G_1 \to G_0$ is surjective. For each $\sigma \in \Sigma$, 3.7 gives that $\sigma = g_0\pi_1$ for some $g_0 \in G_0$.

Hence, if $\sigma \in C$, we conclude that $C = C_0\pi_1$ with C_0 a conjugacy domain in G_0 containing g_0. Moreover, finding a point $z \in (Z, \Sigma)(F, \varphi)$ with $\varphi_z = \sigma$ reduces to finding a point $s \in S'$ with local Frobenius substitution with respect to the cover Z_0/S' contained in C_0. The classical Chebotarev density theorem gives a non-zero density of primes s with that property, which proves (1).

For (2), if $C \neq \Sigma$, then (1) applied to $\neg\theta \equiv \langle Z/S, \Sigma \setminus C \rangle$ shows that $\theta \notin T^\infty_{(R,\varsigma),\mathrm{gen}}$.

Corollary 5.14. *With notation of 4.14, we have*

$$\mathrm{ACFA}_0 = T_0^\infty \quad \text{and} \quad \mathrm{ACFA}_p = T_p^\infty.$$

Proof. A sentence θ over $\mathbb{Q}$ makes sense over some $\mathbb{Z}[1/n]$. Galois stratification for fields with Frobenius will produce a Galois formula $\mathcal{A}$ over some $\mathbb{Z}[1/n']$ with $n|n'$ which is equivalent to θ over fields with high enough power of Frobenius. On the other hand, the stratification procedure for existentially closed difference fields yields the same Galois formula $\mathcal{A}$. The criteria for a Galois sentence belonging to ACFA_0 and T_0^∞ are exactly the same, so we conclude that $\theta \in \mathrm{ACFA}_0$ if and only if $\theta \in T_0^\infty$. We argue similarly in characteristic p.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

6. Effective quantifier elimination

6.1. Effective (direct difference) algebraic geometry

Definition 6.1.

(1) A ring R is *primitive recursive*, if (modulo some Gödel numbering), R is a primitive recursive set and the operations of addition, multiplication, multiplicative inverse are primitive recursive functions.
(2) A primitive recursive field k has a *splitting algorithm* if there is a primitive recursive algorithm for factoring elements of $k[T]$ into irreducible factors.
(3) A primitive recursive field k has *elimination theory* if every finitely generated (explicitly presented) extension of k has a splitting algorithm.
(4) A field k is called *effective*, if it is primitive recursive and k is perfect with a splitting algorithm.
(5) A domain R is *effective*, if its fraction field K is effective, R is primitive recursive, and R is a primitive recursive subset of K.

Definition 6.2.

(1) An inversive difference ring (R, ς) is *primitive recursive*, if R is a primitive recursive ring, and the difference operator ς and its inverse ς^{-1} are primitive recursive functions.
(2) An inversive difference field (k, ς) is called *effective*, if it is primitive recursive and k is effective.
(3) An inversive transformal domain (R, ς) is *effective*, if its fraction field (K, ς) is effective, (R, ς) is primitive recursive, and R is a primitive recursive subset of K.

Example 6.3. The transformal domains $(\mathbb{Z}, \mathrm{id})$, $(\mathbb{Q}, \mathrm{id})$, $(\mathbb{F}_q, \varphi_p)$ are effective.

Definition 6.4. Let (R, ς) be an effective transformal domain.

(1) We say that an algebraic variety V over R is *effectively presented* if V is of finite presentation over R and its presentation is explicitly given, and similarly for morphisms.
(2) An object (X, Σ) of $\mathscr{D}^{\mathrm{av}}_{(R,\varsigma)}$ is *effectively presented* if X_0, X_1, $X_{0\varsigma}$ and all the morphisms $\pi_1 : X_1 \to X_0$, $\pi_2(\sigma) : X_1 \to X_{0\varsigma}$, $\sigma \in \Sigma$, are effectively presented. We make an analogous definition for morphisms in $\mathscr{D}^{\mathrm{av}}_{(R,\varsigma)}$.
(3) A normal almost direct Galois stratification $\mathcal{A} = \langle X, Z_i/X_i, C_i \,|\, i \in I \rangle$ is *effectively presented* if the base (X, σ) is effectively presented and all the pieces Z_i, X_i are affine normal and effectively presented.

Remark 6.5. By [7, 19.2.10], an effective field k has elimination theory and it can serve as a base field for a well-behaved and well-understood *effective/constructive algebraic geometry*. Indeed, by the detailed treatments in [15,7,13], the following operations on effectively presented algebraic varieties over k are known to be primitive recursive:

(1) computing fibre products;
(2) decomposing a variety into irreducible components;
(3) computing the image of a morphism;
(4) computing the relative algebraic closure;
(5) computing the loci of flatness/smoothness/étaleness/geometrically connected fibres of a morphism;
(6) normalisation of a (normal) integral variety in an extension of its function field;
(7) computation of Galois groups, Galois closure and decomposition subgroups in a given Galois cover.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Moreover, if the input data for the above algorithms is given over an effective ring R, the algorithms can effectively compute an element $f \in R$ so that the output data is defined over the localised ring R_f.

Remark 6.6. Given an effective difference field (k, ς), the operations in $\mathscr{D}^{\mathrm{av}}_{(k,\varsigma)}$ reduce to classical operations on algebraic varieties over k, so we automatically obtain a rich framework for *effective direct difference algebraic geometry.*

6.2. Effective quantifier elimination for ACFA

Theorem 6.7. *Let $\theta(x) = \theta(x; a)$ be a first order formula in the language of difference rings in variables $x = x_1, \ldots, x_n$ with parameters a from an effective difference field (k, ς). A primitive recursive procedure can compute an effectively presented direct Galois stratification $\mathcal{A}$ of the difference affine n-space over (k, ς) such that*

$$\theta^\sharp \equiv^{\mathrm{ACFA}}_{(k,\varsigma)} \mathcal{A}^\sharp.$$

Proof. The goal is to show that the algorithm can be described without reference to indefinite loops and unbounded searches, and that various induction proofs can in fact be transformed into procedures using bounded loops.

The outer loop, following the proof of 5.9, is bounded by the complexity of $\theta(x)$, and the only nontrivial procedures it invokes are instances of 5.6, so it will suffice to show that taking direct images of an effective direct Galois stratification via 5.6 is primitive recursive.

Now, 5.6 is done by induction on dimension, so its main loop is bounded by dimensions of the varieties involved in the direct presentations (X, σ) and (Y, σ). The next possible problem is a possible jump in the number of direct components produced by the direct decomposition 2.21 on the 'bad loci' of lower dimension excised at each step, but Cohn [4, Solution to Problem I*, Chapter 8, No. 14] already argued that the procedure is primitive recursive, and Hrushovski even gives explicit bounds for the number of components in terms of degrees of the correspondences involved in [9, Proposition 2.2.1].

There are no more dangerous control loops to consider, so it suffices to verify that all the algebraic-geometric constructions used in all the constituent steps of the proof of 5.6 are primitive recursive. By inspection, all these operations reduce to the algorithms from 6.5 and we are done.

Corollary 6.8. *Let (k, ς) be an effective difference field. The theory $\mathrm{ACFA}_{(k,\varsigma)}$ of existentially closed difference fields extending (k, ς) is decidable by a primitive recursive procedure.*

Proof. We repeat the argument of 5.12 in an effective way. Let θ be a sentence with parameters in (k, ς). Using 6.7, a primitive recursive procedure can compute a direct Galois stratification $\mathcal{A}$ on $S = \mathrm{Spec}(k, \varsigma) \in \mathscr{D}^{\mathrm{a}}_{(k,\varsigma)}$ so that θ is equivalent to the Galois formula $\mathcal{A}^\sharp$. Since $\mathrm{Spec}(k)$ is a point, $\mathcal{A}$ consists of a single direct Galois cover,

$$\mathcal{A} = \langle X, (Z, \Sigma)/(X, \sigma), C \rangle.$$

The sentence θ is entailed by $\mathrm{ACFA}_{(k,\varsigma)}$ if and only if $C = \Sigma$, and this can be checked by a primitive recursive procedure.

Corollary 6.9. *The theories ACFA_0 and ACFA_p are primitive recursive decidable.*

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

6.3. Effective quantifier elimination for fields with powers of Frobenius

Theorem 6.10. *Let $\theta(x)$ be a first order formula in the language of difference rings in variables $x = x_1, \ldots, x_n$ over an effective transformal domain (R, ς) of finite ς-type over $\mathbb{Z}$. A primitive recursive procedure can compute an effectively presented direct Galois stratification $\mathcal{A}$ of the difference affine n-space over a ς-localisation (R', ς) of R and a positive integer N such that*

$$\theta^\sharp \equiv^{\text{Frob},N}_{(R',\varsigma)} \mathcal{A}^\sharp.$$

Proof. An essential ingredient of the proof is the effectivity of Hrushovski's bound needed for 4.11. It is argued in [10] that a primitive recursive procedure can compute a ς-localisation of R and an integer $N > 0$ so that 4.11 holds.

The rest of the proof is analogous to 6.7, bearing in mind the effective algebraic geometry over an effective domain in which every operation is done modulo a localisation as in 6.5.

Corollary 6.11. *Let (R, ς) be $(\mathbb{Z}[1/n], \mathrm{id})$ for a non-zero integer n or $(\mathbb{F}_q, \varphi_r)$ for some prime powers q and r. The theory $T^{\infty,gen}_{(R,\varsigma)}$ is decidable by a primitive recursive procedure. Moreover, given a $\theta \in T^{\infty,gen}_{(R,\varsigma)}$, a primitive recursive procedure can compute the (finite) list of exceptional cases consisting of*

(1) *points $s \in \mathrm{Spec}^\varsigma(R)$ for which $\theta_s \notin T^\infty_{(\mathbf{k}(s),\varsigma^s)}$;*
(2) *pairs (s, k) consisting of a point $s \in \mathrm{Spec}^\varsigma(R)$ with $\theta_s \in T^\infty_{(\mathbf{k}(s),\varsigma^s)}$ and a finite field k with $(\bar{k}, \varphi_k)$ extending $(\mathbf{k}(s), \varsigma^s)$ with $(\bar{k}, \varphi_k) \not\models \theta_s$.*

Proof. In view of 6.10, the argument of 5.13 becomes effective. Given a sentence θ over (R, ς), a primitive recursive procedure computes a ς-localisation R' of R, an integer $N > 0$ and a basic Galois stratification on $S' = \mathrm{Spec}(R', \varsigma)$

$$\mathcal{A} = \langle S', (Z, \Sigma)/(S', \varsigma), C\rangle,$$

such that

$$\theta^\sharp \equiv^{\text{Frob},N}_{(R',\varsigma)} \mathcal{A}^\sharp.$$

Then $\theta \in T^\infty_{(R,\varsigma),\text{gen}}$ if and only if $C = \Sigma$, which can be verified by a primitive recursive test.

In the case where we started with $(R, \varsigma) = (\mathbb{F}_q, \varphi_r)$, and we are given a $\theta \in T^\infty_{(\mathbb{F}_q,\varphi_r)}$, potential exceptions must be sought among those finite fields k of size at most N for which $(\bar{k}, \varphi_k)$ extends $(\mathbb{F}_q, \varphi_r)$ and we need to check whether $(\bar{k}, \varphi_k)$ satisfies θ or not.

For each of those k, substituting φ_k for the difference operator in θ yields a first-order sentence in the language of rings on an algebraically closed field $\bar{k}$, and such statements can be decided by a well-known primitive recursive procedure for algebraically closed fields.

In the case of $R = \mathbb{Z}[1/n]$, the algorithm produced an explicit n' with $n|n'$ so that $R' = \mathbb{Z}[1/n']$. In order to find the exceptional cases, it suffices to consider only the characteristics dividing n'. Thus, for each prime p dividing n', we apply the first part of the corollary to decide whether $\theta_p \in T^\infty_p$. If so, we use the above algorithm for listing the exceptional finite fields k of characteristic p for which $(\bar{k}, \varphi_k) \not\models \theta_p$.

Corollary 6.12. *The theories T^∞_0 and T^∞_p are primitive recursive decidable. Moreover, if $\theta \in T^\infty_0$, a primitive recursive procedure can compute the finite list of:*

(1) *primes p with $\theta_p \notin T^\infty_p$;*
(2) *pairs (p, q) such that $\theta_p \in T^\infty_p$ but $(\bar{\mathbb{F}}_p, \varphi_q) \not\models \theta_p$.*

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

6.4. Applications to effective difference algebra

Our results have direct consequences for effective/constructive difference algebra, allowing us to, for example, rediscover the primitive recursiveness of the *perfect ideal membership problem* (Cohn states that the problem can be solved by an 'effective procedure', see [4, Chapter 8, No. 14]). Recall, an ideal I in a difference ring is called *perfect*, if $a\sigma(a) \in I$ implies that a and $\sigma(a)$ are both in I. The *perfect closure* $\{E\}$ of a set E is the least perfect ideal containing E.

Corollary 6.13. *Let (k, ς) be an effective difference field. A primitive recursive procedure can decide, given difference polynomials $f, f_1 \dots, f_n$ over (k, ς), whether*

$$f \in \{f_1, \dots, f_n\}.$$

Proof. Following [16, 2.19], [17, 2.29], the following conditions are equivalent

(1) $f \in \{f_1, \dots, f_n\}$;
(2) $V(f_1, \dots, f_n) \subseteq V(f)$;
(3) $\mathrm{ACFA}_{(k,\varsigma)} \vdash \forall x_1 \cdots \forall x_m \bigwedge_{i \leq n} f_i(x_1, \dots, x_m) = 0 \to f(x_1, \dots, x_m) = 0$,

and the last condition is decidable by a primitive recursive procedure via 6.8.

Appendix A. Directly presented difference schemes

The goal of this Appendix is to show how our framework of direct presentations relates to the notion of *directly presented difference schemes* from [10], and assumes that the reader is familiar with basic notation and concepts of that paper.

Proposition A.1 *([10, Sect. 4.3], [18, 3.1, 3.2]). Let (R, ς) be a difference ring.*

(1) *The forgetful functor from the category of difference (R, ς)-algebras to the category of R-algebras has a left adjoint $[\varsigma]_R$, i.e., for every R-algebra A we have a homomorphism $A \to [\varsigma]_R A$ inducing the functorial isomorphism*

$$\mathrm{Hom}_{(R,\varsigma)}([\varsigma]_R A, (C, \sigma)) = \mathrm{Hom}_R(A, C),$$

for every (R, ς)-algebra (C, σ).
(2) *Let X be an (algebraic) scheme over R. The functor from the category of difference (R, ς)-schemes to the category of sets, $(Z, \sigma) \mapsto \mathrm{Hom}_R(Z, X)$ (morphisms of locally R-ringed spaces) is representable. More precisely, we have a difference scheme $[\varsigma]_R X$ associated to X, equipped with the universal morphism $[\varsigma]_R X \to X$ of locally R-ringed spaces, inducing a functorial isomorphism*

$$\mathrm{Hom}_R(Z, X) = \mathrm{Hom}_{(R,\varsigma)}((Z, \sigma), [\sigma]_R X),$$

for every (R, σ)-difference scheme (Z, σ).

Definition A.2. Let (R, ς) be a difference ring. An (R, ς)-algebra (A, σ) is *directly presented* if there exists an (R, ς)-epimorphism $(P, \sigma) \to (A, \sigma)$ from some difference polynomial ring $(P, \sigma) = [\varsigma]_R R[\bar{x}] = R[\bar{x}]_\sigma$ whose kernel I is σ-generated by $I \cap R[\bar{x}, \sigma(\bar{x})]$.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Intuitively speaking, there is a choice of a tuple of generators $a \in A$ such that A is σ-generated by a over R and the relations between the generators are all deduced from the relations between a and σa.

Definition A.3 *([10, 6.1])*. Let (R, ς) be a difference ring. Let Y be an algebraic scheme over R and let Z be a closed subscheme of $Y \times_{\mathrm{Spec}(R)} Y_\varsigma$. Let Γ_σ denote the graph of σ on $[\varsigma]_R Y \times_{\mathrm{Spec}^\varsigma(R)} [\varsigma]_R Y_\varsigma$ and we define the difference scheme

$$[\varsigma]_R(Y, Z)$$

as the projection to $[\varsigma]_R Y$ of the difference scheme $[\varsigma]_R Z \cap \Gamma_\sigma$.

Remark A.4. With the above notation, let (F, φ) be a difference field extending (R, ς). Given a point $y \in Y(F)$, clearly $y\varphi \in Y_\varsigma(F)$. We have

$$[\varsigma]_R(Y, Z)(F, \varphi) = \{y \in Y(F) : (y, y\varphi) \in Z(F)\},$$

a familiar notion of a difference scheme defined by a correspondence Z between an algebraic scheme Y and its twist Y_ς.

Lemma A.5. *Let $\pi : R[\bar{x}]_\sigma \to (A, \sigma)$ be an epimorphism of difference algebras over a difference ring (R, ς). Let $\bar{a} = \pi(\bar{x})$ be an associated choice of σ-generators of A, and let X_n be the projective system of Zariski closures constructed in [18, Subsection 2.1]. The following conditions are equivalent:*

(1) *π is a direct presentation of (A, σ) over (R, ς);*
(2) *$X \simeq [\varsigma]_R(X_0, X_1)$.*

Remark A.6. With notation from the previous lemma, if we have that $X_{n+1} \simeq X_n \times_{X_{n-1,\varsigma}} X_{n,\varsigma}$ for $n \geq 1$, then X is directly presented in a very strong sense.

The following results illustrate how near an arbitrary difference scheme is to a directly presented one.

Fact A.7.

(1) *If $(R, \varsigma) \to (A, \sigma)$ is a morphism of transformal domains of finite σ-type, then a finite σ-localisation of A is directly presented. This follows from a known result of difference algebra [19, Theorem 3.2.6] that a localisation of A is finitely σ-presented over A, followed by a simple choice of a longer tuple of generators in order to get a direct presentation.*
(2) *The 'Preparation Lemma' from [18, Subsection 2.1] yields the strong form of direct presentation through A.6, provided we shrink both A and R.*
(3) *An affine or projective difference scheme of finite total dimension over $\mathbb{Z}$ or a difference field can be embedded as a closed subscheme into a directly presented scheme with the same underlying algebraically reduced well-mixed structure, see [10, Corollary 4.36].*

Since directly presented difference schemes will mostly be used in the context where we will be interested only in their points with values in difference fields, we seek a framework that describes them suitably along the lines of A.4, and which is easily extended to generalised difference schemes.

Remark A.8. For a direct presentation (X, σ), in view of A.4 and 2.12, we have that

$$[\varsigma]_R(X_0, X_1)(F, \varphi) = (X, \sigma)^\sharp(F, \varphi) \simeq (X, \sigma)(F, \varphi).$$

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002

Thus, in considerations of difference field-valued points, we can neglect the distinction between a direct presentation and its associated difference scheme.

Remark A.9. Suppose that $(X, \Sigma)/(Y, \sigma)$ is a *finite* Galois cover of transformally integral difference schemes of finite transformal type over a transformal domain (R, ς) with group G as in [16] (the extension of associated function fields is algebraically finite). By σ-localising Y (and X), we can obtain a direct Galois cover with a rather special property that ${}^{\pi_1}() : G_1 \to G_0$ is an isomorphism (and both groups are isomorphic to G).

Note that more general direct covers considered in this paper (in spite of having finite fibres) correspond to situations in which the extension of the underlying function fields is algebraic (of finite transformal type) but not necessarily finite.

References

[1] The Stacks Project Authors, Stacks project, http://math.columbia.edu/algebraic_geometry/stacks-git.
[2] N. Bourbaki, Éléments de mathématique. Algèbre commutative. Chapitre 5: Entiers. Chapitre 6: Valuations, Actualités Scientifiques et Industrielles, vol. 1308, Hermann, Paris, 1964.
[3] Zoé Chatzidakis, Ehud Hrushovski, Model theory of difference fields, Trans. Amer. Math. Soc. 351 (8) (1999) 2997–3071.
[4] Richard M. Cohn, Difference Algebra, Interscience Publishers, John Wiley & Sons, New York–London–Sydney, 1965.
[5] M. Fried, G. Sacerdote, Solving Diophantine problems over all residue class fields of a number field and all finite fields, Ann. of Math. (2) 104 (2) (1976) 203–233.
[6] Michael D. Fried, Dan Haran, Moshe Jarden, Effective counting of the points of definable sets over finite fields, Israel J. Math. 85 (1–3) (1994) 103–133.
[7] Michael D. Fried, Moshe Jarden, Field Arithmetic, third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, vol. 11, Springer-Verlag, Berlin, 2008. Revised by Jarden.
[8] Alexandre Grothendieck, Revêtements étales et groupe fondamental (SGA 1), in: Documents Mathématiques (Paris), vol. 3, Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–1961. Directed by A. Grothendieck, with two papers by M. Raynaud, updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin (50 #7129)].
[9] Ehud Hrushovski, The Manin–Mumford conjecture and the model theory of difference fields, Ann. Pure Appl. Logic 112 (1) (2001) 43–115.
[10] Ehud Hrushovski, The elementary theory of the Frobenius automorphisms, arXiv:math/0406514, 2004. The most recent version of the paper (2012) is available at http://www.ma.huji.ac.il/~ehud/FROB.pdf.
[11] Serge Lang, Algebra, third edition, Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
[12] Angus Macintyre, Generic automorphisms of fields, in: Joint AILA-KGS Model Theory Meeting, Florence, 1995, Ann. Pure Appl. Logic 88 (2–3) (1997) 165–180.
[13] David A. Madore, Fabrice Orgogozo, Calculabilité de la cohomologie étale modulo l, arXiv:1304.5376.
[14] Mark Ryten, Ivan Tomašić, ACFA and measurability, Selecta Math. (N.S.) 11 (3–4) (2005) 523–537.
[15] A. Seidenberg, Constructions in algebra, Trans. Amer. Math. Soc. 197 (1974) 273–313.
[16] Ivan Tomašić, A twisted theorem of Chebotarev, Proc. Lond. Math. Soc. (3) 108 (2) (2014) 291–326.
[17] Ivan Tomašić, Galois stratification and ACFA, Ann. Pure Appl. Logic 166 (5) (2015) 639–663.
[18] Ivan Tomašić, Twisted Galois stratification, Nagoya Math. J. 222 (2016) 1–60.
[19] Michael Wibmer, Algebraic difference equations, lecture notes, http://www.algebra.rwth-aachen.de/de/Mitarbeiter/Wibmer/AlgebraicDifferenceEquations.pdf, 2013.

Please cite this article in press as: I. Tomašić, Direct twisted Galois stratification, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.07.002