Model Theory of Finite Difference Fields and Simple Groups

Mark Jonathan Ryten

Submitted in accordance with the requirements of the degree of PhD

The University of Leeds

Department of Pure Mathematics

February 2007

Abstract

Asymptotic classes are classes of finite structures which have uniformly definable estimates for the cardinalities of their first-order definable sets akin to those in finite fields given by the Lang-Weil estimates. The goal of the thesis is to prove that the finite simple groups of a fixed Lie type and Lie rank form asymptotic classes. This requires the following:

1. The introduction describes the background.

2. Chapter 4 shows a general method of generating one asymptotic class of structures from another through the notion of bi-interpretability. Specifically, the notions we introduce are those of *uniform parameter bi-interpretability* and *strong uniform parameter bi-interpretability.* We prove that being an asymptotic class is preserved under strong uniform parameter bi-interpretability.

3. Chapter 5 shows that classes of finite simple groups of a fixed Lie type and Lie rank are strongly uniformly parameter bi-interpretable with specific classes of finite fields or finite difference fields. This reduces our task to demonstrating that certain classes of finite difference fields form asymptotic classes.

4. Chapter 2 yields a definability of measure result for the finite σ-degree sets in the theory $ACFA$. The principal result of the chapter is Theorem 2.1.1, and it is published in work with Ivan Tomasic, in [25]. In a similar vein, Chapter 3 develops the asymptotic theory of finite fields equipped with fractional powers of the Frobenius. Equipped with this almost theory, we demonstrate the existence of many asymptotic classes of finite difference fields. In particular, we demonstrate that the classes of finite difference fields found in Chapter 5 to be uniformly parameter bi-interpretable with certain classes of finite simple groups do form asymptotic classes. Combining our results we achieve the goal of the thesis.

Acknowledgements

This PhD has taken the best part of a decade. Many things have happened; there are many people to thank. I shall, of course, mistakenly omit someone, and I apologise for this:

It is difficult to thank **Dugald Macpherson** enough. When I returned to England and went to Leeds I was an unknown and unwell quantity. Dugald gave me a project that would grow as I gained in knowledge and confidence, gave me time, patience and kindness. I do not think one could ask for a more generous or better supervisor.

I thank **Ehud Hrushovski** for the wonderful mathematics that lies at the core of this thesis and for answering many of my questions over many years.

I studied and learnt model theory with a fantastic group of students: in particular, **Assaf Hasson**, **Moshe Kamensky**, **Alex Ussvyatov** and **Yoav Yaffe**. Much of what I learnt and know today is thanks to discussions with them.

Not only do many of the ideas in this thesis come from discussions with **Richard Elwes**, but he had the goodness to house me for years during my treks up to Leeds.

Since I think of this PhD more as a tapestry of my last decade than as a research project, I must tell of the giants that have strode over my life throughout this time like colossal heroes of old:

This all started at 3 The Mead. I liked maths at school, but it was **Humphrey Cole** who showed me exciting, interesting maths. Then, I began to *love* it. Without love, this could never have finished. So I thank him, and I shall always remember him dearly.

My father always seemed to think a PhD in mathematics was a wonderful thing.

Unflappable and ever convinced the results will be splendid, it is a struggle to live up to his high hopes and expectations, but I am very happy to have him in my corner.

My mother's views on this PhD were mixed: she was very happy and proud that I was doing research and that I had gone to Israel. She was worried that I would not finish, and perhaps time justified that worry. Either way, she has always listened to me, sat with me and offered me sense and love.

Lily let me into her home with open arms, took care of me, introduced me to her commonsense and her brimming cup of Arabic aphorisms. How can one repay such a friend? **Charles** also let me into his home with great love and affection. We spent two years working on our PhDs side by side, and I will always remember them with pleasure.

All in all, I think that when I look back at this overlong project, I will remember it more affectionately than any other period in my life. Although I had known **Mina** for years before I went to Israel, her reign began with the start of the PhD. Her visits to Jerusalem, our walks, our adventures, and the bad period too, formed a core for our life together. I never would have had the guts to continue at just about everything that I have sweated at, if it had not been for Mina. Thanks is not really enough.

Contents

Chapter 1

Introduction

1.1 The thesis

This thesis lies at a confluence of model theory, classical algebraic geometry and the theory of finite simple groups. It examines the notions of *measurable* groups and *asymptotic classes of groups*.

Initially, the goal of the research was to classify low-dimensional measurable groups and primitive measurable group actions. In the course of the research it became apparent that these classifications were too difficult to obtain in full generality. However, there are analogous classifications for asymptotic classes of groups: namely to classify low-dimensional asymptotic classes of groups, and to classify uniformly definable primitive actions in asymptotic classes of groups. These classifications have been achieved, incorporating model theory of measurable structures, model theory of difference fields and the theory of finite simple groups. Ultraproducts of members of asymptotic classes of groups form a very rich and interesting sub-class of measurable groups, and so the restricted classifications are satisfying in their own right. This work is joint with Richard Elwes, in a manuscript in preparation. Although the results there depend on this thesis, they are not included here.

The core of the classification of low-dimensional asymptotic classes of groups, and the classification of uniformly definable primitive actions in asymptotic classes of groups lies in the following elegant, simple statement:

THEOREM 1.1.1 *Any family of finite simple groups of Lie type of bounded Lie rank forms an asymptotic class of groups.*

In fact, the proof of this result is deep, and its proof is the ultimate goal of this thesis.

The thesis is structured into the introduction and four subsequent chapters.

Chapter 2 yields a definability of measure result for the finite σ-degree sets in the theory $ACFA$. The principal result of the chapter is Theorem 2.1.1, and a proof of this theorem is published in joint work with Ivan Tomasic, in [25]. The proof we give in Chapter 2 is different from the published proof and is not joint work: here we use

classical methods of model theory; they are more to my taste, and very much in the flavour of the entire thesis.

Chapter 3 develops the asymptotic theory of finite fields equipped with fractional powers of the Frobenius. Equipped with this almost theory, we demonstrate the existence of many asymptotic classes of finite difference fields.

Chapter 4 shows a general method of generating one asymptotic class of structures from another through the notion of bi-interpretability. Specifically, the notions we introduce are those of *uniform parameter bi-interpretation* and *strong uniform parameter bi-interpretation.*

Chapter 5 shows that classes of finite simple groups of Lie type of bounded Lie rank are uniformly parameter bi-interpretable with asymptotic classes of finite difference fields identified in Chapter 3. This will form a crucial part of the proof of Theorem 1.1.1. In addition, this result combined with the results of Chapter 3 yields the asymptotic theory of the finite Suzuki and finite Ree groups.

In the introduction we shall endeavour to achieve several things. We shall give a broad and basic description of the model-theoretic phenomena that arise in the research we conducted. Ultimately, everything that is included in the thesis is done so because it is a necessary result in proving Theorem 1.1.1. However, this covers a range of model-theoretic techniques, and so a general introduction is useful. We will use the class of algebraically closed fields as a benchmark in the introduction to illustrate the types of model-theoretic phenomena we shall later encounter, and the methods we shall employ. We shall also endeavour where possible to explain how various techniques or phenomena pertain to our proof of Theorem 1.1.1; examples we give are those most relevant to the thesis. In short, the introduction is intended to give the flavour of the thesis. Necessarily, the introduction concludes with sections outlining technical, algebraic tools used later.

1.2 Basics of model theory

1.2.1 Structures, definable sets, axiomatisations and elementary classes

We have to begin somewhere. I take the notion of a first-order language $\mathcal{L}$ and an $\mathcal{L}$-structure as understood. Two wonderful references are [18] and [26]. But let us take a basic example. We define the language of rings $\mathcal{L}_{\text{rings}}$ as having two function symbols $\cdot$ and $+$ each of arity (number of inputs) 2, two constant symbols 0 and 1, and no additional relation symbols. A ring R interprets $\mathcal{L}_{\text{rings}}$ and is an $\mathcal{L}_{\text{rings}}$-structure.

A class $\mathcal{C}$ of $\mathcal{L}$-structures is said to be an **elementary class**, or **axiomatisable**, if there is a set of sentences T in $\mathcal{L}$ such that $\mathcal{C}$ is exactly the class of $\mathcal{L}$-structures that satisfy the sentences in T. We call a set of consistent sentences a **theory**. In this case, we say T is the the theory of $\mathcal{C}$. If an $\mathcal{L}$-structure $\mathcal{M}$ satisfies all the sentences of T, then we write $\mathcal{M} \models T$. It is easy to write an axiomatisation of the class of rings or the class of fields in $\mathcal{L}_{\text{rings}}$. One may also axiomatise the class of algebraically closed fields. An axiomatisation of a class of $\mathcal{L}$- structures is a typical goal in model theory: it captures exactly a determining set of properties of the class.

For a general first-order language $\mathcal{L}$ and $\mathcal{L}$-structure $\mathcal{M}$, a **definable set** is a subset of $\mathcal{M}^n$ for some n which is precisely the interpretation of an $\mathcal{L}$-formula with parameters from $\mathcal{M}$. We denote the system of all definable sets by $\text{Def}(\mathcal{M})$. For the case of $\mathcal{L}_{\text{rings}}$ and R a ring, we may give an alternative description of $\text{Def}(R)$. We say $\text{Def}(R)$ is the smallest system of sets with $\text{Def}(R) \subseteq \cup_{i\in\mathbb{N}}\wp(R^i)$, which contains the algebraic sets of R (these are the zero sets of ideals $I \lhd R[\bar{X}]$) and which is closed under boolean operations and projections. We mention the special case of an algebraically closed field $\tilde{K}$. There, by Chevalley's Theorem, we see that $\text{Def}(\tilde{K})$ is precisely the system of constructible sets in powers of $\tilde{K}$.

An **$\emptyset$-definable set** is a subset of $\mathcal{M}^n$ for some n which is precisely the interpretation of an $\mathcal{L}$-formula *without* use of parameters from $\mathcal{M}$.

Now we focus on the two examples of languages and structures which are central to

this thesis.

First, we consider $\mathcal{L}_{\text{groups}}$. It has two functions, $^{-1}$ of arity 1, and $\cdot$ of arity 2. It has one constant symbol 1. The class of groups is clearly axiomatisable in $\mathcal{L}_{\text{groups}}$. If G is a group then we may describe $\text{Def}(G)$ analogously to the fields case: we define a **group string** S to be a finite string of variables and their inverses, and of elements of G and their inverses. We define a **group polynomial** in n variables to be an equation $S = 1$ where S is a group string in n variables. We define a **group variety** $V \subseteq G^n$ to be the set of solutions in G^n to a system of group polynomials in n variables. Here then, $\text{Def}(G)$ is the smallest system of sets with $\text{Def}(G) \subseteq \cup_{i\in\mathbb{N}}\wp(G^i)$, containing all the group varieties of G, and closed under both boolean operations and projections.

Secondly we consider $\mathcal{L}_{\text{diff}}$, the language of difference rings. A **difference ring** is a ring R with a specified endomorphism $\sigma : R \mapsto R$. We define $\mathcal{L}_{\text{diff}}$ to be the language $\mathcal{L}_{\text{rings}}$ augmented by a function symbol σ of arity 1. Then it is easy to see that the class of difference rings is an elementary class, axiomatisable in $\mathcal{L}_{\text{diff}}$. Difference fields are difference rings where the underlying ring is a field. An inversive difference field is a difference field (K, σ) where σ is an automorphism of K; the class of inversive difference fields is also an elementary class. It is inversive difference fields that we are most interested in. Now we describe $\text{Def}(K, \sigma)$. A **difference polynomial** over K is a polynomial with coefficients from K, with monomials in variables x_i and their σ-iterates $\sigma^j(x_i)$. For instance $\sigma(x) - x$ is a difference polynomial in 1 variable. A **difference equation** is an equation $P = 0$ where P is a difference polynomial. A **σ-closed set** in n variables is the zero set of a collection of difference equations in n variables. For instance, if (K, σ) is a difference field, the σ-closed set defined by $\sigma(x) - x = 0$ is the fixed subfield of σ. In the specific case where K is an algebraic closure of the finite field $\mathbb{F}_p$ and $\sigma = \text{Frob} : x \mapsto x^p$ this would be the prime subfield $\mathbb{F}_p$. Difference fields play a crucial role in the thesis, and the introduction contains a technical section 1.4.2 which summarises concepts from the theory of difference fields that will be used.

1.2.2 Ultraproducts, asymptotic theories and some central topics of this thesis

If I is an infinite set then a **filter** F on I is a collection of subsets of I which (a) does not contain $\emptyset$, (b) is closed under finite intersections, and (c) is closed under taking supersets. Maximal filters exist and are called **ultrafilters**. An ultrafilter $\mathcal{U}$ is characterised by the property that if $X \subseteq I$, then $X \in \mathcal{U}$ if and only if $I \backslash X \notin \mathcal{U}$. A **principal ultrafilter** is one of the form $\{X \subseteq I : a \in X\}$ for some $a \in I$.

Now suppose that $\mathcal{C} = \{C_i : \ i \in I\}$ is a collection of $\mathcal{L}$-structures. Often the C_i will be finite. Let $\mathcal{U}$ be an ultrafilter on I. We define an equivalence relation $\sim_{\mathcal{U}}$ on $\prod_{i \in I} C_i$ by $(a_i)_{i \in I} \sim (b_i)_{i \in I}$ if $\{i : a_i = b_i\} \in \mathcal{U}$. Let $C := \prod_{i \in I} C_i / \sim_{\mathcal{U}}$. Then the reader can check that C is naturally an $\mathcal{L}$-structure: constants and functions are defined componentwise. Let $a \in C$ have a representative $(a_i)_{i \in I}$. For a unary relation R of $\mathcal{L}$, $R(a)$ holds if $\{i : C_i \models R(a_i)\} \in \mathcal{U}$. Relations of higher arity are similar. We call the $\mathcal{L}$-structure C an **ultraproduct** of the members of $\mathcal{C}$ with respect to the ultrafilter $\mathcal{U}$.

The fundamental theorem about ultraproducts is called $\mathcal{L}$os's theorem:

THEOREM 1.2.1 *Let $\theta(x_1, \ldots, x_n)$ be an $\mathcal{L}$-formula. Let $a_1, \ldots, a_n \in C$ have representatives $(a_{1i})_{i \in I}, \ldots, (a_{ni})_{i \in I}$ respectively. Then $C \models \theta(a_1, \ldots, a_n)$ if and only if $\{i \in I : C_i \models \theta(a_{1i}, \ldots, a_{ni})\} \in \mathcal{U}$.*

$\mathcal{L}$os's theorem shows that in some sense an ultraproduct gives an average of its component structures.

We shall make use of many non-principal ultraproducts in this thesis, and it would involve much superfluous notation to define specific index sets and ultrafilters each time. We shall sometimes use the notation $\prod_{i \in I} D_i / \sim$. This is always meant to denote a *non-principal* ultraproduct. Usually, an index set I is understood, or it is left to the reader to see that for the given purposes an appropriate index set I may be selected. The D_i will always be an I-indexed collection of $\mathcal{L}$-structures in a language $\mathcal{L}$. In all the ultraproducts we consider, both $\mathcal{L}$, and the set of structures $\mathcal{C}$ from which the D_i are selected, will be transparent. We shall usually suppress the particular non-

principal ultrafilter $\mathcal{U}$ on I which is used. It is not important. What is important is that non-principal ultrafilters exist, and that $\mathcal{L}$os's Theorem 1.2.1 may be applied to any non-principal ultraproduct. Thus in the notation $\prod_{i\in I} D_i/\sim$, the symbol $\sim$ is purely notational, and it denotes the equivalence relation on $\prod_{i\in I} D_i$ where two strings are equivalent if they agree on a set of components in the unstated ultrafilter $\mathcal{U}$. We shall also use the jargon 'components of the ultraproduct' and 'ultrafilter-many components'. A component of the ultraproduct $D = \prod_{i\in I} D_i/\sim_{\mathcal{U}}$ is a single $\mathcal{L}$-structure D_i. If we say something $\mathcal{E}$ occurs on ultrafilter-many components of D or that $\mathcal{E}$ occurs ultrafilter-many times, then this is to say that there is a set $J \subseteq I$ such that $J \in \mathcal{U}$, and for each $j \in J$, $\mathcal{E}$ occurs on D_j.

We may ask which $\mathcal{L}$-sentences hold in every structure in $\mathcal{C}$. We call this collection the **theory of all** $\mathcal{C}$ members. By $\mathcal{L}$os's theorem 1.2.1 these are exactly the sentences which hold in all ultraproducts of members of $\mathcal{C}$. However, the principal ultrafilters give dull ultraproducts (such an ultraproduct will be isomorphic to a member of the class.) More interesting is the theory T_∞ of all non-principal ultraproducts of members of the class. Clearly T_∞ is exactly the collection of $\mathcal{L}$-sentences which hold in all but finitely many members of $\mathcal{C}$, so we might refer to it as the **almost theory** of $\mathcal{C}$. If $\mathcal{C}$ is a class of finite $\mathcal{L}$-structures where for any $n \in \mathbb{N}$ there are only finitely members of $\mathcal{C}$ up to $\mathcal{L}$-isomorphism of cardinality less than n (such as when $\mathcal{L}$ is a finite language), then this is tantamount to asking which sentences hold for all members of $\mathcal{C}$ of greater than a fixed cardinality. In this case we may also call T_∞ the **asymptotic theory** of $\mathcal{C}$.

Let us give three examples of classes of structures central to the thesis. For the first two, an elegant axiomatisation of the almost theory has already been obtained. In chapter 3 we present one for the final class.

The first is the class of finite fields. In 1968 James Ax gave an axiomatisation of the asymptotic theory of finite fields; he called models of that theory **pseudo-finite fields**. The axiomatisation of a pseudo-finite field K is threefold: (a) K is perfect, (b) The absolute Galois group of K is $\hat{\mathbf{Z}}$, and (c) K is pseudo-algebraically closed (PAC), that is to say every absolutely irreducible variety defined over K has a K-rational point. It

is not immediately clear that these axioms can be expressed in $\mathcal{L}_{\text{rings}}$, but Ax shows that this is in fact the case. The truth of the third axiom for ultraproducts of finite fields follows from the Lang-Weil estimates:

THEOREM 1.2.2 *Let e, n, r be integers greater than 1. There is a positive constant C, such that for every prime power q and polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[X_1, \ldots, X_n]$ of total degree $\leq e$, if the algebraic set V defined by $f_1(X) = \ldots = f_r(X) = 0$ (where $X = (X_1, \ldots, X_n)$) is an absolutely irreducible variety of dimension d, then $||V(\mathbb{F}_q)| - q^d| \leq Cq^{d-\frac{1}{2}}$.*

The second example subsumes the first. For a field of characteristic p we denote the Frobenius automorphism $x \mapsto x^p$ as Frob. Model-theorists have studied the class of difference fields $\mathcal{C} = \{(\tilde{\mathbb{F}}_p, \text{Frob}^n) : p \text{ a prime}, n \in N\}$ for many years. Macintyre and later Chatzidakis and Hrushovski axiomatised and developed the model theory of the theory $ACFA$ (algebraically closed fields with an automorphism), a candidate for the almost theory of $\mathcal{C}$. The axiomatisation for $(K, \sigma) \models ACFA$ is given in Section 1.4.2. In his manuscript [13] Hrushovski proves a theorem giving estimates for difference fields analogous to the Lang-Weil estimates for finite fields. We refer to his theorem as Hrushovski's *correspondence estimates*. To understand his precise statement we need some notation: suppose $q = p^n$ where p is a prime and $n \geq 1$. Then let $\varphi_q :=\text{Frob}^n$. Suppose X is an affine variety defined by a set of polynomial equations $E = \{e_i : 1 \leq i \leq m\}$, with coefficients in a characteristic p field k. Then let X^{φ_q} be the affine variety defined by the set of polynomial equations $E^* = \{e_i^* : 1 \leq i \leq m\}$, where each e_i^* is obtained by applying φ_q to the coefficients of e_i. Let $\Phi_q(k) := \{(x, \varphi_q(x)) : x \in k\}$. Then Hrushovski's precise statement is:

THEOREM 1.2.3 *Let X be an affine variety over a base field k. Let $q = p^n$ where p is a prime and $n \geq 1$. Let $S \subseteq (X \times X^{\varphi_q})$ be an irreducible subvariety. Assume $\dim(S) = \dim(X) = d$, the maps $S \mapsto X$, $S \mapsto X'$ are dominant, and one is quasi-finite. Let $a = [S : X]/[S : X']_{insep}$. Then*

$$|S(k) \cap \Phi_q(k)| = aq^d + O(q^{d-\frac{1}{2}})$$

The reader will notice the similarity between these estimates and the Lang-Weil estimates. Using these estimates Hrushovski proved that $ACFA$ is indeed the asymptotic

theory of difference fields $(\tilde{\mathbb{F}}_p, \mathrm{Frob}^n)$. We call this the *elementary equivalence theorem for ACFA*, and it is presented explicitly in this thesis as Theorem 2.1.3. We shall use a version of Theorem 1.2.3 to prove the main theorem of Chapter 2 (Theorem 2.1.1). The version we use is presented as Theorem 2.1.2.

The third example is central to the thesis. Let m and n be coprime natural numbers with $n > 1$ and let p be a prime. Then we define the class of finite difference fields $\mathcal{C}_{(m,n,p)} := \{(\mathbb{F}_{p^{nk+m}}, \mathrm{Frob}^k) : k \in \mathbf{N}\}$. In Chapter 3 we introduce a theory $PSF_{(m,n,p)}$ in the language $\mathcal{L}_{\mathrm{diff}}$. The theory $PSF_{(m,n,p)}$ is the theory of a pseudo-finite field of characteristic p with an automorphism σ which satisfies $\mathrm{Frob}^m\sigma^n = \mathrm{id}$. It is the asymptotic theory of $\mathcal{C}_{(m,n,p)}$. In Section 5.4 we will show that for the special case of $n = 2,\ m = 1,\ p = 2$, the class $\mathcal{C}_{(1,2,2)}$ is uniformly parameter bi-interpretable with the class of finite Suzuki groups, and also with the class of finite Ree groups of type ${}^2F_4$; consequently the asymptotic theory $PSF_{(1,2,2)}$ may be translated into the asymptotic theory of the finite Suzuki groups, or of these Ree groups. Similarly in the case $n = 2,\ m = 1,\ p = 3$, the class $\mathcal{C}_{(1,2,3)}$ is uniformly parameter bi-interpretable with the class of finite Ree groups of type ${}^2G_2$, and consequently the asymptotic theory $PSF_{(1,2,3)}$ may be translated into the asymptotic theory of the finite Ree groups of type ${}^2G_2$. Bi-interpretations are introduced just below in subsection 1.2.6; the notion of uniform parameter bi-interpretations is is the key notion of Chapter 4 (see Definition 4.2.3).

1.2.3 Elementary extensions, existentially closed models and model companions

Let $\mathcal{M} \subseteq \mathcal{N}$ be a containment of $\mathcal{L}$-structures. We say $\mathcal{N}$ is an **elementary extension** of $\mathcal{M}$ if for any $\mathcal{L}$-formula $\theta(\bar{x}, \bar{d})$ with parameters $\bar{d} \subseteq \mathcal{M}$, if there is a tuple $\bar{c} \subseteq \mathcal{N}$ for which $\mathcal{N} \models \theta(\bar{c}, \bar{d})$ then there is another tuple $\bar{b} \subseteq \mathcal{M}$ such that $\mathcal{M} \models \theta(\bar{b}, \bar{d})$. If $\mathcal{N}$ is an elementary extension of $\mathcal{M}$ then we write $\mathcal{M} \prec \mathcal{N}$. Let $\mathcal{C}$ be a class of $\mathcal{L}$-structures. Let $M \in \mathcal{C}$. We say $\mathcal{M}$ is **existentially closed in C** if for any $\mathcal{L}$-structure $\mathcal{N} \in \mathcal{C}$, if $\mathcal{M} \subseteq \mathcal{N}$ then any quantifier-free formula over M which has a solution in N has a solution in M. The prototypical example is again an algebraically closed field $\tilde{K}$; all algebraically closed fields are existentially closed inside the class of fields. Hilbert's weak

nullstellensatz (that maximal ideals over an algebraically closed field $\tilde{K}$ correspond to tuples in $\tilde{K}$) is a consequence of this; conversely, recalling that the sets of $\mathrm{Def}(\tilde{K})$ are the constructible sets, then one can deduce that $\tilde{K}$ is existentially closed from Hilbert's weak nullstellensatz. The PAC property and Hrushovski's correspondence estimates 1.2.3 can similarly be thought of as nullstellensatzes in their contexts.

If T is a theory in the language $\mathcal{L}$ then T is **model-complete** if for any pair of models $M, N \models T$ with $M \subseteq N$, then $M \prec N$. T has a **model companion** T^* if (a) T^* is a theory in $\mathcal{L}$, (b) every model of T embeds into a model of T^* and every model of T^* embeds into a model of T, and (c) T^* is model-complete. Model companions are unique. The theory of algebraically closed fields is the model companion of the theory of fields. The theory $ACFA$ described above is the model companion of the theory of difference fields.

1.2.4 Quantifier eliminations

Understanding $\mathrm{Def}(\mathcal{M})$ is of paramount importance to the model-theorist. Usually, for algebraic structures like groups or rings or difference rings, $\mathrm{Def}(\mathcal{M})$ ostensibly captures only the most basic algebraic data about the structure. So the question becomes, how much of the deeper structure is captured in $\mathrm{Def}(\mathcal{M})$? That deeper structure may be topological: a linear group embedded in affine space has an induced Zariski topology, a profinite group carries a natural topology. Is the topology embedded in the group theoretic structure? One famous question of this flavour is the open subgroup question: is every finite index subgroup of a profinite group open?

So let us consider $\mathrm{Def}(\mathcal{M})$. It is formed inductively. The first tier of sets is the tier of **atomic sets**. These are the graphs of equations $t_1 = t_2$ where t_1 and t_2 are terms (iterated functions) in the language with parameters from $\mathcal{M}$, or graphs of relations with parameters from $\mathcal{M}$. We refer to the second tier as the **quantifier-free sets**. These are the sets obtained from atomic sets by boolean operations. Then we have the $\exists$**-sets** (projections of quantifier free sets), and the $\forall$**-sets** (complements of $\exists$-sets). In general a Σ_n**-set** (respectively a Π_n**-set**) is a set defined by a formula which starts with an existential (universal) quantifier and has $n-1$ alternations of existential and

universal quantifiers. We more natually refer to Σ_2-sets as $\exists\forall$-sets, and to Π_2-sets as $\forall\exists$-sets. So for instance if $\theta(y_1, y_2, \ldots, y_n, x_1, x_2, \ldots, x_m, \bar{z})$ is quantifier-free then the set defined by

$$\forall y_1 \forall y_2 \ldots \forall y_n \exists x_1 \exists x_2 \ldots \exists x_m (\theta(y_1, y_2, \ldots, y_n, x_1, x_2, \ldots, x_m, \bar{z}))$$

is $\forall\exists$. Then $\mathrm{Def}(\mathcal{M})$ is the collection of all such sets as n ranges over the natural numbers.

The problem with $\mathrm{Def}(\mathcal{M})$ is that in general we may have little idea what a set obtained by iterated projections and boolean operations looks like. In the case of the algebraically closed field $\tilde{K}$ however, this problem does not exist. Chevalley's theorem tells us that $\mathrm{Def}(\mathcal{M})$ consists exactly of the constructible sets. Projections add no complexity. Model theorists would say "algebraically closed fields eliminate quantifiers". In general, suppose we have a theory T. Then we say T **eliminates quantifiers** if for any $\mathcal{L}$- formula $\theta(\bar{x})$, there is a quantifier-free $\mathcal{L}$-formula $\theta^*(\bar{x})$ such that for any model $\mathcal{M} \models T$ and tuple $\bar{c} \subseteq \mathcal{M}$, then $\mathcal{M} \models \theta(\bar{c}) \Leftrightarrow \theta^*(\bar{c})$.

In some cases we may not be fortunate enough to eliminate all quantifiers. The structures we are most interested in in this thesis are a case in point. However, we obtain an approximation to quantifier elimination which is sometimes referred to as near model completeness. Let T be a theory. T is **near model complete** if for every $\mathcal{L}$-formula $\theta(\bar{x})$ there is an $\mathcal{L}$-formula $\theta^*(\bar{x})$ which is a boolean combination of $\exists$-formulae such that for all models $\mathcal{M} \models T$ and tuples $\bar{c} \subseteq \mathcal{M}$, then $\mathcal{M} \models \theta(\bar{c}) \Leftrightarrow \theta^*(\bar{c})$. The asymptotic theory of finite fields (defined in subsection 1.2.2) is near model complete.
Let $\mathcal{L}_{\mathrm{rings},c}$ be the language of rings with constants $c = \{c_{ni} : \ n > 1, \ 1 \leq i \leq n\}$. In [10], the $\mathcal{L}_{\mathrm{rings},c}$-theory T of enriched pseudo-finite fields was introduced. Enriched pseudo-finite fields are pseudo-finite fields, and have the elimination form that for any $\mathcal{L}_{\mathrm{rings},,c}$-formula $\theta(\bar{x}, c)$, there is an $\mathcal{L}_{\mathrm{rings},c}$-formula $\theta^*(\bar{x}, c)$ such that for any model $\mathcal{M} \models T$ and tuple $\bar{d} \subseteq \mathcal{M}$, then $\mathcal{M} \models \theta(\bar{d}) \Leftrightarrow \theta^*(\bar{d})$; the formula $\theta^*(\bar{x})$ is a conjunction of formulas $\exists T(g(\bar{x}, c, T) = 0)$, where T is a single variable and $g(\bar{x}, c, T) \in \mathbb{Z}[\bar{x}, c, T]$. Otherwise put, we have every formula equivalent to a conjunction of formulas $\exists T(t_1(\bar{x}, T) = t_2(\bar{x}, T))$ where t_1 and t_2 are terms in the language.

We shall call this **positive near model completeness**. In [10], positive near model completeness was made use of to generalise the Lang-Weil estimates (presented above as Theorem 1.2.2): in the language of this thesis the positive near model completeness and the Lang-Weil estimates show that the class of finite fields forms an asymptotic class. Let us define the equivalent notions for $\forall\exists$-formulae to be **near*-model completeness** and **positive near*-model completeness** .

Let m and n be coprime natural numbers with $n > 1$. Let p be a prime. In Chapter 3 we demonstrate the near model completeness of the asymptotic theory $PSF_{(m,n,p)}$ (see section 1.2.2 for a definition) of the class of finite difference fields $\mathcal{C}_{(m,n,p)}$. We also demonstrate the positive near model completeness of enriched finite difference fields $PSF_{(m,n,p,c)}$ (see subsection 3.3.2 for a definition). Using that, one may deduce the near*-model completeness of the asymptotic theories of finite Suzuki groups and both types of finite Ree groups, but we do not include this in the thesis. More importantly, in the same way that the Lang-Weil estimates and positive near model completeness of the asympotic theory of finite fields imply that finite fields form an asympotic class, positive near model completeness of $PSF_{(m,n,p,c)}$ and our generalisation (Theorem 2.1.1) of Theorem 1.2.3 are shown in Chapter 3 to imply that $\mathcal{C}_{(m,n,p)}$ is an asymptotic class of difference fields.

1.2.5 Dimension theories

We have repeatedly mentioned algebraically closed fields. The reader will be acquainted with the dimension theory for algebraic varieties. Over algebraically closed fields, since all definable sets are finite unions of locally closed sets, a dimension theory obviously extends to all definable sets. This is part of a much larger phenomenon in model theory. Dimension theories are central to modern model theory, especially in the study of stable and simple theories.

As an example, we now consider a rank known as S_1-rank. Let M be an uncountably saturated model. The S_1 rank is defined on any set which is the interpretation in M of a formula $\theta \in \mathrm{Def}(\mathcal{M})$:

1. $S_1(\theta) > 0$ iff θ has infinitely many solutions.

2. $S_1(\theta) > n+1$ iff there exists an infinite sequence $(b_i)_{i\in\omega}$ of distinct elements and a formula $\varphi(x,y)$ such that:

   (a) for some $k \in \mathbb{N}$, for any k distinct elements $S_1(\varphi(x,b_{i_1}) \wedge \ldots \wedge \varphi(x,b_{i_k})) \leq n$

   (b) ($S_1(\theta \ \wedge \ \varphi(x,b_i)) > n$ for each i.

In subsection 1.2.7 of this introduction we introduce asymptotic classes. They are central to the thesis. It will transpire that any non-principal ultraproduct of members of an asymptotic class has finite S_1-rank. Finite S_1-rank structures have been much studied by model-theorists. However, the S_1-rank is combinatorial and often hard to characterise. In this thesis we show the classes $\mathcal{C}_{(m,n,p)}$ are asymptotic classes, but we work with a more natural notion of dimension for difference fields that bounds the S_1-rank above. It is the notion of σ-degree, and it is defined in Section 1.4.2. The most important fact for us is that in $ACFA$ σ-degree is definable: see Section 2.1.3 in Chapter 2 for an explanation.

1.2.6 Interpretations and bi-interpretations

One important measure of model theoretic complexity is the notion of the interpretation of one structure in another. Suppose $\mathcal{M}$ is an $\mathcal{L}_1$-structure and $\mathcal{N}$ is an $\mathcal{L}_2$-structure. We say $\mathcal{N}$ **interprets** $\mathcal{M}$ if

- there is a set $X \in \mathrm{Def}(\mathcal{N})$ and an equivalence relation $E \in \mathrm{Def}(\mathcal{N})$ on X. Let $p : X \mapsto X/E$ be the quotient map; we see that p naturally extends to a map $X^n \mapsto (X/E)^n$.

- there are definable subsets $S_i \subseteq X^{n_i}$ of cartesian powers of X which also lie in $\mathrm{Def}(\mathcal{N})$, and the quotients X/E together with $p(S_i)$ interpret the relation symbols, function symbols, and constant symbols of $\mathcal{L}_1$, in such a way that the resulting $\mathcal{L}_1$-structure $\mathcal{M}^*$ is isomorphic to $\mathcal{M}$.

- If there is no need for an equivalence relation E, then we say $\mathcal{M}$ **is definable in** $\mathcal{N}$.

- If there is no need for parameters in the interpretation we say $\mathcal{N}$ **$\emptyset$-interprets** $\mathcal{M}$.

Some important examples of interpretations are (1) the reals as a field interpeting the complexes, (2) the integers equipped with $+$ and $\cdot$ interpreting the rationals, (3) Zermelo-Fraenkel set theory interpreting Peano Arithmetic and (4) a field K interpreting a linear group over K.

Suppose as above that $\mathcal{N}$ defines $\mathcal{M}$ as $\mathcal{M}^*$ via the $\mathcal{L}_1$-isomorphism $f : \mathcal{M} \to \mathcal{M}^*$. Then the structure **induced** on $\mathcal{M}$ by $\mathcal{N}$ is the system of sets $\{f^{-1}(Y \cap \mathcal{M}^{*m}) : Y \in \mathrm{Def}(\mathcal{N})\}$. It is certainly as rich as the system $\mathrm{Def}(\mathcal{M})$. In some cases it is richer: for instance, the complex numbers as a field do not define the reals.

In other cases, two structures $\mathcal{M}$ and $\mathcal{N}$ may interpret each other in a special way that shows they have the same complexity. We call this a parameter bi-interpretation. If $\mathcal{M}$ is an $\mathcal{L}_1$-structure and $\mathcal{N}$ is an $\mathcal{L}_2$-structure, a **parameter bi-interpretation** between $\mathcal{M}$ and $\mathcal{N}$ is firstly an interpretation $\mathcal{M}^*$ of $\mathcal{M}$ in $\mathcal{N}$ via an $\mathcal{L}_1$-isomorphism $f : \mathcal{M} \to \mathcal{M}^*$, together with an interpretation $\mathcal{N}^*$ of $\mathcal{N}$ in $\mathcal{M}$ via an $\mathcal{L}_2$-isomorphism $g : \mathcal{N} \to \mathcal{N}^*$. The isomorphism f induces an isomorphism f' from $\mathcal{N}^*$ to an $\mathcal{L}_2$-structure $\mathcal{N}^{**}$ interpreted in $\mathcal{M}^*$ and in turn interpreted in $\mathcal{N}$. Similarly, the isomorphism g induces an isomorphism g' from $\mathcal{M}^*$ to an $\mathcal{L}_1$-structure $\mathcal{M}^{**}$ interpreted in $\mathcal{N}^*$ and in turn interpreted in $\mathcal{M}$. In a parameter bi-interpretation the isomorphisms $g'f : \mathcal{M} \to \mathcal{M}^{**}$ and $f'g : \mathcal{N} \to \mathcal{N}^{**}$ are definable in $\mathcal{M}$ and $\mathcal{N}$ respectively.

If there is no need for parameters in the bi-interpretation we say there is an **$\emptyset$-bi-interpretation** between $\mathcal{N}$ and $\mathcal{M}$.

The reader will see that where there is a bi-interpretation between $\mathcal{N}$ and $\mathcal{M}$ and in fact $\mathcal{N}$ and $\mathcal{M}$ in the bi-interpretation are defined in each other, then in some sense $\mathrm{Def}(\mathcal{N})$ and $\mathrm{Def}(\mathcal{M})$ are identical. A basic example is that the group $SL_2(\tilde{K})$ is bi-

interpretable with the algebraically closed field $\tilde{K}$, and no equivalence relations are necessary in the bi-interpretations. In this case a corollary of the bi-interpretation is that there is no additional structure induced on $SL_2(\tilde{K})$ by its obvious embedding in $\mathbf{A}^4$: its induced Zariski topology is obtainable at the level of group varieties. If $\mathcal{M}$ and $\mathcal{N}$ are bi-interpretable then often a nice property of $\mathcal{M}$ may be inherited by $\mathcal{N}$.

The difference between parameter bi-interpretations and $\emptyset$-bi-interpretations will be an issue that requires delicate treatment in the thesis, for parameter interpretations and bi-interpretations are inherently 'weaker' than $\emptyset$-interpretations or $\emptyset$-bi-interpretations.

Ultimately, in Chapter 5, we shall show that families of finite simple groups of Lie Type of bounded Lie rank form asymptotic classes because their members are parameter bi-interpretable with the members of certain families of finite fields or finite difference fields. The bi-interpretations will necessarily make use of parameters. In order that the families of finite simple groups are proved to be asymptotic classes it is insufficient to show that they are pairwise bi-interpretable with specific finite fields or difference fields. We shall require a uniformity in the family of parameter bi-interpretations, which we call *strong uniform parameter bi-interpretations.* These are defined in Chapter 4, and there we prove the following fundamental lemma:

PROPOSITION 1.2.4 *1. Suppose $\mathcal{D}$ is an asymptotic class in a language $\mathcal{L}_2$. Suppose $\mathcal{C}$ is a class of $\mathcal{L}_1$-structures and suppose $\mathcal{C}$ is strongly uniformly parameter bi-interpretable with $\mathcal{D}$. Then $\mathcal{C}$ is an asymptotic class.*

1.2.7 Asymptotic classes

The three examples of section 1.2.2 are bound by a common feature: their structure is largely determined by the solution sizes given by the Lang-Weil estimates or Hrushovski correspondence estimates. Let $\mathcal{C}$ be either (a) the class of finite fields or (b) the class of difference fields $\mathcal{C} = \{(\tilde{\mathbb{F}}_p, \mathrm{Frob}^n) : p \text{ a prime}, \ n \in N\}$. In the case of (a) let U be the formula $x = x$, and in case (b) let U be the formula $\sigma(x) = x$. In each case, the appropriate estimates mean we may fix a definable set D of the right type and look at its set of rational points $D(C)$ for any $C \in \mathcal{C}$. We can then estimate $|D(C)|$ as a polynomial in the cardinality of $|U(C)|$. In the case of finite fields, looking at the

Lang-Weil estimates, the sets D that can be estimated must be absolutely irreducible varieties. But this was generalised in [10] so that D may be taken to be any definable set in the language of rings. Taking finite fields as their motivation, Macpherson and Steinhorn considered a class of finite $\mathcal{L}$-structures $\mathcal{C}$, where for any $C \in \mathcal{C}$ definable sets have cardinalities given approximately by expressions $\mu \cdot |C|^d$ for fixed numbers μ and d. In [23], they initiated the study of asymptotic classes and measurable structures. Here are their original definitions:

DEFINITION 1.2.5 Let $\mathcal{L}$ be a first order language, and $\mathcal{C}$ be a collection of finite $\mathcal{L}$-structures. Then $\mathcal{C}$ is a *1-dimensional asymptotic class* if the following hold for every $m \in \mathbb{N}$ and every formula $\varphi(x, \bar{y})$, where $\bar{y} = (y_1, \ldots, y_m)$.
(i) There is a positive constant C and a finite set $E \subset \mathbb{R}^{>0}$ such that for every $M \in \mathcal{C}$ and $\bar{a} \in M^m$, either $|\varphi(M, \bar{a})| \leq C$, or for some $\mu \in E$,

$$||\varphi(M, \bar{a})| - \mu|M|| \leq C|M|^{\frac{1}{2}}.$$

(ii) For every $\mu \in E$, there is an $\mathcal{L}$-formula $\varphi_\mu(\bar{y})$, such that $\varphi_\mu(M^m)$ is precisely the set of $\bar{a} \in M^m$ with

$$||\varphi(M, \bar{a})| - \mu|M|| \leq C|M|^{\frac{1}{2}}.$$

Their first basic proposition is so central to work around asymptotic classes that it is almost part of the definition:

PROPOSITION 1.2.6 *Suppose $\mathcal{C}$ is a 1-dimensional asymptotic class of finite $\mathcal{L}$-structures. Then the following holds, for every $m, n \in \mathbb{N}$ and every formula $\varphi(\bar{x}, \bar{y})$, where $\bar{x} = (x_1, \ldots, x_n)$ and $\bar{y} = (y_1, \ldots, y_m)$.*
(i) There is a positive constant C and a finite set D of pairs (d, μ) with $d \in \{0, \ldots, n\}$ and $\mu \in \mathbb{R}^{>0}$, such that for every $M \in \mathcal{C}$ and $\bar{a} \in M^m$, if $\varphi(M^n, \bar{a})$ is non-empty then for some $(d, \mu) \in D$,

$$||\varphi(M^n, \bar{a})| - \mu|M|^d| \leq C|M|^{d-\frac{1}{2}}.$$

(ii) For every $(d, \mu) \in D$, there is an $\mathcal{L}$-formula $\varphi_{d,\mu}(\bar{y})$, such that $\varphi_{d,\mu}(M^m)$ is precisely the set of $\bar{a} \in M^m$ with

$$||\varphi(M^n, \bar{a})| - \mu|M|^d| \leq C|M|^{d-\frac{1}{2}}.$$

There is no particular reason to restrict to 1-dimensional asymptotic classes. Elwes [12] generalises in the following way:

DEFINITION 1.2.7 *A class $\mathcal{C}$ of finite $\mathcal{L}$-structures is an N-dimensional asymptotic class if*

(i) for every $\mathcal{L}$-formula $\varphi(x, \overline{y})$ where length$(\overline{y}) = m$, there exists finite $D \subset \{0, ..., N\} \times \mathbb{R}^{>0} \cup \{(0,0)\}$ and a partition $\{\Phi_{(d,\mu)} : (d, \mu) \in D\}$ of $\{\{M\} \times M^m : M \in \mathcal{C}\}$ so that for $(M, \overline{a}) \in \Phi_{(d,\mu)}$
we have

$$||\varphi(M, \overline{a})| - \mu |M|^{\frac{d}{N}}|| = o(|M|^{\frac{d}{N}})$$

as $|M| \longrightarrow \infty$.

(ii) Moreover each $\Phi_{(d,\mu)}$ is definable, that is to say $\{\overline{a} \in M : (M, \overline{a}) \in \Phi_{(d,\mu)}\}$ is uniformly $\emptyset$-definable across $\mathcal{C}$.

The definition above considers only sets in 1 variable, but Elwes shows, in a proposition similar to 1.2.6, that the equivalent condition for sets in n variables is automatic, the only change being that now the dimension of a set in n variables lies in $\{0, \ldots, Nn\}$.

We shall refer to the dimension in Definition 1.2.7 variously as *asymptotic dimension* or simply as the *dimension* of a particular asymptotic class. Definition 1.2.7 is the key definition for the purposes of this thesis, as the asymptotic classes crucial to the work are typically of asymptotic dimension greater than 1, and so, concretely, it is the definition of asymptotic classes which we will use throughout.

We shall refer to clause (i) of Definition 1.2.7 as the first criterion for asymptotic classes, and (ii) as the second criterion for asymptotic classes, or the definability of measure.

Let us also note that the dimension in 1.2.7 is not unique for an asymptotic class. If $\mathcal{C}$ is an N-dimensional class, then $\mathcal{C}$ is also a $k \cdot N$-dimensional asymptotic class for any $k \in \mathbb{N}$. Normally, if we compute dimension, we shall compute the minimal possible

dimension N for an asymptotic class.

It will transpire in Chapter 5 that the families of finite simple groups of Lie type of bounded Lie rank form asymptotic classes but not of dimension 1: in such families there are uniformly definable families of sets such that each set is much smaller in cardinality than than the particular group in which it is defined.

Taking non-principal ultraproducts of members of an asymptotic class yields an infinite structure with a non-standard counting measure coming from the μ above. The generalisation, to an infinite measurable structure, is natural. Here is a definition:

DEFINITION 1.2.8 Let $\mathcal{M}$ be an $\mathcal{L}$-structure and let $\mathrm{Def}(M)$ be the union, over all positive integers n, of the collections of parameter definable non-empty subsets of M^n. Then $\mathcal{M}$ is *measurable* if there is a function $h : \mathrm{Def}(M) \to \mathbb{N} \times \mathbb{R}^{>0}$ satisfying the following (where we write $h(X)$ as $(\dim(X), \mathrm{meas}(X))$).

(i) If $X \in \mathrm{Def}(M)$ is finite non-empty then $h(X) = (0, |X|)$.

(ii) For every formula $\varphi(\bar{x}, \bar{y})$ there is finite $D \subset \mathbb{N} \times \mathbb{R}^{>0}$ so that:
(a) for all $\bar{a} \in M^m$, $h(\varphi(M^n, \bar{a})) \in D$.
(b) for all $(d, \mu) \in D$, $\{\bar{y} \in M^m : h(\varphi(M^n, \bar{y})) = (d, \mu)\}$ is 0-definable.

(iii) Let $X, Y \in \mathrm{Def}(M)$ and $f : X \to Y$ be a definable surjection. By (ii), there is $r \in \omega$ and $(d_1, \mu_1), \ldots, (d_r, \mu_r) \in \mathbb{N} \times \mathbb{R}^{>0}$ so that if $Y_i := \{\bar{y} \in Y : h(f^{-1}(\bar{y})) = (d_i, \mu_i)\}$, then $Y = Y_1 \cup \ldots \cup Y_r$ is a partition of Y into non-empty disjoint definable sets. Let $h(Y_i) = (e_i, \nu_i)$ for $i = 1, \ldots, r$. Also let $c := \mathrm{Max}\{d_1 + e_1, \ldots, d_r + e_r\}$, and suppose this maximum is attained by $d_1 + e_1, \ldots, d_s + e_s$. Then $h(X) = (c, \mu_1\nu_1 + \ldots + \mu_s\nu_s)$.

If $h(X) = (d, \mu)$, we call d the *dimension* of X and μ the *measure* of X, and h the *measuring function*. We often write $h_i(X)$ for the projection of $h(X)$ to the i^{th} coordinate (for $i = 1, 2$).

A measure μ on M is said to be *normalised* if M itself has measure 1.

We say that a complete theory T is *measurable* if it has a measurable model.

1.3 The results of this thesis put in context

We now give chapter-related results proved in this area and how ours fit in:

Chapter 2: The whole chapter is to prove Theorem 2.1.1. The debt to Hrushovski's Theorem 1.1 in [13] cannot be overstated. One can draw an analogy between our Theorem 2.1.1's relation to Hrushovski's correspondence estimates and the relation between the main theorem of [10] and the Lang-Weil estimates: in both cases definable estimates for a base class of families of definable sets are extended to a larger class. The lemmas 2.4.3 and 2.4.4 in Section 2.4 are simply relativisations to the difference fields setting of lemmas 3.5 and 3.7 of [10]. Theorem 2.1.1 is published in [25]. Here I have endeavoured to prove the result in a more classical way, using only notions of definability, first-order compactness, and results about the theory of algebraically closed fields and the theory $ACFA$. The proof here, though perhaps more long-winded, really is in the same spirit as the lovely paper [10], and I prefer it.

Chapter 3: Again, the debt to Hrushovski's work in [13], the work of Chatzidakis and Hrushovski in [8], and the work of Chatzidakis, Hrushovski and Peterzil in [9], is immense. Simply, none of these results would exist without their core work. We are essentially describing the first-order theory of certain uniformly definable reduct difference fields of models of $ACFA$ (the solution sets to the equations $\mathrm{Frob}^m\sigma^n = \mathrm{id}$). Our addition to existing knowledge is that we have axiomatised this class of reducts, and described their model theory in their own right, and not relative to the enveloping models of $ACFA$.

We should point out that our reduct difference fields were not new. In Theorem 3.3.22 we apply a strong result from [9] directly concerning them.

The classes $\mathcal{C}_{(m,n,p)}$ and the resulting models of the theories $PSF_{(m,n,p)}$ have prime p characteristic. $ACFA$ and our results in Chapter 1 are valid, however, for characteristic 0. The reason for this is essentially accidental: when I began to consider these classes it was to find the exact classes of finite difference fields that matched a class of finite simple Suzuki or Ree groups. These are the classes $\mathcal{C}_{(1,2,2)}$ and $\mathcal{C}_{(1,2,3)}$. So much was my focus that the work was called 'Square Roots of the Frobenius'. I managed the conceptual leap to generalise to arbitrary fractional powers of Frobenius, but alas, did not examine the effect of relaxing the restriction on the prime. My feeling is very very strongly that there is no problem whatsoever with relaxing this restriction, and thus obtaining characteristic 0 pseudo-finite difference fields in our framework. Unfortunately, this work is not included in the thesis.

We have included decidability results at the end of Section 3.3.4 that follow directly from the decidability results in [8] 1.6. Let us just point out that the decidability results here answer the last question in [24].

Chapter 4: The first section develops a tool to capture the definability of measure in the theory of finite simple groups of a fixed Lie rank and Lie type. I do not know any direct precursor to this work.

The second section is a restatement in a convenient form of the group generation results for supersimple groups found in [29]. I learnt of these results initially in [15]. We apply them essentially through Lemma 4.3.11, which is in turn based on 4.3.10. Behind Lemma 4.3.10 is the result that in a simple group defined in a theory such as $ACFA$ or $PSF_{(m,n,p)}$), if the group has 'finite dimension', then for any infinite definable subset X invariant under conjugation, there is $t = t(X)$ such that the group is generated in at most t steps by X. By Hrushovski's results these groups are exactly the simple pseudo-finite groups. So imagine such a family of simple groups $G(q)$. Then the number t translates into an absolute upper bound on the number of steps it takes $X(q)$ to generate $G(q)$. Hrushovski states the particular case of generation by conjugacy classes as Theorem 1.9 of [13]. It seems that if X is an $\mathcal{L}_{\text{groups}}$-definable set (as for example conjugacy classes are), then this result is already a consequence of the work

of Francoise Point in [24].

Chapter 5: Here we construct our uniform bi-interpretations between families of finite simple groups and families of finite fields or finite difference fields. Several mathematicians have made notable contributions in this area:

Simon Thomas's thesis [27] dealt with classification of locally finite, stable simple groups. His methods involved interpreting fields of definition uniformly inside finite simple groups of Lie type. We have differed in places in our construction but the ideas we use to interpret fields are similar. In particular Thomas found the field of definition inside groups of type ${}^2B_2$ and ${}^2G_2$. He did not find the difference field automorphism living inside those groups. Adding this to his work as well as the wealth of results on finite fields and finite difference fields, and working inside our framework of uniform parameter bi-interpretations, we may obtain an elimination form for the groups of type ${}^2B_2$ and ${}^2G_2$ and an axiomatisation for their almost theory. It is also the uniform bi-interpretability which allows us to exhibit asymptotic classes of finite simple groups.

Another notable contribution to this area is [20].

The question of whether the almost theory of a family of finite simple groups of a fixed Lie type and Lie rank is decidable was posed in [24]. Hrushovski already includes an affirmative answer as Theorem 1.7 of [13], and although we may see it in our context, there is no need for the full uniform bi-intepretability to deduce this result.

Inverse questions have been addressed:

What are the finite rank definable simple groups in pseudo-finite fields, in $ACFA$ or in theories $PSF_{(m,n,p)}$?

Hrushovski addresses the issue of definable simple groups in pseudo-finite fields in the more general setting of simple definable groups in a bounded PAC field F: in Theorem 9.5 of [15] he shows that they are Chevalley groups over Galois extensions of F.

Comments in older versions of that manuscript suggest that he was perfectly aware as early as 1991 that groups of type ${}^2B_2$ and ${}^2G_2$ were different. These comments do not seem to be in the final version. We show in Section 3.4 that such groups cannot be defined over a pure bounded PAC field. Hrushovski asserts the strong Theorem 1.8 in [13]: in $ACFA$ the finite rank definable simple groups are exactly the pseudo-finite simple groups of a fixed Lie rank and Lie type; as a theorem not depending on the classification of finite simple groups this seems magnificent.

What are the simple pseudo-finite groups?

John Wilson tackles this question in [30]. He obtains the result that every simple pseudo-finite group is elementarily equivalent to a Chevalley group over a pseudo-finite field. The work draws from results of Felgner and Point ([24]). He leaves the open question of whether every simple pseudo-finite group is, in fact, isomorphic to a Chevalley group over a pseudo-finite field. Our results on the uniform parameter bi-intepretations between groups and families of finite fields or finite difference fields mean the answer to this question is 'yes'.

1.4 Background concepts of the thesis

1.4.1 Concepts from classical algebraic geometry

The thesis takes a traditional view of algebraic geometry. Throughout, we work inside universal domains for algebra - saturated, algebraically closed fields. A wonderful reference for this viewpoint of algebraic geometry is [21]. Let us make precise a few of the key terms of which we make use. Suppose we work inside the universal domain $\tilde{K} \models ACF$; we will denote an arbitrary field by K. In this section and the next, variables (such as x) will denote singletons or, for ease of notation, tuples.

- $\langle\cdot\rangle$: if R is a ring and $J \subseteq R$, then we use the notation $\langle J\rangle$ for the ideal in R generated by the elements of J.

- *Algebraic sets:* An algebraic set $A \subset \tilde{K}^n$ is the solution set to a system of

polynomial equations

$$\{P_0(X_1, X_2, \ldots, X_n), P_1(X_1, X_2, \ldots, X_n), \ldots, P_m(X_1, X_2, \ldots, X_n)\}$$

where for each $0 \leq i \leq m$ we have $P_i \in \tilde{K}[X_1, \ldots, X_n]$ (see [21] pp.24).

- *Ideal of an algebraic set:* For an algebraic set $A \subset \tilde{K}^n$ we denote by $I(A)$ the ideal of polynomials in $\tilde{K}[X_1, \ldots, X_n]$ which vanish on A. (see [21] pp.24). Conversely, the algebraic set in the universal domain determined by an ideal I, we shall refer to as $V(I)$.

- *Affine Varieties:* Affine varieties are absolutely irreducible algebraic sets (see [21] pp.24).

- *Generic points:* We shall refer to a generic point x_0 of an algebraic set A over a small set B. We have:

$$x_0 \text{ generic in } A \text{ iff } \text{tr.deg}(x_0/B) = \max(\text{tr.deg}(x/\text{acl}(B)) : \ x \in A) \qquad (1.1)$$

(see [21] pp.28)

- *Fields of definition:* Let I be some ideal in $\tilde{K}[X_1, \ldots, X_n]$, and suppose that I has a $\tilde{K}$-basis of polynomials whose coefficients lie in a subfield K. Then K is said to be a field of definition for I. The concept extends to a field of definition for an algebraic set A, and furthermore, there exists a unique smallest field of definition for I (see [21] pp. 62).

- *Purely inseparable extensions and the inseparable degree:* Suppose that $F \subseteq E$ is an algebraic extension of characteristic p fields. An element $\alpha \in E$ is said to be purely inseparable over F if there exists an $n \geq 0$ such that $\alpha^{p^n} \in F$. Then if every element of E is purely inseparable over F we say that E is a purely inseparable extension of F. If E is a finite extension of F then the inseparable degree $[E : F]_{\text{ins}}$ is the maximum degree of a purely inseparable extension of F within E.

- *Morphisms of varieties:* These are introduced in chapters IV and V of [21], and we shall not delve into details here. However various properties and invariants of morphisms are important to us. Suppose that $f : V \mapsto W$ is a morphism of

varieties. Then f is a *quasi-finite* morphism of varieties if all the fibres of f are finite in cardinality. Suppose that the morphism is defined over the small subfield K. The morphism is *dominant* or *generically onto* if some $y \in W$ is generic over K, and there is $x \in V$ with $f(x) = y$. Suppose that f is both dominant and quasi-finite. In such a case, generic points are mapped to generic points, and we may suppose that $y \in W, x \in V$ are generic over K, and $f(x) = y$. Then $K(x)$ is a finite extension of $K(y)$. The degree $[K(x) : K(y)]$ is an invariant of the morphism and is called the *degree* of f. Similarly, the inseparable degree $[K(x) : K(y)]_{\text{ins}}$ is an invariant called the *inseparable degree* of f. See [21] pp.90 for details.

- *Correspondences, Rational Maps, Birational Maps:* As in [21] pp.100, a *correspondence* T between two varieties V and W will be a subvariety of the product $V \times W$. Suppose (x, y) is a generic point of T over a field of definition K, and that $K(y) \subseteq K(x)$. We then call T a *rational map* from V to W. If T has projections generically onto both V and W and if it is a rational map in both directions of degree 1 then we say it is a *birational map*. Now let x' be a point in V. If each coordinate y_j of y may be written $y_j = \frac{f(x)}{g(x)}$ where f and g are polynomials and $g(x') \neq 0$ then we say the rational map is *defined* at x', of *holomorphic* at x'. If T is birational, $(x', y') \in T$ and T is holomorphic both at x' and y' then we say it is *biholomorphic* at (x', y').

- *Varieties:* For us, a variety is a constructible set biholomorphic with an affine variety: suppose $T \subseteq V \times W$ is a birational, everywhere biholomorphic map. Suppose the projection of T in V is onto V. Then we say the image A of the projection of T in W is a variety.

An important example for us will be the following - which we call the *hyperbolisation trick*: say $W \subseteq \mathbb{A}^m$ is an affine variety defined by a prime ideal $I \subseteq \tilde{K}[X_1, \ldots, X_m]$. Let $f \in \tilde{K}[X_1, \ldots, X_m] \backslash I$. Consider $A = W \cap \{x \in \tilde{K}^m : f(x) \neq 0\}$. Now define $V \subseteq \mathbb{A}^{m+1}$ by the prime ideal in $\tilde{K}[X_1, \ldots, X_m]$ generated by I and the polynomial $fX_{m+1} - 1$. Consider the correspondence $T \subseteq V \times W$ written in coordinates $(x_1, \ldots, x_{m+1}, y_1, \ldots, y_m)$ and defined by

polynomials $x_i - y_i$ for $i = 1$ to m. Then T is a birational, everywhere biholomorphic map; its projection is onto V, and its image in W is A. So A is a variety. Since A is an open subset in the Zariski topology, we may refer to it as an open variety. Since it is birational, biholomorphic with an affine variety, we may also refer to it as an open affine variety.

- *Algebraic closures and relative algebraic closures:* In model theory we have the notion of the algebraic closure of a set. In the case of the theory of algebraically closed fields this closure is equivalent to the field-theoretic algebraic closure, and is denoted by $\mathrm{acl}_{\mathrm{alg}}(\cdot)$.

  Suppose we have a field K, and suppose $A \subseteq K$. Then we write $\mathrm{acl}_{\mathrm{alg}}(A, K)$ or equivalently $\mathrm{acl}_{\mathrm{alg}}{}^{K}(A)$ for the smallest field F such that $A \subseteq F \subseteq K$ and $\tilde{F} \cap K = F$, where $\tilde{F}$ is the algebraic closure of F. We call F the relative algebraic closure of A in K.

- *Radical of an ideal:* The radical of an ideal I in the ring A, denoted $\sqrt{I}$ can be seen in various ways. We shall define it as:

  $$\sqrt{I} = \{x \in A : \ \exists n \in \mathbb{N} \text{ s.t. } x^n \in I\}$$

  It can be shown that $\sqrt{I}$ is the intersection of all prime ideals containing I (see [2] proposition 1.8).

- $f^{p^{-n}}$: Let k_p be a field of characteristic p. Let $\bar{X} = X_1 \dots X_r$, and suppose $f(\bar{X}) \in k_p[\bar{X}]$. So suppose that $f = b_0 + b_1\bar{X}^{m_1} + \ldots + b_n\bar{X}^{m_n}$, where each $\bar{X}^{m_i} = X_1^{a_{1,i}} \dots X_r^{a_{r,i}}$ for a collection of positive integers $\{a_{t,i} \in \mathbb{N} : \ 1 \leq t \leq r, \ 1 \leq i \leq n\}$, and $b_i \in k_p$ for $1 \leq i \leq n$. By $f^{p^{-n}}$ we mean $f^{p^{-n}} = b_0^{p^{-n}} + b_1^{p^{-n}}\bar{X}^{m_1} + \ldots + b_n^{p^{-n}}\bar{X}^{m_n}$.

- *Total degree:* Let $X_1^{a_1}X_2^{a_2} \dots X_n^{a_n}$ $(a_i \in \mathbb{N})$ be a monomial. Its total degree is $\sum_{i=1}^{n} a_i$. If $P(X_1, X_2, \ldots, X_n)$ is a polynomial, its total degree is the maximum of the total degrees of its constituent monomials.

- *Correspondences:* Let $V(x)$ and $A(z)$ be algebraic sets. Then a correspondence between V and A is an algebraic set $T(xz)$ such that $T \subseteq V \times A$. In such a

situation, there are two canonical projections: π_1 is the projection from T to x, and π_2 is the projection from T to z.

- *Locus:* Let $x = (x_1, \ldots, x_n)$ be a point in $\tilde{K}^n$ where $\tilde{K}$ is the universal domain, let $B \subseteq \tilde{K}$, and let p be the prime ideal of functions over $\mathrm{acl}(B)$ which vanish at x.Then $V(p)$ is the locus of x over B.

- *Conjugate varieties:* Suppose σ is an automorphism of the field K, $x = (x_1, \ldots, x_l)$, and $A(x)$ is an algebraic set defined by polynomials $\{f_i(x, k_1, \ldots, k_n) : \ 1 \leq i \leq m\}$, where the coefficients $k_1, \ldots, k_n \in K$. Then $\sigma(A)$ may be defined as (i) $\{(\sigma(x_1), \ldots, \sigma(x_n)) : \ (x_1, \ldots, x_n) \in A\}$ or (ii) the algebraic set defined by the polynomials $\{f_i(x, \sigma(k_1), \ldots, \sigma(k_n)) : \ 1 \leq i \leq m\}$; the definitions are equivalent. We refer to $\sigma(A)$ as a conjugate of A.

- *Algebraic dimension:* Suppose that $\tilde{K}$ is uncountably saturated. Let X be a set definable over the small field $B \subseteq \tilde{K}$. Then the algebraic dimension of X is the maximal transcendence degree of a point in $X(\tilde{K})$ over B. We write the algebraic dimension of X as $\dim_{\mathrm{alg}}(X)$.

1.4.2 Concepts from difference algebra

Here we describe the basics of difference algebra and the model theory of difference fields. We want to present enough material for the reader to understand the background statements of chapter 2. The basic text on difference algebra is [11]. There is also a very useful introductory page in [8], and what we now present is very similar to that, if not in some places identical.

- *Difference rings:* A difference ring for us is a ring A together with an injective map of rings $\sigma : A \mapsto A$. Unless otherwise stated, all the maps we consider are onto - they are automorphisms of A.

- $\mathcal{L}_{\mathrm{diff}}$: In terms of model theory, the language we consider is the language $\mathcal{L}_{\mathrm{diff}}$ of difference rings, which is exactly the language of rings augmented by a unary function symbol σ. In this language, it is easy to write axioms stating that σ is an automorphism.

- *Difference polynomial rings:* For (K, σ) a difference field and $X = (X_1, \ldots, X_n)$, we define the difference polynomial ring $K\langle X \rangle$ to be the ring

$$K[X_1, \ldots, X_n, \sigma(X_1), \ldots, \sigma(X_n), \sigma^2(X_1), \ldots]$$

. The isomorphism σ extends to this polynomial ring in the obvious way. Notice that even if σ is an automorphism on K, this extension clearly is not an automorphism.

- *σ-ideals*: For a difference ring (A, σ) there is a natural notion of a σ-ideal. It is an ideal closed under the action of σ. A reflexive σ-ideal is a σ-ideal $\mathcal{I}_\sigma$ where if $\sigma(a) \in \mathcal{I}_\sigma$ then $a \in \mathcal{I}_\sigma$.

- *Universal domains for difference algebra:* These exist and are first-order. They are captured by completions of the theory $ACFA$. The papers [8] and [9] are devoted to the study of that theory. Here is the axiomatisation of $ACFA$ according to [8]:

  Let $ACFA$ be the theory axiomatised by the scheme of axioms expressing the following properties of the $\mathcal{L}$-structure (K, σ):

  (i) σ is an automorphism of K,

  (ii) K is an algebraically closed field,

  (iii) For every variety U, and variety $V \subseteq U \times \sigma(U)$ projecting generically onto U and $\sigma(U)$, and every algebraic set W properly contained in V, there is an $a \in U(K)$ such that $(a, \sigma(a)) \in V \backslash W$ (by $U(K)$ we denote the K-rational points of U).

- *σ-polynomials and σ-closed sets*: Let (M, σ) be a difference ring. Let x be a tuple of variables. A σ-polynomial $F(x)$ is a polynomial in variables x and its σ-iterates, with coefficients in M. A σ-closed set in M is the solution set in some cartesian power M^n of a system of σ-polynomials. For example, if x is a single variable then the σ-closed set defined by the σ-polynomial $\sigma(x) = x$ is the fixed set in M of the operator σ.

- *σ-degree*: Let $K \subseteq L$ be two difference fields, and let a be a tuple from L; we denote by $K(a)_\sigma$ the field $K(\sigma^k(a))_{k \in \mathbb{Z}}$ and we say that is is generated by a; a

subextension of a difference field finitely generated over K is itself finitely generated. Assume that $L = K(a)_\sigma$; we define $\deg_\sigma(L/K)$, or sometimes $\deg_\sigma(a/K)$, to be the transcendence degree of L over K. In general, if A is a set of parameters, let A_σ be the difference field generated by A. For an $\mathcal{L}_{\text{diff}}$-parameter definable set $\psi(x)$ we write $\deg_\sigma(\psi(x)) \leq n$ to express that if A is a set containing the parameters for ψ and $\psi(a)$ holds, then $\deg_\sigma(a/A_\sigma) \leq n$.

- *$acl_\sigma(A)$:* In a difference field (K, σ), suppose $A \subseteq K$. Then we write $\text{acl}_\sigma(A)$ for the smallest difference subfield of (K, σ) which contains A and is algebraically closed inside K. Thus, $\text{acl}_\sigma(A) = \text{acl}_{\text{alg}}(\cup_{i\in\mathbb{Z}}\sigma^i(A))$.

Chapter 2

ACFA and Finite Dimensional Measurable Sets

2.1 Chapter Introduction

In this chapter we derive a definable measure for families of sets of finite σ-degree inside a big model of $ACFA$. The notion of definability we obtain is made precise in the statement of the main theorem of the chapter: Theorem 2.1.1, and that result will be sufficient for the applications in later chapters. This chapter is concerned with the theory $ACFA$. Background for that theory is given in Section 1.4.2.

2.1.1 Notation and Key Definitions

In what follows x and y denote tuples unless specifically stated otherwise. Frob will denote a frobenius automorphism.
First, suppose that $\mathcal{L}$ is a language, where $\mathcal{L}$ will either be $\mathcal{L}_{\text{diff}}$, the language of difference rings, or $\mathcal{L}_{\text{rings}}$, the language of rings. Suppose K is the underlying ring in an $\mathcal{L}$-structure.

By $\theta(x,y)(K)$ we denote an $\mathcal{L}$-definable set $\theta(x,y)$ whose intended meaning is a family of sets parameterised by tuples $y \in K$. By a *member of the family* $\theta(x,y)$ we shall mean a set $\theta(x,y_0)$ in variable x with a parameter y_0. The parameter set of $\theta(x,y)(K)$ is defined as $\{y \in K : \exists x(x \in K \wedge \theta(x,y))\}$. Let us denote the parameter set of $\theta(x,y)(K)$ by $P(\theta)(K)$. Since $\theta(x,y)$ is defined without parameters, we can make statements about the family of sets $\theta(x,y)$ over a class $\mathcal{C}$ of $\mathcal{L}$-structures. We may refer to the parameter sets in arbitrary members of $\mathcal{C}$ via notation $P(\theta)(y)$ or just $P(\theta)$.

A sub-family of $\theta(x,y)(K)$ is given as $\theta(x,y) \wedge y \in Q$ where $Q \subseteq P(\theta)(K)$. A *parameter definable sub-family* of $\theta(x,y)(K)$ is given as $\theta(x,y) \wedge Q(y)$ where $Q(K) \subseteq P(\theta)(K)$ and $Q(y)$ is a formula in the language $\mathcal{L}(K)$. If the formulae involved are without parameters we use the term $\emptyset$*-definable sub-family.*

A stratification of $\theta(x,y)(K)$ is a partition of $\theta(x,y)(K)$ into disjoint sub-families. Formally, there is an index J and a set of sub-families $\{\theta(x,y) \wedge Q_j(y) : j \in J\}$, where $P(\theta)(K) = \coprod_{j \in J} Q_j(K)$. The convention will be to say $\theta(x,y)(K)$ *is stratified into a set* $S = \{Q_j(K) : j \in J\}$. If the $Q_j(K)$ are parameter definable sets then we say the

stratification is *parameter definable*, or is a stratification by *parameter definable sub-families*. As before, if the formulae involved are without parameters, we may instead use the terms $\emptyset$-*definable* and stratification by $\emptyset$-*definable sub-families*.

If $\theta(x, y)$ is $\emptyset$-definable, and if $Q(K) \subseteq P(\theta)(K)$ for any $\mathcal{L}$-structure K in some class of $\mathcal{L}$-structures $\mathcal{C}$, we say Q is a *sub-family* for the class $\mathcal{C}$. Similarly, if $\{Q_j : j \in J\}$ are such that for any $\mathcal{L}$-structure $K \in \mathcal{C}$, $P(\theta)(K) = \coprod_{j \in J} Q_j(K)$, then we say that $\theta(x, y)$ is *stratified for the class* $\mathcal{C}$ by the Q_j,

If we are in the context where the sets/families are given by formulae, we may omit the explicit reference to the structure K. Suppose $\theta(x, y)$ is definable without parameters and that $Q(y)$ is an $\mathcal{L}$-formula representing a sub-family of $\theta(x, y)$ for some class of $\mathcal{L}$-structures $\mathcal{C}$; we shall say $Q(y)$ is a *uniformly definable sub-family* for the class $\mathcal{C}$. Similarly, if $\{Q_j(y) : j \in J\}$ are formulas without parameters such that for any $\mathcal{L}$-structure $K \in \mathcal{C}$, $P(\theta)(K) = \coprod_{j \in J} Q_j(K)$, then we say that $\theta(x, y)$ is *uniformly, definably stratified for the class* $\mathcal{C}$ by the Q_j, or that the stratification is uniformly definable for $\mathcal{C}$. If the class $\mathcal{C}$ is understood, we may omit explicit reference to it.

Let $\theta(x, y)(K)$ be a family of sets in K. Let $P_{I,\mathcal{G}}$ be a set and let I be a function $I : \theta(x, y)(K) \to P_{I,\mathcal{G}}$. For instance, I might be a function mapping a family of algebraic sets to their algebraic dimension. We may stratify $\theta(x, y)(K)$ into its I-fibres $\{I^{-1}(j) : j \in P_{I,\mathcal{G}}\}$. We then say I stratifies the family $\theta(x, y)(K)$. In our example, this would be stratifying $\theta(x, y)(K)$ into sub-families of constant dimension. If the collection of fibres may be taken to be $\{Q_j(K) : j \in P_{I,\mathcal{G}}\}$ for a collection of definable sets we shall say that I is parameter definable in $\theta(x, y)$ for K.

Similarly, if $\theta(x, y)$ is a family and I is a function, both across $\mathcal{C}$, then we may also stratify $\theta(x, y)$ into its I-fibres across $\mathcal{C}$. If the fibres may be taken to be uniformly definable sub-families $\{Q_j(y) : j \in P_{I,\mathcal{G}}\}$ across $\mathcal{C}$, we shall say I is uniformly definable in $\theta(x, y)$ across $\mathcal{C}$.

Below, a definable family of σ-closed sets is a family $\theta(x, y) \wedge P(\theta)(y)$ where $\theta(x, y)$

defines a σ-closed set, but where there is no such restriction on the form of the parameter set formula $P(\theta)(y)$. Similarly, a quantifier-free family $\theta(x,y) \wedge\ P(\theta)(y)$ has $\theta(x,y)$ quantifier-free, but there is no restriction on the form of $P(\theta)(y)$.

Suppose that $\theta(x,y)$ is a family of sets in the language of difference rings across a class $\mathcal{C}$ of models . We define $\theta_n(y) = \{y : \deg_\sigma(\theta(x,y)) = n\}$. By $\theta_n(x,y) = \theta(x,y) \wedge \theta_n(y)$ we shall mean, in any $\aleph_0$-saturated model $(K,\sigma) \models ACFA$, the sub-family of $\theta(x,y)(K)$ consisting of those members of σ-degree n. If $\theta(x,y)$ is an $\emptyset$-definable family, then the subfamily $\theta_n(x,y)$ is also $\emptyset$-definable, as we shall see in subsection 2.1.3.

2.1.2 Statement of main theorem

THEOREM 2.1.1 *Let $\theta(x,y)$ be a family of sets definable in the language of difference rings. Then $\theta_n(x,y)$ can be partitioned into finitely many $\mathcal{L}_{\text{diff}}$-$\emptyset$-definable subfamilies $\theta_{n,\mu_i}(x,y)$, ($\mu_i \in\ \mathbb{R}^+$) such that the following holds: there is a constant $C \in \mathbb{R}^+$ such that for all pairs of the form ($\tilde{\mathbb{F}}_p$, Frob^k) but finitely many, for any $y_0 \in \tilde{\mathbb{F}}_p$*

$$P(\theta_{n,\mu_i})(y_0)\ \Rightarrow\ \mid\ \mid \theta(\tilde{\mathbb{F}}_p, y_0) \mid\ -\ \mu_i p^{kn}\ \mid \leq C p^{k(n-\frac{1}{2})}$$

Here, we allow p to run over all primes and k to run over the natural numbers.

This theorem will allow us to assign a measure, in the sense of [23], to the finite σ-degree sets of $ACFA$. The situation is analogous to the situation in finite fields. In that case, the Lang-Weil estimates were seen in [10] to generalise to numerical estimates for all first-order definable sets in finite fields. In this chapter we follow the same pattern.

2.1.3 Key background results

In the statement of 2.1.1 we are already implicitly assuming definability of the family $\theta_n(x,y)$. Let us justify this: in Section 7 of [8] it is written: 'let $\psi(x,y)$ be a formula (in $\mathcal{L}_{\text{diff}}$), n a positive integer; then the set of elements b such that $\deg_\sigma(x,b) \geq n$ is definable'. We will not produce a proof here, but perhaps more interestingly, say that the proof would be virtually identical to the proofs of definability of dimension for geometric structures in [16], but using the analogue to algebraic boundedness for $ACFA$ described in (1.8) of [8].

I now quote a version of Hrushovski's correspondence estimates from [13] which we shall use. This (Theorem 2.1.2) was communicated by Hrushovski personally, although it may be deduced from, and is essentially Theorem 1.1 of [13].

We need some notation. Suppose $\tilde{K}$ is an algebraically closed field of characteristic p. Let $n, r \in \mathbb{N}$ and $q = p^r$. Let $V(x)$ be an affine variety over $\tilde{K}$ and let $I(V)$ be the ideal of V in $\tilde{K}[x]$. Suppose $I(V)$ is generated by a set $S = \{f_l(x, y) : \ 1 \leq l \leq n\}$ of polynomials, for some parameters $y \in \tilde{K}$. Then we let the variety $V^q(z)$ be the variety defined by the set of polynomials $R = \{f_l(z, y^q) : \ 1 \leq l \leq n\}$. Suppose $W(xz)$ is a variety and $W(xz) \subseteq V(x) \times V^q(z)$. Then we define $\Delta_q(W)(\tilde{K}) = \{xz : \ xz \in W(\tilde{K}) \wedge z = x^q\}$. We are considering the x and z as tuples. Suppose $x = (x_1, x_2, \ldots, x_m)$ and $z = (z_1, z_2, \ldots, z_m)$. Then by $z = x^q$ we mean $z_i = x_i^q$ for each $1 \leq i \leq m$. Details and references about various aspects of classical algebraic geometry that arise in the statement of Theorem 2.1.2 and what follows are summarised in the Section 1.4.1. Then the following is the statement of Hrushovski's correspondence estimates of which we make use:

THEOREM 2.1.2 *Let $\tilde{K}$ be an algebraically closed field of characteristic p. Let $r \in \mathbb{N}$ and $q = p^r$. Let $V(x)$ be an affine variety over $\tilde{K}$, and let $W(xz) \subseteq V(x) \times V^q(z)$ be an irreducible subvariety. Assume $dim(W) = dim(V) = d$, the projection $\pi_1 : \ W \mapsto V$ is dominant of degree δ and the projection $\pi_2 : \ W \mapsto V^q$ is quasi-finite of purely inseparable degree δ'.*

There is a constant C depending on the total degree of W (but not on q or the parameters from $\tilde{K}$) such that

$$\left||\Delta_q(W)(\tilde{K})| - \frac{\delta}{\delta'} q^d\right| \leq C q^{d-1/2}.$$

Notice that there is no specification that $W(xz)$ is a closed subvariety of $V(x) \times V^q(z)$; this is intentional since it does not need to be. In fact, we shall apply 2.1.2 in situations where W is not closed. In particular, in our main application at the end of the chapter (Theorem 2.3.14) W will be an affine open variety of the form $A \backslash \text{Zeroes}(f)$ where A is a closed affine variety in $V \times V^q$ and f is a single polynomial $f = f(x, z)$.

The relation between Theorem 2.1.1 and 2.1.2 is analogous to the relation of the generalised estimates in [10] to the Lang-Weil estimates.

In the same way that the generalised estimates of [10] lead to a non-standard counting measure on pseudo-finite fields, we shall also obtain a non-standard counting measure on all finite σ-degree sets in models of $ACFA$. We obtain the measure by using another main theorem in [13]:

THEOREM 2.1.3 *Let* $\mathcal{D} := \{(\tilde{\mathbb{F}}_p, \mathrm{Frob}^r) : r \in \mathbb{N},\ p \text{ a prime}\}$. *Every model of* $ACFA$ *is elementarily equivalent to a non-principal ultraproduct of members of* $\mathcal{D}$.

The remainder of the chapter is divided into three sections that lead to a proof of Theorem 2.1.1.

1. In section 2.2 we gather preliminary algebraic and algebraic-geometric results.
2. In section 2.3 we exhibit definable cardinality estimates for σ-closed sets of finite σ-degree. The techniques are analogous to those used in [10] to obtain cardinality estimates for algebraic sets.
3. In section 2.4, we complete the proof of Theorem 2.1.1, again by applying techniques analogous to those used in [10].

2.2 Stratification of families of Constructible Sets

In this section we work in the language of rings and in the theory of algebraically closed fields. Algebraically closed fields will be denoted by tildas: $\tilde{K}$ is algebraically closed. If we wish to specify that the characteristic of $\tilde{K}$ is some prime p, we shall refer to the field as $\tilde{K}_p$. In all instances, the prime field will be referred to as F.

DEFINITION 2.2.1 Let $\mathcal{C}$ be a class of $\mathcal{L}$-structures, and let K be an $\mathcal{L}$-structure. Let $S_1 = \{Q_{1j} : j \in J\}$ and $S_2 = \{Q_{2i} : i \in I\}$ be either (i) stratifications of $\theta(x,y)(K)$, or (ii) stratifications of $\theta(x,y)$ over $\mathcal{C}$. Then $S_3 = \{Q_{3r} : r \in R\}$ is a *boolean combination of* S_1 *and* S_2, if either we are in case (i) and it is a stratification of $\theta(x,y)(K)$ and each $Q_{3r}(K)$ is a boolean combination of elements of S_1 and S_2, or we

are in case (ii) and it is a stratification of $\theta(x,y)$ over $\mathcal{C}$ and uniformly across $\mathcal{C}$, each Q_{3r} is a boolean combination of elements of S_1 and S_2.

The following is obvious, but gives the flavour of what we shall do:

LEMMA 2.2.2 *Let $\mathcal{C}$ be a class of fields.*

1. *Any boolean combination of parameter definable stratifications of $\theta(x,y)(K)$ is a parameter definable stratification of $\theta(x,y)(K)$. Similarly, any boolean combination of uniformly definable stratifications of $\theta(x,y)$ over $\mathcal{C}$ is a uniformly definable stratification of $\theta(x,y)$ over $\mathcal{C}$.*

2. *A parameter definable sub-family $(\theta(x,y) \wedge Q(y))(K)$ may be seen as one of two stratifying sets in a parameter definable stratification of $\theta(x,y)(K)$ by setting the stratification to be $\{\theta(x,y) \wedge Q(y) \ ; \ \theta(x,y) \wedge \neg Q(y)\}$. Similarly, a uniformly definable sub-family $\theta(x,y) \wedge Q(y)$ for $\mathcal{C}$ may be seen as one of two stratifying sets in a uniformly definable stratification of $\theta(x,y)$ for $\mathcal{C}$, again by setting the stratification to be $\{\theta(x,y) \wedge Q(y) \ ; \ \theta(x,y) \wedge \neg Q(y)\}$.*

Similarly, we shall need some basic facts about stratifications under projections.

FACT 2.2.3 Let $\mathcal{C}$ be a class of algebraically closed fields. Let $\psi(x_1,w)$ and $\theta(x_2,y)$ be two $\emptyset$-definable families of sets in algebraically closed fields. Let $f : P(\psi)(w) \twoheadrightarrow P(\theta)(y)$ be a $\emptyset$-definable map of their parameter sets. Suppose that $\theta(x_2,y)$ is uniformly stratified over algebraically closed fields by $S_1 = \{Q_j(y) : j \in J\}$. Then $\psi(x_1,w)$ is uniformly stratified over algebraically closed fields by $S_2 = \{f^{-1}(Q_j(y)) : j \in J\}$.

This has two immediate, important applications:

1. Suppose that we have $\psi(x,yz)$ and $\theta(x,y)$ is the y-projection of ψ. By this we mean:

$$\theta(x,y) =_{\text{def}} \{(x,y) : \exists z(\psi(x,yz))\} \tag{2.1}$$

   Thus any stratification of $\theta(x,y)$ has a pullback to a stratification of $\psi(x,yz)$.

2. Suppose that f is 1-to-1, that $x_1 = x_2 = x$, and f has the property:

$$ACF \models \forall wyx(f(w) = y \ \Rightarrow \ \theta(x,y) \Leftrightarrow \psi(x,w)) \tag{2.2}$$

So as sets, the f-pre-image of any $y \in P(\theta(y))$ parameterises the identical family member to the one parameterised by y itself. In this situation, $\psi(x, w)$ and $\theta(x, y)$ are the identical *family* of sets, just parameterised differently. We may apply Fact 2.2.3 to f or f^{-1}. This is like a rearrangement: any (parameter definable/ uniformly definable over algebraically closed fields) stratifying property for the family of sets in terms of $\psi(x, w)$ can be rearranged into a (parameter definable/ uniformly definable over algebraically closed fields) stratifying property in terms of $\theta(x, y)$, and vice-versa. We shall use this fact when f is a projection (see Lemmas 2.2.12 and 2.2.11).

Now suppose that f has fibres of size at most $m < \infty$. This time, suppose that $\psi(x, w)$ is uniformly stratified over algebraically closed fields by $S = \{Q_j(w) : j \in J\}$. Then we may uniformly stratify $\theta(x, y)$ according to tuples of natural numbers $(e_j : j \in J)$ where if $y_0 \in P(\theta)(\tilde{K})$ is associated to the tuple $(e_j : j \in J)$, it signifies that in the f-fibre of y_0, there are exactly e_j elements stratified into the subfamily Q_j under S for each $j \in J$.

The Family Stratification Lemma

LEMMA 2.2.4 *1. Suppose that $\tilde{K}$ is an $\aleph_0$-saturated model of ACF and that $\theta(x, y)(\tilde{K})$ is a family of constructible sets in $\tilde{K}^n$. Suppose that as a definable set $\theta(x, y)$ is defined with a finite set of parameters $B \subset \tilde{K}$. Suppose that $\theta(x, y)(\tilde{K})$ is stratified into a set of non-empty sub-families $S = \{Q_j(\tilde{K}) : j \in J\}$. Suppose that for any $y_0 \in P(\theta)(\tilde{K})$ there is a B-definable set Y_{y_0} such that (i) $y_0 \in Y_{y_0}$ and (ii) there is some $j \in J$ with $Y_{y_0} \subseteq Q_j(\tilde{K})$. Then S is a parameter definable stratification of $\theta(x, y)(\tilde{K})$. In fact, each $Q_j(\tilde{K})$ is a finite union of sets of the form Y_{y_0}. Also, J is a finite set.*

2. Now suppose that $\theta(x, y)$ is an $\emptyset$-definable family. Let P_I be a set and let I be a function from all members of $\theta(x, y)$ over all algebraically closed fields to P_I. Suppose that for any $\aleph_0$-saturated model $\tilde{K} \models ACF$ and $y_0 \in P(\theta)(\tilde{K})$, there is an $\emptyset$-definable set Y_{y_0} such that (i) $y_0 \in Y_{y_0}$ and (ii) I is a single constant value over all algebraically closed fields $\tilde{L}$ in the sub-family $(\theta(x, y) \wedge Y_{y_0}(y))(\tilde{L})$. Then I is uniformly definable in $\theta(x, y)$. The number of attainable possibilities for I is

finite.

PROOF 1. Observe that $P(\theta)(\tilde{K}) = \cup_{y_0 \in P(\theta))(\tilde{K})} Y_{y_0}$, where all the Y_{y_0} are B-definable. Since B is finite and $\tilde{K}$ is $\aleph_0$-saturated, there are elements $y_l \in P(\theta)(\tilde{K})$ and a collection $R = \{Y_{y_l} : 1 \leq l \leq s\}$ such that $P(\theta)(\tilde{K}) = \cup_{l=1}^{s} Y_{y_l}$. Then each Q_j is a union of elements of R. By compactness, it follows that J is finite.

2. Pick $\tilde{K}_0 \models ACF_0$ where $\tilde{K}_0$ is $\aleph_0$-saturated. By part 1 there is a finite set J and a set of $\emptyset$-definable sets $S = \{Q_j(y) : j \in J\}$ such that the $Q_j(\tilde{K}_0)$ witness the stratification of $P(\theta(x,y))(\tilde{K})$ by the fibres of I. Furthermore, by the second statement in Part 1, each $Q_j(\tilde{K}_0)$ may be written as a union of $\emptyset$-definable sets of the form $Y_{y_0}(\tilde{K}_0)$. By compactness, there is a prime q and natural numbers n_j such that for all primes $p > q$ and algebraically closed fields $\tilde{K}_p$, $P(\theta)(\tilde{K}_p) = \coprod_{j \in J} Q_j(\tilde{K}_p)$ and each $Q_j(\tilde{K}_p) = \cup_{l=1}^{n_j} Y_{y_{lj}}(\tilde{K}_p)$. By the hypothesis of part 2, I is constant over all fields $\tilde{K}_p$ on $Y_{y_{lj}}(\tilde{K}_p)$. Since in characteristic 0, for each $j \in J$ we have that I is constant on each of the sets Y_{lj} for $1 \leq l \leq n_j$, it follows by the assumptions that in any algebraically closed field $\tilde{L}$ that I is constant on $Q_j(\tilde{L})$. Thus, I is definably stratified for the class of all algebraically closed fields of characteristic 0 or characteristic $p > q$. Now we may repeat this procedure for each characteristic p with $p \leq q$. Since all the sets of the form J are finite, it follows that the number of attainable possibilities for I is finite. □

In the rest of this section we shall use Lemma 2.2.4 (Part 2) to demonstrate that various properties of algebraic and constructible sets are uniformly definable. First we begin with a simple, illustrative example.

EXAMPLE 2.2.5 Consider the family of algebraic sets $A(x,y)$ given by $x^2 - y = 0$, where x and y are single variables. We define I to be the cardinality $I(y) = |A(x,y)|$, and we shall apply 2.2.4 (Part 2) to show that I is uniformly definable over all algebraically closed fields.

Suppose $\text{char}(\tilde{K}) \neq 2$ and $y_0 \in \tilde{K}^{\times}$. Then there are two square roots of y_0 which we denote by x_0 and $-x_0$. We may write the $\mathcal{L}_{\text{rings}}(\tilde{K})$ sentence:

$$\theta_0(x_0, -x_0, y_0): \quad y_0 = x_0^2 \ \wedge \ y_0 = (-x_0)^2 \ \wedge \ \neg(x_0 = -x_0) \tag{2.3}$$

The sentence $\theta_0(x_0, -x_0, y_0)$ is equivalent to $I(y_0) = 2$, but uses parameters $x_0, \ -x_0 \in \mathrm{acl}_{\mathrm{alg}}(F(y_0))$. Our goal is to code $I(y_0)$ without parameters. But notice that the following formula, which is satisfied by y_0, asserts the existence of parameters such as x_0 and $-x_0$, and is sufficient to code $I(y_0)$:

$$\theta_1(y): \quad \exists xw\big(y = x^2 \ \wedge \ y = w^2 \ \wedge \ \neg(x = w)\big) \tag{2.4}$$

Importantly, $\theta_1(y)$ only uses the variable y. But the fact that $\theta_1(y_0)$ holds is still equivalent to $I(y_0) = 2$. So we may set Y_{y_0} as

$$Y_{y_0}(y) := \theta_1(y) \tag{2.5}$$

Inspecting $\theta_1(y)$, we see that it is equivalent to $I(y) = 2$. Now pick an algebraically closed field $\tilde{K}_2$, of characteristic 2, and let $y_1 \in \tilde{K}_2$. Then y_1 has a unique square root. Let $x_1 = \sqrt{y_1}$. In this case we may write the $\mathcal{L}_{\mathrm{rings}}(\tilde{K})$ sentence $\theta_2(x_1, y_1)$: $x_1^2 = y_1 \ \wedge \ (\forall w)(w^2 = y_1 \ \Rightarrow \ w = x_1)$. Again, θ_2 uses the parameter $x_1 \in \tilde{K}_2$. However we may obtain a formula $\theta_3(y)$, solely in parameter y, that asserts the existence of x_1; this is in the same way as $\theta_1(y)$ was obtained from $\theta_0(y_0)$. We obtain $Y_{y_1}(y)$: $\exists x\big(x^2 = y \ \wedge \ (\forall w)(w^2 = y \ \Rightarrow \ w = x)\big)$. The formula Y_{y_1} is seen to be equivalent to $I(y) = 1$. The reader can check that the formula we have obtained is just the statement 'characteristic=2 or $y = 0$' in disguise.

REMARK 2.2.6 This example is typical of the method we shall use to demonstrate that various properties of a family of algebraic sets $A(x, y)$ are uniformly definable. We aim to apply 2.2.4 (Part 2), and thus to pick some $\tilde{K}$, $y_0 \in P(A)(\tilde{K})$ and suppose $I(y_0) = m$. With some parameters $a \in \tilde{K}$, we shall find an $\mathcal{L}_{\mathrm{rings}}(a, y_0)$ sentence $\theta_1(y_0, a)$ which implies and is implied by the statement $I(y_0) = m$. Then, in the proofs, we shall leave it to the reader to observe that there is another formula $\theta(y)$ which y_0 satisfies and also implies and is implied by the statement $I(y) = m$: it is obtained from $\theta_1(y_0, a)$ by asserting the existence of the parameters a, but not referring to a specifically, and by substituting the variable y for the parameter y_0. Then we shall set $Y_{y_0}(y) = \theta(y)$.

To use Lemma 2.2.4 we shall need the following facts from [28]; they are also reported in the identical fashion that they are reported here (but in French), in [6]:

FACT 2.2.7 . In this statement, x is a tuple of indeterminates, and by $|x|$ we mean the size of the tuple x. These statements make use of various notions from algebra and algebraic geometry, such as the notion of the radical of an ideal ($\sqrt{\cdot}$). For relevant definitions see 1.4.1.

1. There is a constant $A(n, e)$ such that for all fields K and polynomials $f_1(x), \ldots, f_n(x), g(x) \in K[x]$ of total degree $\leq e$ and where $|x| \leq n$, if $g(x) \in \langle f_1(x), \ldots, f_n(x)\rangle$ then $g(x) = f_1(x)h_1(x) + \ldots + f_n(x)h_n(x)$ for polynomials $h_1(x), \ldots, h_n(x) \in K[x]$ of degree $\leq A(n, e)$.

2. There is a constant $B(n, e)$ such that for all fields K, if $|x| \leq n$ and the ideal I of $K[x]$ is generated by polynomials of degree $\leq e$, then if I is not prime, then there exist polynomials $g(x), h(x)$ of degree $\leq B(n, e)$ such that $g(x), h(x) \notin I$ and $g(x)h(x) \in I$.

3. There is a constant $C = C(n, e)$ such that for all fields K, if $|x| \leq n$, and the ideal I in $K[x]$ is generated by polynomials of total degree $\leq$ e, if for some $g(x) \in K[x]$, $g(x) \in \sqrt{I}$, then $g(x)^C \in I$.

4. There is a constant $D = D(n, e)$ such that for all fields K, if $|x| \leq n$ and the ideal $I \subseteq K[x]$ is generated by polynomials of total degree $\leq e$, there are at most D minimal prime ideals containing I, and each is generated by polynomials of degree $\leq D$.

We now demonstrate that various properties of algebraic sets are uniformly definable, making use of Lemma 2.2.4: for the first application of Lemma 2.2.4 let us briefly mention the definable multiplicity property (DMP) for strongly minimal sets. This concept was introduced in [14], and it is defined thus:

DEFINITION 2.2.8 If T is a strongly minimal theory then it has the *definable multiplicity property* (DMP) if for all natural k, m and $\psi(\bar{x}, \bar{b})$ of rank k, multiplicity m, there exists a formula $\theta \in \mathrm{tp}(\bar{b})$ such that for all $\bar{b}' \models \theta$, $\mathrm{MR}(\psi(\bar{x}, \bar{b}')) = k$ and $\mathrm{mult}(\psi(\bar{x}, \bar{b}')) = m$.

REMARK 2.2.9 In Definition 2.2.8 suppose $\bar{b}' \in M'$ where $M' \models T$. Then the multiplicity mult in Definition 2.2.8 may be taken to refer to the number of type completions over M' of the formula $\psi(\bar{x}, \bar{b}')$ of maximal Morley rank. It is a fact (see [14]) that any completion of the theory ACF of algebraically closed fields has the DMP. Then, applying Lemma 2.2.4 to the definition of the DMP, we see that the multiplicity mult is uniformly definable over algebraically closed fields.

LEMMA 2.2.10 *Let $V(x, y)$ be a 0-definable family of algebraic sets given by a set of polynomials $\{f_j(x, y) : j \in J\}$. Let $V(z, v)$ be the same family in variables z and parameters v: so $V(z, v)$ is given by $\{f_j(z, v) : j \in J\}$. Let $A(xz, t)$ be a third 0-definable family of algebraic sets given by polynomials $\{g_l(xz, t) : l \in L\}$. Suppose that t is parsed as $t = syv$. Then we have the following:*

1. *The sub-family of irreducible members of $V(x, y)$ is uniformly definable over algebraically closed fields.*

2. *Algebraic dimension is uniformly definable in $V(x, y)$ over algebraically closed fields.*

3. *Let π_x be the projection from $A(xz, t)$ to x. Now assume that the family $A(xz, t)$ is such that for any $\tilde{K}$ and $t_0 \in P(A)(\tilde{K})$, $\pi_x(A(xz, t_0)) \subseteq V(x, y_0)$, where $t_0 = s_0 y_0 v_0$. Then the sub-family of $A(xz, t)$ where π_x is onto $V(x, y)$ is uniformly definable over algebraically closed fields. The sub-family where π_x is of everywhere finite fibre is also uniformly definable over algebraically closed fields. Similarly, if $A(xz, t)$ and $V(x, y)$ are families of irreducible varieties, then the sub-families of $A(xz, t)$ where π_x is generically onto, or of generically finite fibre, are both uniformly definable over algebraically closed fields.*

PROOF We make use of 2.2.7:

1. We must show that the set $S := \{y : \ y \in P(V) \ \wedge \ V(x, y) \text{ is irreducible}\}$ is uniformly definable across all algebraically closed fields. For $y_0 \in \tilde{K}$ we write $\langle\{f_j(x, y_0) : j \in J\}\rangle$ for the ideal generated by the $f_j(x, y_0)$ in $\tilde{K}[x]$. Then we may also write $S = \{y : \ y \in P(V) \ \wedge \ \sqrt{\langle\{f_j(x, y) : j \in J\}\rangle} \text{ is prime}\}$. Now, suppose $y_0 \in \tilde{K}$ and we consider the ideal $I_{y_0} = \langle\{f_j(x, y_0) : j \in J\}\rangle$. By 2.2.7 (4), $\sqrt{I_{y_0}}$ is generated by polynomials of total degree less than or equal to some

$e \in \mathbb{N}$ which is independent of the particular choice y_0. Thus, by 2.2.7 (2), there is some $b \in \mathbb{N}$ such that $\sqrt{I_{y_0}}$ is not prime if and only if there are $f(x)$ and $g(x)$ of total degree less than b with $f(x), g(x) \notin \sqrt{I_{y_0}}$ and $f(x)g(x) \in \sqrt{I_{y_0}}$; again, b is independent of y_0 . But by 2.2.7 (3), there is some $c \in \mathbb{N}$ such that this is equivalent to there being $f(x)^c, g(x)^c \notin I_{y_0}$, but $(f(x)g(x))^c \in I_{y_0}$. Since the total degree of $f(x)$ and $g(x)$ is bounded by b, by 2.2.7 (1) this last statement and its negation are expressible in the pure language of rings. Its negation is what we required.

2. This follows from the uniform definability of Morley Rank in a strongly minimal theory; a nice general presentation of this result is for *geometric structures* in Lemma 2.3 of [16], particularly part (ii), which asserts the uniform definability of the rank for geometric structures.

3. The onto projections are obviously definable.

Let X and Y be constructible sets such that mult(X)=mult(Y)=1. A projection $(\pi : X \mapsto Y)$ is generically onto if and only if

$$\mathrm{MR}(\pi(X)) = \mathrm{MR}(Y)$$

where MR is the Morley Rank. It follows that we may uniformly define a sub-family of $A(xz, t)$ where π is generically onto if MR is uniformly definable in the family of images of π.

In the last part we saw that the MR is uniformly definable in any family of constructible sets (see Lemma 2.3 of [16]). Now write $A(xz, t)$ as $A(x, zt)$. By the uniform definability of Morley Rank, we may uniformly define $\{zt : \mathrm{MR}(A(x, zt)) = 0\}$. From this we see that both projections of everywhere finite fibre, and projections of generically finite fibre, are uniformly definable. □

2.2.1 Stratification by degree or inseparable degree of a projection

Now let $A(xz, t)$ be a family of 0-definable algebraic sets, as in Lemma 2.2.10. Then there is a uniformly definable sub-family of $A(xz, t)$ across algebraically closed fields,

denoted by $A^*(xz,t)$, where by Lemma 2.2.10, for each $t \in P(A^*)$ we have

1. $A^*(xz,t)$ is an irreducible variety;
2. $\pi_x(A^*(xz,t)) \subseteq V(x,y)$ and $V(x,y)$ is an irreducible variety;
3. the projection π_x to the variable x is (onto/generically onto) of (everywhere finite /generically finite fibre).

In the next lemma we relabel this A^* as A; also, since we are only interested in the case where y is a subtuple of t, we may assume that $y = t$. The remainder of this section is concerned with the proof of the following lemma:

LEMMA 2.2.11 *Let $A(xz,y)$ and $V(x,y)$ be 0-definable families of irreducible varieties. Let π_x be the projection from $A(xz,y)$ to the variable x. For $y_0 \in P(A)(\tilde{K})$, let $\pi_x(y_0)$ be the projection π_x restricted to the algebraic set $A(xz,y_0)$. So we may see $\pi_x(y)$ as a family of projections. We suppose for any $\tilde{K}$ and $y_0 \in P(A)(\tilde{K})$, that $\mathrm{Im}(\pi_x(y_0)) \subseteq V(x,y_0)$, that $\pi_x(y_0)$ is generically onto $V(x,y_0)$, and that $\pi_x(y_0)$ has generically finite fibres. Then both the degree of $\pi_x(y)$ and the inseparable degree of $\pi_x(y)$ are uniformly definable in the family $A(xz,y)$ over algebraically closed fields.*

We shall prove 2.2.11 by showing that the criteria of Lemma 2.2.4 (Part 2) are met by both the degree and inseparable degree.

Background to proof of 2.2.11

If $S = \{h_j : 1 \leq j \leq m\}$ is a finite set of polynomials with $h_j \in \tilde{K}[x]$ then let $I = \langle S \rangle$ be the ideal generated by S in $\tilde{K}[x]$. Let $V(I)$ be the algebraic set defined by I. Then we say that V is presented by the set of polynomials S. In other words, V is defined by the formula $\varphi : \wedge_{j=1}^{m} h_j(x) = 0$. Similarly, let $R = \{g_r : 1 \leq r \leq s\}$ be a finite set of polynomials with $g_r \in \tilde{K}[xz]$, $J = \langle R \rangle$ and let $W(J)$ be the algebraic set defined by the ideal J. We shall find ourselves considering a projection $\pi : W \mapsto V$ when we wish to uniformly define the degrees/inseparable degrees of families of projections in which π may be a member. Let $I(V) = \sqrt{I}$ and $J(W) = \sqrt{J}$ be the ideals in $\tilde{K}[x]$ of the algebraic sets V and W respectively. The analysis of degree and inseparable degree of the projection π is done by examining the extension $\mathrm{Frac}(\tilde{K}[xz]/\sqrt{J})/\mathrm{Frac}(\tilde{K}[x]/\sqrt{I})$.

It may be that $I \neq \sqrt{I}$. Given a family of algebraic sets $V(x,y)$, we wish to give a presentation of $V(x,y)$ by polynomials in parameter y as the solution set of some $S = \{h_j(x,y) : 1 \leq j \leq m\}$, so that for each member of the family, in the notation we have adopted, $I = \sqrt{I}$.

LEMMA 2.2.12 *Let $V(x,y)$ be a family of $\emptyset$-definable algebraic sets. Suppose $V(x,y)$ is presented as the solution set of a set of polynomials $S = \{h_j(x,y) : 1 \leq j \leq m\}$. Then $V(x,y)$ may be uniformly stratified into sub-families $\{A_i(x,y) : i \in I\}$ with the following property:*

Let $A(x,y) = A_i(x,y)$. Then there are some $n, k \in \mathbb{N}$ depending on i such that $A(x,y)$ can be presented as a formula of the form

$$\exists(z_1, z_2, \ldots, z_k)(\bigwedge_{l=1}^{n} f_l(x, z_1, z_2, \ldots, z_k) = 0 \ \wedge \ \bigwedge_{r=1}^{k} g_r(z_r, y) = 0)$$

where

1. *each $g_r(z_r, y)$ is a purely inseparable polynomial satisfied by z_r over the field generated by y.*
2. *Let $y_0 \in P(A)(\tilde{K})$. Recall that F is the prime field of $\tilde{K}$. Let $\widetilde{F(y_0)}$ be the algebraic closure of the field $F(y_0)$. If $z_{r0} \in \widetilde{F(y_0)}$ such that $g_r(z_{r0}, y_0) = 0$ for $1 \leq r \leq k$, then $\langle f_l(x, z_{10}, z_{20}, \ldots, z_{k0}) : 1 \leq l \leq n\rangle = I(V(x, y_0))$.*

Concretely, we have the following equivalence:

$$A(x,y) \iff P(A)(y) \ \wedge \ \exists(z_1, z_2, \ldots, z_k)(\bigwedge_{l=1}^{n} f_l(x, z_1, z_2, \ldots, z_k) = 0 \ \wedge \ \bigwedge_{r=1}^{k} g_r(z_r, y) = 0)$$

PROOF We aim to show the criteria of Lemma 2.2.4 (Part 2) are met. So let $\tilde{K}$ be an algebraically closed field and $y_0 \in P(V)(\tilde{K})$. Let $S_{y_0} = \{h_j(x, y_0) : 1 \leq j \leq m\}$. Let Y be the set of coefficients of the polynomials in S_{y_0}; then $Y \subseteq \tilde{K}$. Let $I = \langle S_{y_0}\rangle$ in $\tilde{K}[X]$, and let $F(Y)^{\text{ins}}$ be the pure inseparable closure of the field $F(Y)$. Then recall that $I(V(I))$ is generated by a finite set of polynomials $R = \{f_j(x, \bar{z}) : 1 \leq j \leq n\}$, where $\bar{z}$ is a tuple of elements from $F(Y)^{\text{ins}}$. (There are many references to this in the literature - see for example [21] pp.74, C7⇒C6. Essentially, this is by a simple automorphism argument: if an automorphism fixes Y then it fixes $V(I)$, so it must fix

the field of definition of $V(I)$. So the field of definition of $V(I)$, which we denote F_0, lies in the definable closure of the set Y, so it lies in the purely inseparable closure of $F(Y)$. Furthermore, by Hilbert's basis theorem, $F_0/F(Y)$ is a finite extension.)

Thus, we may write the $\mathcal{L}_{\text{rings}}(F(y_0))$-sentence

$$\exists(z_1, z_2, \ldots, z_k)(\forall x(\bigwedge_{l=1}^{n} f_l(x, z_1, z_2, \ldots, z_k) = 0 \Leftrightarrow \bigwedge_{j=1}^{m} h_j(x, y_0) = 0) \wedge \bigwedge_{r=1}^{k} g_r(z_r, y_0) = 0) \tag{2.6}$$

representing $I(V(I))$ where the z_r and g_r, y_0, and the f_l have the properties demanded by the statement of the lemma. It will be convenient to refer to the tuple $z = (z_1, z_2, \ldots, z_k)$.

To apply lemma 2.2.4 (Part 2) it suffices to show the following: in the notation of expression 2.6, there is a 0-definable set $Y_{y_0}(y)$ containing y_0, where for any algebraically closed field $\tilde{L}$ and $y_1 \in Y_{y_0}(\tilde{L})$, then $I(V(x, y_1)) \subseteq \tilde{L}[x]$ is generated by a set of polynomials $R = \{f_l(x, z_1) : \ 1 \leq l \leq n\}$, $z_1 = (z_{11}, z_{21}, \ldots, z_{k1})$, each $z_{l1} \in \tilde{L}$ for $\ 1 \leq l \leq k$,

$$\bigwedge_{r=1}^{k} g_r(z_{r1}, y_1) = 0 \tag{2.7}$$

and each polynomial $g_r(Z, y_1)$, in indeterminate Z, is purely inseparable.

Now the strong version of Hilbert's Nullstellensatz states that for any ideal $I \subseteq \tilde{K}[\bar{X}]$, $I(V(I)) = \sqrt{I}$, where $\sqrt{I}$ is the radical of I. So it will suffice to show that there is a 0-formula $Y_{y_0}(y)$ such that the following demands are satisfied:

Demands on Y_{y_0}

1. $Y_{y_0}(y_0)$ holds.
2. Suppose $y_1 \in \tilde{L}$ and $Y_{y_0}(y_1)$ holds. For $1 \leq r \leq k$, let $z_{r1} \in \tilde{L}$ satisfy $g_r(z_{r1}, y_1)$, as in expression 2.7. Each polynomial $g_r(Z, y_1)$, in indeterminate Z, is purely inseparable. Let $J_{y_1} = \langle f_l(x, z_{11}, z_{21}, \ldots, z_{k1})\rangle \subseteq \tilde{L}[x]$, where the polynomials f_l are as in expression 2.7. Let $I_{y_1} = \langle h_j(x, y_1) : \ 1 \leq j \leq m\rangle$. Then $J_{y_1} = \sqrt{I_{y_1}}$.

We shall now construct $Y_{y_0}(y)$ by refining a series of formulas. Each sub-formula is chosen to be a particular formula satisfed by y_0, so demand 1 will be automatically

satisfied.

To begin, let us treat the pure inseparability of the polynomials $g_r(Z, y)$. Suppose characteristic$(\tilde{K}) = p$. We can select the original $g_r(Z, y_0)$ to be of a simple form:

$$g_r(Z, y_0) \ =_{\text{def}} \ Z^{p^t} - q_r(y_0)$$

for some $t \in \mathbb{N}$, and where $q_r(y_0)$ is a constant term in $\mathcal{L}_{\text{rings}}(y_0)$. It is clear that for any characteristic p field $\tilde{L}$, and parameter $y_1 \in \tilde{L}$, then $g_r(Z, y_1)$ is purely inseparable over $F(y_1)$. So in this case we define the formula char to be

$$\text{char}(y) \ = \ _{\text{def}} \ 1 + 1 + \ldots + 1 \ (p \text{ times}) \ = 0 \tag{2.8}$$

Alternatively, characteristic$(\tilde{K}) = 0$, and then we may write

$$g_r(Z, y_0) \ =_{\text{def}} \ Z - q_r(y_0)$$

again where $q_r(y_0)$ is a constant term in $\mathcal{L}_{\text{rings}}(y_0)$. It is clear that for any field $\tilde{L}$ and parameter $y_1 \in \tilde{L}$, then $g_r(Z, y_1)$ defines Z to be in $F(y_1)$ (and thus clearly purely inseparable over $F(y_1)$). So in this case

$$\text{char}(y) \ =_{\text{def}} \ y = y \tag{2.9}$$

Now let θ_0 be defined by:

$$\theta_0^*(y, z_1, z_2, \ldots, z_k) \ = \ _{\text{def}} \ (\forall x(\bigwedge_{l=1}^{n} f_l(x, z_1, z_2, \ldots, z_k) = 0 \Leftrightarrow \bigwedge_{j=1}^{m} h_j(x, y) = 0) \wedge \bigwedge_{r=1}^{k} g_r(z_r, y) = 0 \ \wedge \ \text{char}(y))$$

$$\theta_0(y) \ =_{\text{def}} \ \exists(z_1, z_2, \ldots, z_k)(\theta_0^*(y, z_1, z_2, \ldots, z_k)) \tag{2.10}$$

Then it is clear that the requirements on $g_r(Z, y_1)$ for pure inseparability, in demand 2, are met if $Y_{y_0}(y_1) \Rightarrow \theta_0(y_1)$. It is also clear that if $Y_{y_0}(y_1) \Rightarrow \theta_0(y_1)$ then the algebraic set defined by J_{y_1} is identical to the algebraic set defined by I_{y_1}.

So to meet all of demand 2 for Y_{y_0}, it is now enough that we construct a sub-formula asserting that $J_{y_1} = \sqrt{J_{y_1}}$. To do so we need the following preparatory statement:

Claim: Let $W(x,w)$ be a $\emptyset$-definable family of algebraic sets given by a set of polynomials $G = \{g_j(x,w) : \ 1 \leq j \leq c\}$. For $w_0 \in P(W)(\tilde{K})$, we define the ideal $I_{w_0} = \langle g_j(x,w_0) : \ 1 \leq j \leq c\}\rangle$. Then the sub-family of W given by $\{w : \ I_w = \sqrt{I_w}\}$ is uniformly definable over algebraically closed fields.

Proof of Claim: Consider G as a set of polynomials in the variables x, with coefficients w. Recall that for any polynomial ideal I, $\sqrt{I}$ is the intersection of the minimal prime ideals of I. So, by Fact 2.2.7 (4), there is $D \in \mathbb{N}$ such that over all algebraically closed fields $\tilde{K}$, for any $w_0 \in P(W)(\tilde{K})$, $\sqrt{I_{w_0}}$ is generated by polynomials of total degree $\leq D$; also, the constant D is independent of w_0. Thus we need an $\mathcal{L}_{\text{rings}} - 0-$formula which defines over algebraically closed fields the set $\{w : \$ all polynomials of total degree $\leq D$ which have a power in I_w are themselves in $I_w\}$. By Fact 2.2.7 (3), there is $C \in \mathbb{N}$ such that if there is a polynomial $g(x) \in \tilde{K}[x]$ of total degree $\leq D$ and $k \in \mathbb{N}$ with $g(x)^k \in I_{w_0}$, then $g(x)^C \in I_{w_0}$. Thus, to say that $I_{w_0} = \sqrt{I_{w_0}}$ is to say:

'There is no $g(x) \in \tilde{K}[x]$ of degree $\leq D$ such that $g(x)^C \in I_{w_0}$ and $g(x) \notin I_{w_0}$.'

Notice that $g(x)^C$ has total degree $\leq C \cdot D$. Thus, using Fact 2.2.7 (1), the quoted statement is a uniformly definable statement; the claim follows. **End of proof of claim**

Apply the claim to the family of ideals in parameter $z = (z_1, z_2, \ldots, z_k)$ given by the family $R = \{f_l(x,z) : \ 1 \leq l \leq n\}$ of sets of polynomials, which is also in parameter $z = (z_1, z_2, \ldots, z_k)$. So there is a formula $\theta_1^*(z)$ defined without parameters such that if $z^* \in \tilde{L}$ is a tuple with $z^* = (z_1^*, z_2^*, \ldots, z_k^*)$, and $\theta_2^*(z^*)$ holds, then for $J = \langle\{f_l(x,z^*) : 1 \leq l \leq n\}\rangle$ we have $J = \sqrt{J}$. We now conclude:

$$Y_{y_0}(y) \ =_{\text{def}} \ \exists(z_1, \ldots, z_k)(\theta_0^*(y, z_1, \ldots, z_k)) \ \wedge \ \theta_1^*(z_1, \ldots, z_k)) \quad \square \tag{2.11}$$

REMARK 2.2.13 Consider a sub-family in the stratification of Lemma 2.2.12:

$$A(x,y) \ =_{\text{def}} \ P(A)(y) \wedge \exists(z_1, z_2, \ldots, z_k)(\bigwedge_{l=1}^{n} f_l(x, z_1, z_2, \ldots, z_k) = 0 \wedge \bigwedge_{r=1}^{k} g_r(z_r, y) = 0)$$

and consider

$$B(x,y,z_1,z_2,\ldots,z_k) =_{\text{def}} P(A)(y) \wedge \bigwedge_{l=1}^{n} f_l(x,z_1,z_2,\ldots,z_k)=0 \wedge \bigwedge_{r=1}^{k} g_r(z_r,y)=0$$

Let $z=(z_1,z_2,\ldots,z_k)$. We have that $A(x,y)$ and $B(x,yz)$ are the identical *family* of sets; it is the parameterisation that is different. Let $f: P(B)(yz) \mapsto P(A)(y)$ be the natural projection of parameter sets. Since by construction, the g_r are purely inseparable over y, f is 1-to-1, and so by Fact 2.2.3 a stratification of $B(x,yz)$ may be 'rearranged' into a stratification of $A(x,y)$.

Proof of Lemma 2.2.11

PROOF Let us fix some notation. We shall assume $V(x,y)$ is given by a set of 0-polynomials $S=\{h_j(x,y): 1\leq j\leq m\}$, and we assume that $A(xz,y)$ is given by a set of 0-polynomials $U=\{f_l(xz,y): 1\leq l\leq u\}$. We shall denote specific family members by subscripts: so for some $\tilde{K}$ and $y_0\in P(A)(\tilde{K})$, we let $S_{y_0}=\{h_j(x,y_0): 1\leq j\leq m\}$ and we let $I_{y_0}=\langle\{h_j(x,y_0): 1\leq j\leq m\}\rangle$ be an ideal in $\tilde{K}[x]$. Similarly, we let $U_{y_0}=\{f_l(xz,y_0): 1\leq l\leq u\}$ and $J_{y_0}=\langle\{f_l(xz,y_0): 1\leq l\leq u\}\rangle$.

By Remark 2.2.13 we may assume:

$$\text{For all } \tilde{K} \text{ and } y_0\in P(A)(\tilde{K}),\quad I_{y_0}=\sqrt{I_{y_0}} \text{ and } J_{y_0}=\sqrt{J_{y_0}} \tag{2.12}$$

For a finite extension of fields L/K we write the degree of the extension as $[L:K]$ and the inseparable degree as $[L:K]_{\text{i}}$. Under assumption 2.12 and under the assumptions in the statement of the lemma, the degree of π_{y_0} (denoted deg) satisfies

$$\deg(\pi_{y_0})=[\text{Frac}(\tilde{K}[xz]/J_{y_0}):\text{Frac}(\tilde{K}[x]/I_{y_0})] \tag{2.13}$$

and the inseparable degree of π_{y_0} (deg.ins) satisfies

$$\text{deg.ins}(\pi_{y_0})=[\text{Frac}(\tilde{K}[xz]/J_{y_0}):\text{Frac}(\tilde{K}[x]/I_{y_0})]_{\text{i}} \tag{2.14}$$

We shall prove both that both degree and inseparable degree are uniformly definable in the family $A(xz,y)$ over algebraically closed fields, by applying Lemma 2.2.4 (Part 2). We prove both results simultaneously. So suppose that $y_0\in P(A)(\tilde{K})$. We shall construct a $\emptyset$-definable set $Y_{y_0}(y)$ such that $\tilde{K}\models Y_{y_0}(y_0)$ and for all $\tilde{L}$ and $y_1\in P(A)(\tilde{L})$

such that $Y_{y_0}(y_1)$ holds, the degree and inseparable degree of π_{y_1} will be constant.

Let $G = \tilde{K}[x]/I_{y_0}$ and let $H = \mathrm{Frac}(G)$. Similarly, let $B = \tilde{K}[xz]/J_{y_0}$ and let $M = \mathrm{Frac}(B)$. There is $n \in \mathbb{N}$ such that there are $t_i \in M$ and we may write $M = H(t_1, t_2, \ldots t_n, t_{n+1})$ where $H(t_1, t_2, \ldots, t_n)/H$ is purely inseparable, and $M/H(t_1, t_2, \ldots, t_n)$ is a separable extension primitively generated by t_{n+1}. This is classical theory of fields and may be found in, for instance, [22]: briefly, $H(t_1, t_2, \ldots t_n)/H$ is the maximal purely inseparable extension inside the finite extension M/H (it exists by Proposition 6.11 of [22]), and then the fact that $M/H(t_1, t_2, \ldots t_n)$ can be primitively generated follows from the Primitive Element Theorem (see Theorem 4.6 of [22]). Let $H_0 = H$ and for $1 \leq i \leq n+1$ let $H_i = H(t_1, t_2, \ldots, t_i)$.

Claim: (1) Let $T_1, T_2, \ldots, T_{n+1}$ be indeterminates. There is a polynomial $g(x) \in \tilde{K}[x]$ such that: for each $1 \leq i \leq n+1$ there is a monic polynomial $m_i \in \tilde{K}[x, T_1, \ldots, T_i]_{(g)}$ such that the ring $R_i = \tilde{K}[x, T_1, \ldots, T_i]_{(g)}/\langle I_{y_0}, m_1, \ldots, m_i \rangle$ is an integral domain, $\mathrm{Frac}(R_i) \cong H_i$, and there is the following commutative diagram:

$$\begin{array}{ccccc}
\tilde{K}[x, T_1, \ldots, T_i]_{(g)} & \twoheadrightarrow & (\tilde{K}[x]_{(g)}/I_{y_0})[T_1, \ldots, T_i] & \hookrightarrow & (\mathrm{Frac}(\tilde{K}[x]/I_{y_0}))[T_1, \ldots, T_i] \\
\downarrow & & \downarrow & & \downarrow \\
R_i & \cong & R_i & \subseteq & H_i
\end{array}$$

Let $\mathrm{char}(\tilde{K}) = p$. For $1 \leq i \leq n$, the polynomial m_i may be written in the form

$$T_i^{p^{n_i}} - q_i$$

where $n_i \in \mathbb{N}$ and $q_i \in \tilde{K}[x, T_1, \ldots, T_{i-1}]_{(g)}$. The polynomial m_{n+1} can be written

$$\sum_{j=0}^{N} q_{nj} T_{n+1}^j$$

where $N \in \mathbb{N}$, $q_{nN} = 1$, $q_{nj} \in \tilde{K}[x, T_1, \ldots, T_n]_{(g)}$, and there is at least one j_0 with $1 \leq j_0 \leq N$ such that:

(a) $p \not| j_0$

(b) $q_{nj_0} \notin \langle I_{y_0}, m_1, \ldots, m_n \rangle$

(2) Suppose that the situation as described in Part 1 holds: $T_1, \ldots T_{n+1}$ are indeterminates, $I_{y_0} \subseteq \tilde{K}[x]$ is a radical ideal, $g(x) \in \tilde{K}[x]$, for each $1 \leq i \leq n+1$ there are monic polynomials $m_i \in \tilde{K}[x, T_1, \ldots, T_i]_{(g)}$ of the form described in Part 1 with respect to a distinguished prime p (if $n \geq 1$), the ring $R_i = \tilde{K}[x, T_1, \ldots, T_i]_{(g)}/\langle I_{y_0}, m_1, \ldots, m_i \rangle$ is an integral domain with $\mathrm{Frac}(R_i) \cong H_i$, and the given commutative diagram holds. Express m_i as a polynomial in the indeterminate T_i with coefficients in the ring $\tilde{K}[x, T_1, \ldots, T_{i-1}]_{(g)}$. Then

(i) For each i with $1 \leq i \leq n+1$, $[H_i : H_{i-1}] =$degree(m_i).

(ii) If $\mathrm{char}(\tilde{K}) = p$, then H_i/H_{i-1} is purely inseparable for $1 \leq i \leq n$.

(iii) If $\mathrm{char}(\tilde{K}) \neq p$, then H_i/H_{i-1} is separable for $1 \leq i \leq n$.

(iv) We may exclude finitely many primes $P_{\mathrm{excl}} = (p_1, \ldots, p_l)$ such that $p \notin P_{\mathrm{excl}}$, and if $\mathrm{char}(\tilde{K}) \notin P_{\mathrm{excl}}$, then H_{n+1}/H_n is separable.

Proof of Claim: (1) The statement is for n, but it could be relativised to any $0 \leq r \leq n+1$. Suppose that Part 1 of the claim holds for some r with $0 \leq r \leq n+1$, and $g \in \tilde{K}[x]$ is a localisation polynomial witnessing the claim. Suppose $g|b$ for $b \in \tilde{K}[x] \backslash I_{y_0}$. Then the claim holds for r, with b in the place of g, with the same m_i. We verify this in the following set of enumerated points. We shall need to refer to the ideal $\langle I_{y_0}, m_1, \ldots, m_i \rangle$ as generated in the ring $\tilde{K}[x, T_1, \ldots, T_i]_{(g)}$, and also in the ring $\tilde{K}[x, T_1, \ldots, T_i]_{(b)}$, so we shall use the notation $I_{(g)}$ and $I_{(b)}$ to distinguish between the two:

1. The reader can verify that $I_{(g)} \cap \tilde{K}[x] = I_{y_0}$, and so $b \notin I_{(g)}$. It follows then that $I_{(b)}$ is a prime ideal in $\tilde{K}[x, T_1, \ldots, T_i]_{(b)}$.

2. Using the previous item, for each $1 \leq i \leq r$ there is a commutative diagram of localisations:

$$\begin{array}{ccc} \tilde{K}[x, T_1, \ldots, T_i]_{(g)} & \subseteq & \tilde{K}[x, T_1, \ldots, T_i]_{(b)} \\ \downarrow (\varphi_i) & & \downarrow \\ R_i & \subseteq & (R_i)_{(\varphi_i(b))} \end{array}$$

(Here, we have labeled the quotient surjection $\varphi_i : \tilde{K}[x, T_1, \ldots, T_i]_{(g)} \twoheadrightarrow R_i$.) Since $\mathrm{Frac}((R_i)_{(\varphi_i(b))}) \cong H_i$, the localised rings $(R_i)_{\varphi_i(b)}$ and b clearly witnesses all of Part 1 of the claim except if $r = n + 1$ we still have not shown that the demand referred to as (b) is met. We address this is the next item.

3. Now suppose that $r = n + 1$ and henceforth let $\langle I_{y_0}, m_1, \ldots, m_n \rangle$ as generated in the ring $\tilde{K}[x, T_1, \ldots, T_n]_{(b)}$ be denoted by $I_{(b)}$, and the same ideal generated in the ring $\tilde{K}[x, T_1, \ldots, T_n]_{(g)}$ be denoted by $I_{(g)}$. Suppose that $q_{nj_0} \in I_{(b)}$. Then for some $\gamma \in \mathbb{N}$ and $a \in I_{(g)}$ we have $q_{nj_0} = \frac{a}{b^\gamma}$. But then $q_{nj_0} \cdot b^\gamma \in I_{(g)}$. We have seen that $b \in \tilde{K}[x, T_1, \ldots, T_n]_{(g)} \backslash I_{(g)}$, and by assumption $q_{nj_0} \in \tilde{K}[x, T_1, \ldots, T_n]_{(g)} \backslash I_{(g)}$. But also by assumption, $I_{(g)}$ is prime in $\tilde{K}[x, T_1, \ldots, T_n]_{(g)}$, so we have a contradiction.

We shall prove Part 1 of the claim by induction on i. We denote the localisation polynomial that witnesses Claim 1 at stage i by g_i. We shall re-choose g_i at each stage such that $g_{i-1} | g_i$, and so by the previous clause of this proof, the induction remains valid.

The case $i = 0$ is vacuous.

Now for the inductive step. Let m^{**}_{i+1} be a monic, minimal polynomial for t_{i+1} in $H_i[T_{i+1}]$. By induction there is a surjection $\mathrm{Frac}(\tilde{K}[x]/I_{y_0}))[T_1, \ldots, T_i] \twoheadrightarrow H_i$. Choose a preimage m^*_{i+1} of m^{**}_{i+1} in $\mathrm{Frac}(\tilde{K}[x]/I_{y_0})[T_1, \ldots, T_i][T_{i+1}]$. Then $m^*_{i+1} = \frac{1}{g^{*'}_{i+1}} \cdot n^*_{i+1}$, where $g^{*'}_{i+1} \in \tilde{K}[x]/I_{y_0}$ and $n^*_{i+1} \in (\tilde{K}[x]/I_{y_0})[T_1, \ldots, T_i][T_{i+1}]$. We let $g^{'}_{i+1}$ be a preimage of $g^{*'}_{i+1}$ in $\tilde{K}[x]$, and we let $g_{i+1} = g_i \cdot g^{'}_{i+1}$. According to the first clause of the proof, we assume from now on that the induction has thus far been witnessed with respect to the polynomial g_{i+1}. By design, there is a monic preimage of m^*_{i+1} in $\tilde{K}[x][T_1, \ldots, T_i][T_{i+1}]_{(g_{i+1})}$, and we choose m_{i+1} to be such a preimage.

If $i \leq n$, then it is clear that we can select m_i^{**} to be of the form:

$$T_i^{p^{n_i}} - q_i^{**}$$

where $n_i \in \mathbb{N}$ and $q_i^{**} \in R_i$. By inspection, the pullback m_i has the required form.

If $i = n+1$ then the extension H_{n+1}/H_n is separable by design. So, the monic polynomial m_{n+1}^{**} may be written:

$$\sum_{j=0}^{N} q_{nj}^{**} T_{n+1}^j$$

where $N \in \mathbb{N}$, $q_{nj}^{**} \in R_n$, and there is a j_0 with $1 \leq j_0 \leq N$, such that $p \not| j_0$ and $q_{nj_0}^{**} \neq 0$. This is by basic separability theory (see [22] ch. 5). By induction, there is a pullback of $q_{nj_0}^{**}$ in $\tilde{K}[x, T_1, \ldots, T_n]_{(g_{n+1})}$ from the natural map $\tilde{K}[x, T_1, \ldots, T_n]_{(g_{n+1})} \mapsto H_n$, so a fortiori $q_{nj_0}^{**}$ cannot be in the kernel. By induction, the kernel is $\langle I_{y_0}, m_1, \ldots, m_n \rangle$. Thus, the pullback m_{n+1} of m_{n+1}^{**} has the required form.

All this leaves us with the commutative diagram:

$$\begin{array}{ccccc}
\tilde{K}[x, T_1, \ldots, T_{i+1}]_{(g_{i+1})} & (\twoheadrightarrow \eta) & (\tilde{K}[x]_{(g_{i+1})}/I_{y_0})[T_1, \ldots, T_{i+1}] & & \\
\downarrow & & \downarrow (\varphi) & & \\
R_i[T_{i+1}] & \cong & R_i[T_{i+1}] & (\twoheadrightarrow \psi) & R_i[T_{i+1}]/\langle m_{i+1}^{**} \rangle \\
\cap\!\!| & & \cap\!\!| & & \downarrow (\mu) \\
H_i[T_{i+1}] & \cong & H_i[T_{i+1}] & \twoheadrightarrow & H_i[T_{i+1}]/\langle m_{i+1}^{**} \rangle
\end{array}$$

We define $R_{i+1} := R_i[T_{i+1}]/\langle m_{i+1}^{**} \rangle$, so we must now (a) show that $\ker(\psi\varphi\eta) = \langle I_{y_0}, m_1, \ldots m_{i+1} \rangle$, (b) show that the map labelled μ is an inclusion, and (c) show $\mathrm{Frac}(R_{i+1}) = H_i[T_{i+1}]/\langle m_i^{**} \rangle = H_{i+1}$.

(a) Suppose $z \in \tilde{K}[x, T_1, \ldots, T_{i+1}]_{(g_{i+1})}$ and $z \in \ker(\psi\varphi\eta)$; so $\varphi\eta(z) = m_{i+1}^{**} \cdot \chi$ for some $\chi \in R_i[T_{i+1}]$. Now $\varphi\eta$ extends the map $\varphi_i : \tilde{K}[x, T_1, \ldots, T_i]_{(g_{i+1})} \mapsto R_i$, (shown in the diagram above in point number 2 at the beginning of the proof of the claim), which by induction is a surjection. So by induction, $\varphi\eta$ is a surjection. Similarly, since the

kernel of the map φ_i is $\langle I_{y_0}, m_1, \ldots, m_i\rangle$ generated in $\tilde{K}[x, T_1, \ldots, T_i]_{(g_{i+1})}$, it follows that the kernel of $\varphi\eta$ is $\langle I_{y_0}, m_1, \ldots, m_i\rangle$ generated in $\tilde{K}[x, T_1, \ldots, T_{i+1}]_{(g_{i+1})}$. Notice that we have adjusted all localisations to localising by g_{i+1}, which we have shown we may do. It follows that $z \in \langle I_{y_0}, m_1, \ldots, m_{i+1}\rangle$.

(b) Suppose $z \in R_i[T_{i+1}]/\langle m_i^{**}\rangle$ and $z \in \ker(\mu)$. It follows that there is $z' \in \psi^{-1}(z)$ with $z' = m_{i+1}^{**} \cdot \frac{\chi_2}{\chi_1}$ for χ_2 a monic polynomial in $R_i[T_{i+1}]$, and $\chi_1 \in R_i$. Now m_{i+1}^{**} is monic so the leading term of z' has coefficient $\frac{1}{\chi_1}$, and since $z' \in R_i[T_{i+1}]$, it follows that χ_1 is a unit in R_i. Let $\chi = \frac{\chi_2}{\chi_1}$. Then $\chi \in R_i[T_{i+1}]$ and $z' = m_{i+1}^{**} \cdot \chi$. Thus $\psi(z') = z = 0$. So μ is an injection.

(c) This is now clear.

(2) By assumption we have the following commutative diagram:

$$\begin{array}{ccc} \tilde{K}[x, T_1, \ldots, T_i, T_{i+1}]_{(g)} & & \\ \downarrow (\varphi) & & \searrow (\mu) \\ H_i[T_{i+1}] & \twoheadrightarrow (\psi) & H_{i+1} \end{array}$$

(i) Suppose $z \in \ker(\psi)$. Then for $z' \in \varphi^{-1}(z)$ we have $z' \in \ker(\mu)$. By assumption, $z' = z_0 + \sum_{j=0}^{i+1} a_j \cdot m_j$ for some $z_0 \in I_{y_0}$, and for each $0 \leq j \leq i+1$, we have $a_j \in \tilde{K}[x, T_1, \ldots, T_{i+1}]_{(g)}$. It follows that $z \in \langle \varphi(m_{i+1})\rangle$. So clearly $\varphi(m_{i+1})$ is a minimal polynomial for the extension H_{i+1}/H_i. But m_{i+1} is monic so its degree is the degree of that extension.

(ii) and (iii) For $1 \leq i \leq n$, the assumptions mean that $\varphi(m_i)$ has the form of the polynomial satisfied by a p-power'th root. Clearly this implies that H_i/H_{i-1} is a purely inseparable extension in the characteristic p case, and a separable extension in the not characteristic p case.

(iv) Let

$$\varphi(m_{n+1}) = \sum_{j=0}^{N} q_{nj}^{**} T_{n+1}^j$$

for $q^{**}_{nj} \in H_n$. The conditions imply that there is some j_0 with $1 \leq j_0 \leq N$ such that $p \not| j_0$ and $q^{**}_{nj_0} \neq 0$. So let $P_{\text{excl}} = \{$ the primes that divide $j_0\}$. Clearly $p \notin P_{\text{excl}}$, and again, by basic separability theory, so long as $\varphi(m_{n+1})$ has a non-zero coefficient in a term of power coprime to the characteristic, then $\varphi(m_{n+1})$, is separable, and consequently, so is H_{n+1}/H_n. **End of Proof of Claim**

We now use the claim to define Y_{y_0}: in a sense, Part 1 of the claim is to show that the projection at parameter y_0 has certain properties, and Part 2 shows that any member with those properties has identical degree and separable degree to the member y_0. What remains is to assert the definability of the properties in Claim 1.

It follows from the claim that $Y_{y_0}(y)$ need only assert:

1. There is a polynomial $g = g(x) \in \tilde{K}[x]$ and a set of elements $t = (t_1, \ldots, t_{n+1})$ with $t_i \in \tilde{K}[xz]_{(g)}/J_{y_0}$ such that $\text{Frac}(\tilde{K}[x,t]/J_{y_0})$ =$\text{Frac}(\tilde{K}[xz]/J_{y_0})$.

2. For each $1 \leq i \leq n+1$, there is a polynomial $m_i(T_1, \ldots, T_i)$, and $m_i(t_1, \ldots, t_i) = 0$.

3. For each $1 \leq i \leq n+1$ the ideal $I_i = \langle I_{y_0}, m_1, \ldots, m_i \rangle$ in $\tilde{K}[x, T_1, \ldots, T_i]_{(g)}$ is prime.

4. Let $\text{char}(\tilde{K}) = p$, or 0 as the case may be. For $1 \leq i \leq n$, the polynomial m_i is of the form

$$T_i^{p^{n_i}} - q_i$$

where $n_i \in \mathbb{N}$ and $q_i \in \tilde{K}[x, T_1, \ldots, T_{i-1}]_{(g)}$. The polynomial m_{n+1} is of the form

$$\sum_{j=0}^{N} q_{nj} T_{n+1}^j$$

where $N \in \mathbb{N}$, $q_N = 1$, $q_j \in \tilde{K}[x, T_1, \ldots, T_n]_{(g)}$, and there is at least one j_0 with $1 \leq j_0 \leq N$ such that:

(a) $p \not| j_0$

(b) $q_{nj_0} \notin \langle I_{y_0}, m_1, \ldots, m_n \rangle$

5. The characteristic is not a divisor of j_0.

(1) and (2) (1) is a conjunction of field-arithmetic statements in parameters from $\tilde{K}$; the conjunction may be replaced with an existential formula asserting the existence of parameters confirming the arithmetic statements. (2) is similar.

For (3), (4) and (5) we first apply the hyperbolicity trick to obtain the isomorphism $\alpha_i : \tilde{K}[x, T_1, \ldots, T_i]_{(g)} \cong \tilde{K}[x, T_1, \ldots, T_i, T]/\langle Tg - 1 \rangle$.

(3) We define $I_i^* = \langle I_{y_0}, \alpha_i(m_1), \ldots, \alpha_i(m_i), Tg - 1 \rangle$ in $\tilde{K}[x, T_1, \ldots, T_i, T]$, and then assertion (c) is equivalent to the assertion that I_i^* is prime in $\tilde{K}[x, T_1, \ldots, T_i, T]$, and the uniform definability of such an assertion is an application of Facts 2.2.7 virtually identical to the application in Lemma 2.2.10 (1).

(4) and (5) Since the statement $q_j \in \tilde{K}[x, T_1, \ldots, T_n]_{(g)}$ may be written $q_j \cdot g^s \in \tilde{K}[x, T_1, \ldots, T_n]$ for some $s \in \mathbb{N}$, this assertion is a conjunction of field arithmetic statements, like (1). For the statement $q_{nj_0} \notin \langle I_{y_0}, m_1, \ldots, m_n \rangle$ in $\tilde{K}[x, T_1, \ldots, T_n]_{(g)}$, we have the equivalent statement

$$\alpha_n(q_{nj_0}) \notin \langle I_{y_0}, \alpha_n(m_1), \ldots, \alpha_n(m_n), Tg - 1 \rangle \text{ in } \tilde{K}[x, T_1, \ldots, T_n, T]$$

and this is uniformly definable using Facts 2.2.7 (1). □

2.2.2 Fine stratification of algebraic sets and projections

LEMMA 2.2.14 *Let $A(x, y)$ be a $\emptyset$-definable family of algebraic sets.*

1. *We have the following:*

   (a) *There is a $\emptyset$-definable family of algebraic sets $V(x, z)$, such that over algebraically closed fields, any irreducible component of a member of $A(x, y)$ is a member of $V(x, z)$.*

(b) *The subfamily $V^*(x,z)$ of $V(x,z)$ of members which are irreducible components of some member of $A(x,y)$ is uniformly definable over algebraically closed fields.*

(c) *There is a $\emptyset$-definable, bounded, finite-to-1 map $f: P(V^*)(z) \mapsto P(A)(y)$ which maps the irreducible components of a member of $A(x,y)$ to $A(x,y)$.*

2. *Suppose $V(x,z)$ may be uniformly stratified by some arbitrary uniform stratification into sub-families $\{V_b: 1 \leq b \leq s\}$. Then $A(x,y)$ may be uniformly stratified according to tuples $e = (e_1, e_2, \ldots e_s)$, where the tuple e signifies that $A(x,y)$ contains e_b irreducible components in the sub-family $V_b(x,z)$, for each $1 \leq b \leq s$.*

PROOF (1a) **Claim 1:** There is a finite set of families of algebraic sets $S = \{V_i(x,y_i): 1 \leq i \leq n\}$ such that any irreducible component of a member of $A(x,y)$ is a member of some member of S.

Proof of Claim 1: Notice that the set of algebraic sets $\{W_j: 1 \leq j \leq r\}$ is the set of irreducible components for an algebraic set X if and only if

- $X = \cup_{j=1}^{r} W_j$
- There are no proper inclusions amongst the W_j.
- The W_j are irreducible.

Now, by Lemma 2.2.4 there is an upper bound on the number of irreducible components in a member of $A(x,y)$. Thus, for a finite collection of $\emptyset$-definable families $W = \{W_j(x,z_j): 1 \leq j \leq r\}$ the set

$$\text{Bad}_W := \{y: A(x,y) \text{ does not have all its components members of members of } W\}$$

is definable without parameters in algebraically closed fields. Call such a finite collection of families a W-set and its associated Bad_W a Bad-W-set. If $W = \cup W_i$ is a W-set given as a union of W-sets, then $\text{Bad}_W = \cap_i \text{Bad}_{W_i}$. Now apply compactness: if the intersection of finitely many Bad_W-sets is always non-empty in algebraically closed fields, then there is some y_0 in some algebraically closed field $\tilde{K}$, such that there is no finite collection of families that contain all the irreducible components of $A(x,y_0)$. This is absurd, and so there is a finite intersection of Bad_W-sets which is empty; and

so there is an empty Bad_W set. The corresponding collection W is the collection of families we sought. **End of proof of Claim 1**

Claim 2: Here, let $S = \{V_i(x, y_i) : \ 1 \leq i \leq n\}$ be a finite set of families of definable sets in algebraically closed fields. By the disjoint union of the members of S we mean a family $V(x, z)$ such that for any algebraically closed field $\tilde{K}$ there is a bijective map $d : \ \coprod_{1 \leq i \leq n} P(V_i)(\tilde{K}) \mapsto P(V)(\tilde{K})$ such that for any $y_{i0} \in P(V_i(\tilde{K}))$, we have $V(\tilde{K}, d(y_{i0})) = V_i(\tilde{K}, y_{i0})$. Then the disjoint union of the members of S is a family of definable sets.

Proof of Claim 2: Let $z = y_1 y_2 \ldots y_n w$ be a tuple of tuples, where $w = w_1 \ldots w_n$ is a tuple of length n; we think of w as the *marker tuple*. We let $V(x, z)$ be the family of definable sets defined by the formula:

$$V(x,z) \ := \ \bigvee_{i=1}^{n} [w_i = 1 \wedge_{j \neq i} w_j = 0] \wedge \bigwedge_{i=1}^{n} [w_i = 1 \ \Rightarrow \ (P(V_i)(y_i) \wedge \wedge_{j \neq i} y_j = 0 \wedge V_i(x, y_i))]$$

$V(x, z)$ is the disjoint union of the members of S. **End of proof of Claim 2**

Now 1a follows from the two claims.

(1b) As we have said, by Lemma 2.2.4 there is an upper bound r on the number of irreducible components in a member of $A(x, y)$. So let $V(x, z)$ be the family found in Part 1a, and let us consider powers of $V(x, z)$. For each $1 \leq i \leq r$, let $V(x_i, z_i)$ be the family $V(x, z)$ expressed in tuples x_i, z_i. Let $x' = x_1 \ldots x_r$ and let $z' = z_1 \ldots z_r$. For each $1 \leq j \leq r$, let $V^j(x', z') := \prod_{i=1}^{j} V(x_i, z_i)$. Consider the family $C(x'x, z'y) := (\coprod_{j=1}^{r} V^j(x', z')) \times A(x, y)$. By the characterisation of the set of irreducible components of an algebraic set described in Part 1a we can define the sub-family $C^*(x'x, z'y)$ of $C(x'x, z'y)$ where if

- we work in $\tilde{K}$,
- $z'_0 y_0 \in P(C^*)(\tilde{K})$,
- in the disjoint union $\coprod_{j=1}^{r} V^j(x', z')$, z'_0 corresponds to a set $V^{j_0}(x', z'_0)$,

- $z'_0 = z_{10} \dots z_{r0}$,

then the set $\{V(x, z_{j0}) : \ 1 \leq j \leq j_0\}$ is the set of irreducible components of $A(x, y_0)$.

There is the natural map φ of families from $C^*(x'x, z'y)$ to $V(x, z)$ which is the composite of the projection map $z'y \mapsto z_1$ and the substitution $z_1 \mapsto z$. There is also the natural projection ψ of families from $C^*(x'x, z'y)$ to $A(x, y)$ where $z'y \mapsto y$. Then a member $V(x, z_0)$ is an irreducible component of the algebraic set $A(x, y_0)$ if and only if $\varphi^{-1}(z_0) \cap \psi^{-1}(y_0) \neq \emptyset$.

(1c) Firstly we may now construct a correspondence $C(yz)$ between the family $P(V^*)$ defined in 1b, and $P(A)$, where a pair $y_0 z_0 \in C(\tilde{K})$ if and only $V^*(x, z_0)$ is an irreducible component of $A(x, y_0)$. The result is not necessarily a map. We may then replace $P(V^*)$ with the disjoint union of the fibres, to obtain a proper map.

(2) This is now a direct application of Fact 2.2.3. □

2.3 Measurability for finite σ-degree σ-closed sets

NOTATION 2.3.1 In the remainder (K, σ) will be a large, uncountably saturated model of $ACFA$. By saturated enough, we note that we want points of algebraic sets and σ-closed sets which are generic over fields of definition to be realised in (K, σ). It follows that ω_1-saturation is sufficient. We shall be interested in the definability or definability without parameters of certain properties. From now, unless we specifically say otherwise, definability is meant in the sense of the language of difference rings. We shall deal with correspondences (see Section 1.4.1 of the Introduction). If $T(xz) \subseteq V(x) \times A(z)$ is a correspondence, we shall denote the projection to x by π_1 and the projection to z by π_2 .

2.3.1 Weak Quantifier Elimination for $ACFA$

There is a weak quantifier elimination form for definable sets in $ACFA$ (see [8] 1.5 and 1.6). That form allows us to view an arbitrary family $\theta(x, y)$ of sets as a family of finite unions of finite fibre projections of quantifier-free, definable sets. More specifically,

$$ACFA \models \quad \theta(x,y) \Longleftrightarrow \bigvee_{i=1}^{k} \exists t\ \theta_i(x,y,t) \tag{2.15}$$

where t is a single variable, $\theta_i = \theta_i\big(x, \sigma(x), \ldots, \sigma^m(x), y, \sigma(y), \ldots, \sigma^m(y), t, \sigma(t), \ldots, \sigma^m(t)\big)$ is a quantifier-free formula in the language of fields, and for any $(K,\sigma) \models ACFA$ and $(x_0y_0t_0) \in \theta_i(K)$, t_0 is algebraic in the sense of fields over $(x_0, \sigma(x_0), \ldots, \sigma^m(x_0), y_0, \sigma(y_0), \ldots, \sigma^m(y_0))$. In particular there is an $n \in \mathbb{N}$ such that any $\theta_i(x_0, y_0, t)$ has at most n solutions in t.

As in the pseudo-finite fields case [10], once we establish definable asymptotic estimates for finite σ-degree, σ-closed sets (see Section 1.4.2 for a definition of σ-degree and σ-closed sets), definable asymptotic estimates for quantifier-free definable sets of finite σ-degree will follow easily. Then using elimination form 2.15 and the method in [10] 3.7, definable asymptotic estimates for all first-order definable families of finite σ-degree sets will be obtained. The key is obtaining definable asymptotic estimates for σ-closed sets.

We also need the following notion of *algebraic dimension*:

DEFINITION 2.3.2 Let $\theta(x,y)$ be a family of sets definable in the language of difference rings. Suppose that $(K,\sigma) \models ACFA$ is ω_1-saturated. Let $y_0 \in P(\theta)(K)$ and let $Y = \mathrm{acl}_\sigma(y_0)$. Then we define $\dim_{\mathrm{alg}}(\theta(x,y_0)) = \max(\mathrm{tr.deg}(x/Y) : \ x \in \theta(K,y_0))$. We call $\dim_{\mathrm{alg}}(\theta(x,y_0))$ the algebraic dimension of $\theta(x,y_0)$. For a type p over $Y = \mathrm{acl}_\sigma(Y)$ with $|Y| < \omega_1$, we may similarly define $\dim_{\mathrm{alg}}(p) = \max(\mathrm{tr.deg}(x/Y) : x \in p(K))$. Then this definition of algebraic dimension simply extends the definition introduced in Section 1.4.1.

DEFINITION 2.3.3 Suppose that $\theta(x,y)$ is a $\emptyset$-definable family of σ-closed sets given by a set of polynomials

$$\{f_j(x, \sigma(x), \ldots, \sigma^l(x), y, \sigma(y), \ldots, \sigma^m(y)) : \ 1 \leq j \leq d\}$$

We now fix some $n \in \mathbb{N}$. We shall define some y-parameterised families of sets that may be obtained from $\theta(x,y)$. These families will be used in conjunction with the sub-family $\theta_n(x,y)$ of $\theta(x,y)$ of members of σ-degree n. Suppose that $x = x_0 = (x_{00}, x_{01}, \ldots x_{0k})$ is a tuple of length $k+1$. Let $N = \max\{n, l\}$.

- We let $x' = (x_0, x_1, \ldots, x_N)$, where for each $0 \leq i \leq N$, $x_i = (x_{i0}, x_{i1}, \ldots, x_{ik})$ is a tuple of length $k+1$. We define the σ-closed set $\mathrm{ext}_n(\theta)(x', y)$ as the set of zeroes of the polynomials:

$$\{f_j(x_0, \sigma(x_0), \ldots, \sigma^l(x_0), y, \sigma(y), \ldots, \sigma^m(y)) : \ 1 \leq j \leq d\} \ \cup \ \{x_i - \sigma^i(x_0) : \ 1 \leq i \leq N\} \tag{2.16}$$

  $\mathrm{ext}_n(\theta)(x', y)$ is a family of y-parameterised σ-closed sets in variables x'. We use the notation ext for 'extending', because we are extending the number of variables in θ so that there are variables for all σ-iterates up to N; for clarity, $\mathrm{ext}_n(\theta)(x', y)$ is an $\mathcal{L}_{\mathrm{diff}}$-set.

- Suppose $A(x, y)$ is a system of polynomials in the variable tuple x and whose parameters are the tuples of iterates $(y, \sigma(y), \ldots, \sigma^m(y))$; suppose that $A(x, y)$ specifically mentions *no* σ-iterates of x. Then for $(M, \sigma) \models ACFA$ and $y_0 \in P(\theta)(M)$, $A(x, y_0)$ is an algebraic set over the parameters $(y_0, \sigma(y_0), \ldots, \sigma^m(y_0))$. We call such an $A(x, y)$ algebraic in x. From $\mathrm{ext}_n(\theta)(x', y)$ we produce a definable set $\mathrm{alg}_n(\theta)(x', y)$ that is algebraic in x': the family $\mathrm{ext}_n(\theta)$ is written in terms of the tuple $(x_0, \sigma(x_0), \ldots, \sigma^N(x_0) \ ; \ x_1, x_2, \ldots, x_N)$. Then $\mathrm{alg}_n(\theta)$ is obtained as the zero set of the polynomials obtained by the substitution $\sigma^i(x_0) \mapsto x_i$ for each $0 \leq i \leq N$ in the defining polynomials of $\mathrm{ext}_n(\theta)(x', y)$. Thus $\mathrm{alg}_n(\theta)(x', y)$ is a family of y-parameterised sets in variable x'. We call its set of defining polynomials $\mathrm{EQ}_{\mathrm{alg}(\theta),n}(x', y)$. The (x', y) pair signifies only that we are writing the polynomials in these specific variables x' and y; of course, they can be substituted. Again, for clarity, $\mathrm{alg}_n(\theta)(x', y)$ is an $\mathcal{L}_{\mathrm{diff}}$-set. However, it may also be seen as an algebraic set in parameters which are y and a finite set of the σ-iterates of y.

- Let $V(x', y) = \mathrm{alg}_n(\theta)$, where $x' = (x_0, \ldots, x_N)$ and for each $0 \leq i \leq N$, $x_i = (x_{i0}, \ldots, x_{ik})$, as above. Let $V(z, v)$ be a copy of $V(x', y)$ in variable tuple z and parameter tuple v. Let $V^2(x'z, yv) = V(x', y) \times V(z, v)$. We construct a family of $y\sigma(y)$-parameterised correspondences inside the y-parameterised family $V^2(x'z, y\sigma(y))$. We call this family of correspondences $\mathrm{shift}_n(\theta)(x'z, y)$. The

polynomials whose zero set defines $\text{shift}_n(\theta)$ are

$$\text{EQ}_{\text{alg}(\theta),n}(x', y) \cup \text{EQ}_{\text{alg}(\theta),n}(z, \sigma(y)) \cup \{z_{ij} - x_{(i+1)j} \ : \ (0 \leq i \leq N-1,\ 0 \leq j \leq k)\}$$

This construction can be considered either locally at a family member $y_0 \in P(\theta)(M)$, or globally: $\text{shift}_n(\theta)(x'z, y)$ can be thought of as a single $\mathcal{L}_{\text{diff}} - 0$-definable formula in parameter y. Even though $\text{shift}_n(\theta)(x'z, y)$ is an $\mathcal{L}_{\text{diff}}$-set, like $\text{alg}_n(\theta)(x', y)$ it may also be seen as an algebraic set in parameters which are y and a finite set of the σ-iterates of y.

We denote the natural projection of $\text{shift}_n(\theta)$ onto the variable x' as π_1 and the projection onto z as π_2. We denote by π_θ the projection onto the variables coding the original data from $\theta(x, y)$: in the coordinates introduced above, π_θ is the projection onto coordinates $(x_{00}, x_{01}, \ldots, x_{0k})$. Similarly, we define $\pi_{\sigma(\theta)}$ to be the projection onto coordinates $(z_{00}, z_{01}, \ldots, z_{0k})$. The reader will observe that all these projections are 0-definable formulae in parameter y, in $\mathcal{L}_{\text{diff}}$.

- Lastly, we define the $\mathcal{L}_{\text{diff}}$-set $\triangle_n(\theta)(x'z, y)$ to be $\{(x', z) : \ (x', z) \in \text{shift}_n(\theta) \ \wedge \ z = \sigma(x')\}$

We shall call the sets $\text{ext}_n(\theta)$, $\text{alg}_n(\theta)$, $\text{shift}_n(\theta)$ and $\triangle_n(\theta)$ *the auxiliary sets for* $\theta_n(x, y)$.

EXAMPLE 2.3.4 We just give an example of a family of σ-closed sets and its auxiliary sets. Consider the family $\theta(x, y)$ defined by the σ-polynomial $y^3x - y\sigma^2(x) - 1 = 0$. When $y = 0$ this is empty, otherwise $\sigma^2(x) = y^2x - \frac{1}{y}$ and $\deg_\sigma(\theta(x, y))$=2. So let's calculate auxiliary sets for $\theta_2(x, y)$. In this case, in the notation of Definition 2.3.3, $k = 0$, $l = 2$, $n = 2$, and so $N = 2$.

$$\text{ext}_2(\theta) = \text{Zeroes}(\{y^3x_{00} - y\sigma^2(x_{00}) - 1 \ , \ x_{10} - \sigma(x_{00}),\ x_{20} - \sigma^2(x_{00})\})$$

$$\text{alg}_2(\theta) = \text{Zeroes}(\{y^3x_{00} - yx_{20} - 1\})$$

$$\text{shift}_2(\theta) = \text{Zeroes}(\{y^3x_{00} - yx_{20} - 1,\ (\sigma y)^3 z_{00} - (\sigma y)z_{20} - 1 \ , \ z_{00} = x_{10},\ z_{10} = x_{20}\})$$

$$\triangle_2(\theta) = \text{Zeroes}(\{y^3x_{00} - yx_{20} - 1,\ (\sigma y)^3 z_{00} - (\sigma y)z_{20} - 1 \ , \ z_{00} = x_{10},\ z_{10} = x_{20},\ z_{00} = \sigma(x_{00}),$$
$$z_{10} = \sigma(x_{10}),\ z_{20} = \sigma(x_{20})\})$$

REMARK 2.3.5 The auxiliary sets $\text{ext}_n(\theta)$, $\text{alg}_n(\theta)$, $\text{shift}_n(\theta)$ and $\triangle_n(\theta)$, were constructed from a set $\theta(x, y)$. We view this as taking the family $\theta(x, y)$ and canon-

ically producing new families: we have a uniform procedure valid for any model $(K, \sigma) \models ACFA$ and $y_0 \in P(\theta)(K)$, for taking $\theta(x, y_0)$ and producing the auxiliary sets in parameter y_0.

Formally, the auxiliary sets are in a different number of variables from $\theta(x, y)$; in Definition 2.3.3, $\text{ext}_n(\theta)$, $\text{alg}_n(\theta)$ were in variable x', and $\text{shift}_n(\theta)$, $\triangle_n(\theta)$ were in variable $x'z$. However, it is easier to adopt the convention of using x for the tuple of variables in the auxiliary sets $\text{ext}_n(\theta)$ and $\text{alg}_n(\theta)$, and using w (or xz where necessary) for the tuple of variables in $\text{shift}_n(\theta)$ and $\triangle_n(\theta)$. The reader should note that we shall interchange between w and xz to denote the variables in the latter auxiliary sets.

REMARK 2.3.6 We try to motivate Definition 2.3.3 and how we shall use it.

Our goal is to give uniform asymptotic estimates for a family $\theta(x, y)$ of σ-closed sets, but for simplicity let us assume we only want to estimate a single σ-closed set $\theta(x)$. Really, our only tool is Theorem 2.1.2, and we must make use of it somehow.

The first point is that Theorem 2.1.2 gives estimates for the $(x, \sigma(x))$ points of correspondences $W \subseteq V \times \sigma(V)$, so we must in some sense write $\theta(x)$ in terms of such a correspondence. Now $\theta(x)$ is a conjunction of algebraic equations in some parameters and in some set of iterates of x: for simplicity let us suppose that we have only one defining polynomial $f(x, \sigma(x), \ldots, \sigma^l(x))$. If we substitute $(x \mapsto x_0, \sigma(x) \mapsto x_1, \ldots, \sigma^l(x) \mapsto x_l)$, then this yields the algebraic equations $f(x_0, \ldots, x_l)$, defining a variety Y. This is essentially what the formula $\text{alg}_n(x, y)$ does. However, this is not so useful; $\theta(x)$ is sitting somewhere inside Y.

If we consider the σ-closed set sitting inside Y defined by the σ-polynomials:

$$f(x_0, \ldots, x_l) \ ; \ x_1 = \sigma(x_0), \ldots, x_l = \sigma^l(x_0) \tag{2.17}$$

then it is clear that the projection onto the first coordinate of this σ-closed set is $\theta(x)$, and also that that projection is a 1:1 map. Also, if $(x_0, \ldots, x_l)$ satisfies $f(x_0, \ldots, x_l) = 0$ then $\sigma(f)(\sigma(x_0), \ldots, \sigma(x_l)) = 0$. Then this means that the σ-closed set $S(x_0, \ldots, x_l, z_0, \ldots, z_l)$

defined by

$$f(x_0,\ldots,x_l)\ ;\ x_1=\sigma(x_0),\ldots,x_l=\sigma^l(x_0)\ ;\ \sigma(f)(z_0,\ldots,z_l)\ ;\ z_0=\sigma(x_0),\ldots,z_l=\sigma(x_l) \tag{2.18}$$

is also in bijection via the first coordinate projection with $\theta(x)$. Examining these equations it is easy to see that for each $1 \leq i \leq l-1$, $z_i = \sigma(x_i) = \sigma(\sigma^i(x_0)) = \sigma^{i+1}(x_0) = x_{i+1}$. It is then verified that we may equally well specify S with the equations:

$$f(x_0,\ldots,x_l)\ ;\ x_1=z_0,\ldots,x_l=z_{l-1}\ ;\ \sigma(f)(z_0,\ldots,z_l)\ ;\ z_0=\sigma(x_0),\ldots,z_l=\sigma(x_l) \tag{2.19}$$

S is now in a form to apply Hrushovski's estimates since it is clear by looking at the latter set of equations that if we write $x' = x_0,\ldots,x_l$ and $z' = z_0,\ldots,z_l$, then they define the $x'\sigma(x')$ points of the correspondence $C(x'z') \subseteq Y \times \sigma(Y)$ defined by

$$f(x_0,\ldots,x_l)\ ;\ x_1=z_0,\ldots,x_l=z_{l-1}\ ;\ \sigma(f)(z_0,\ldots,z_l) \tag{2.20}$$

This is essentially what we do in the construction of $\text{shift}_n(\theta(x,y))$. The lemma that treats bijections between the '$x\sigma(x)$' points of our constructed correspondences and the initial σ-closed sets follows; it is Lemma 2.3.7.

This is not the end of the story, because the auxiliary sets look more complicated than the construction above. The added complication again comes from the fact that we aim to apply Theorem 2.1.2. If we write our correspondences in variables $x'z'$, then it requires us to have finite fibre/quasi-finite fibre projections to x' and to z'. Essentially, this means that generically in our constructed correspondence $C(x'z')$, over the base, z' must be interalgebraic in the field-theoretic sense with x'. Now, there is a further point to make: because Hrushovski's estimates 2.1.2 hold for not necessarily closed subvarieties $W \subseteq V \times \sigma(V)$, it follows that in an application of them to $C(x'z')$, there will be a generic point of the correspondence of the form $z' = \sigma(x')$. So for this generic point, $\sigma(x')$ must be field interalgebraic with x' over the base of definition. Intuitively, for a σ-closed set $\theta(x)$ of σ-degree n, this happens only when we have at least n σ-iterates of x included in our constructed auxiliary correspondence ($\text{shift}_n(\theta(x,y))$. Indeed, this is verified in Lemma 2.3.8. This is the reason why our construction in Definition 2.3.3 includes $N = \max\{n,l\}$ σ-iterates of the original variables x.

LEMMA 2.3.7 *1. Let $(K, \sigma) \models ACFA$. Fix a family parameter $y_0 \in P(\theta_n)(K)$. Then π_θ is a definable bijection from $\triangle_n(\theta)(K, y_0)$ to $\theta(K, y_0)$.*

2. $\pi_{\sigma(\theta)}(\triangle_n(\theta)(K, y_0)) = \sigma(\theta(K, y_0))$.

PROOF 1. By inspection π_θ sends $\triangle_n(\theta)(K, y_0)$ into $\theta(K, y_0)$. On the other hand there is a natural inverse Φ to π_θ:

$$\Phi : \theta \mapsto \triangle_n(\theta) \ \ ; \ \ (x_{00}, x_{01}, \ldots, x_{0k}) \mapsto (x', \sigma(x')) \text{ where :}$$
$$x' = (x_{ij} : \ 0 \leq i \leq N, \ 0 \leq j \leq k) \text{ and } x_{ij} = \sigma^i(x_{0j}) \text{ for } 1 \leq i \leq N, \ 0 \leq j \leq k \quad (2.21)$$

2. The second statement is clear, by Part 1 and because on $\triangle_n(\theta)(K, y_0)$ we have $\pi_{\sigma(\theta)} = \sigma\pi_\theta$. □

LEMMA 2.3.8 *Suppose that (K, σ) is an ω_1-saturated model of $ACFA$ and $y_0 \in P(\theta_n(K))$. Let $w \in \triangle_n(\theta)(K, y_0)$, and let $v = \pi_\theta(w)$. Then*

(i) w and v are $\mathcal{L}_{\text{diff}}$-$\emptyset$-inter-definable over $\text{acl}_\sigma(y_0)$.

(ii) $\deg_\sigma(v/\text{acl}_\sigma(y_0)) = \deg_\sigma(w/\text{acl}_\sigma(y_0)) = \dim_{\text{alg}}(w/\text{acl}_\sigma(y_0))$.

(iii) $\dim_{\text{alg}}(w/\text{acl}_\sigma(y_0)) \leq n$, *and equality is obtained for some $w_0 = x_0 z_0$ where $x_0 z_0 \in K$. Also,* $\deg_\sigma(v/\text{acl}_\sigma(y_0)) \leq n$. *Further, for any points $w_1 \in \triangle_n(\theta)(K, y_0)$ and v_1 such that $\pi_\theta(w_1) = v_1$ and* $\deg_\sigma(v_1/\text{acl}_\sigma(y_0)) = n$, *then also* $\dim_{\text{alg}}(w_1/\text{acl}_\sigma(y_0)) = n$.

PROOF Let $Y = \text{acl}_\sigma(y_0)$.

(i) This follows directly from Lemma 2.3.7 (1).

(ii) The first equality follows from Part (i). Now it is clear that $\deg_\sigma(w/\text{acl}_\sigma(y_0)) \geq \dim_{\text{alg}}(w/\text{acl}_\sigma(y_0))$. Suppose that $\deg_\sigma(v/\text{acl}_\sigma(y_0)) = d$. Since $y_0 \in P(\theta_n(K))$, it follows that $d \leq n$. The first n σ-iterates of v appear in the point w. The rest of this part of the lemma then follows from the following claim:

Claim $\dim_{\text{alg}}(v, \sigma(v), \ldots, \sigma^{n-1}(v)) = d$.

Proof of Claim: On the one hand some finite collection of σ-iterates of v has algebraic dimension d over Y. By applying an appropriate power of σ, we may assume that there is a minimal e such that the collection of iterates $C = \{\sigma^i(v) : 0 \leq i \leq e\}$ has algebraic dimension d over Y. It is also clear that if there is some $f \in \mathbb{N}$ and $\sigma^{f+1}(v) \in \text{acl}_{\text{alg}}(\{\sigma^j(v) : 0 \leq j \leq f\}, Y)$, then for all $k > 0$, $\sigma^{f+k}(v) \in \text{acl}_{\text{alg}}(\{\sigma^j(v) : 0 \leq j \leq f, \}, Y)$. This implies that if $e > n-1$, then $\deg_\sigma(v/\text{acl}_\sigma(y_0)) > n$, and since $n \geq d$ we have a contradiction. So $e \leq n-1$, and we are done. **End of proof of claim and lemma**

(iii) Since $y_0 \in P(\theta_n)(K)$, for any $v \in \theta(K, y_0)$ we have that $\deg_\sigma(v/Y) \leq n$, and further, equality must be attained for some v_0. Then Part (iii) now follows from Part (ii) and Part (i).

COROLLARY 2.3.9 *Let $\theta(x, y)$ be a family of σ-closed sets of σ-degree n. Let $V(x'z, y) \subseteq \triangle_n(\theta)(x'z, y)$ be a family of σ-closed sets. Then $V(x'z, y)$ may be uniformly stratified into finitely many sub-families $\{V_{n,i} : 1 \leq i \leq n\}$ such that over all ω_1-saturated $(K, \sigma) \models ACFA$, for $y_0 \in P(V_{n,i})(K)$ we have $\dim_{\text{alg}}(V(x'z, y_0)) = i$.*

PROOF Let $y_0 \in P(V)(K)$. By Lemma 2.3.8 Part (ii) and Lemma 2.3.7 we have $\dim_{\text{alg}}(V(x'z, y_0))$ =$\deg_\sigma(V(x'z, y_0))$. But then σ-degree is uniformly definable over the family $V(x'z, y)$. □

LEMMA 2.3.10 *Suppose that $\theta(x, y)$ is a family of σ-closed sets, $(K, \sigma) \models ACFA$ is ω_1-saturated and $y_0 \in P(\theta_n)(K)$. Suppose that $V(x'z) \subseteq \text{shift}_n(\theta)(x'z, y_0)$ is a variety of dimension d defined over $\text{acl}_\sigma(y_0)$ and that $V(x'z)$ contains a generic point x_0z_0 over $\text{acl}_\sigma(y_0)$, such that $z_0 = \sigma(x_0)$. Suppose $f(x', z)$ is a polynomial over $\text{acl}_\sigma(y_0)$ such that $\dim_{\text{alg}}(V(x'z) \backslash \text{Zeroes}(f(x', z))) = \dim_{\text{alg}}(V(x'z))$. Then π_1 and π_2 are both generically finite fibre projections on V. Also, $\overline{\pi_2(V \backslash \text{Zeroes}(f))} = \sigma(\overline{\pi_1(V \backslash \text{Zeroes}(f))})$.*

PROOF Let $Y = \text{acl}_\sigma(y_0)$.

Claim: x_0 and z_0 are field inter-algebraic over Y.

Proof of Claim: Suppose that $x_0 = (x_{ij} : 0 \leq i \leq N \ ; \ 0 \leq j \leq k)$ and $z_0 = (z_{ij} : 0 \leq i \leq N \ ; \ 0 \leq j \leq k)$. For $0 \leq i \leq N$, let $x^i = \{x_{ij} : 0 \leq j \leq k\}$ and let $z^i = \{z_{ij} : 0 \leq j \leq k\}$. Then purely in terms of sets of elements: $z_0 \backslash x_0 = \sigma(x^N)$ and $x_0 \backslash z_0 = x^0$.

First we show that $z_0 \in \mathrm{acl}_{\mathrm{alg}}(Y, x_0)$. It suffices to show that $\sigma(x^N) \in \mathrm{acl}_{\mathrm{alg}}(Y, x_0)$. We now argue similarly to previous lemmas: if $\sigma(x^i) \in \mathrm{acl}_{\mathrm{alg}}(Y, x^0, \ldots, x^i)$, then inductively, for all $j \geq 0$ we have $\sigma^j(x^i) \in \mathrm{acl}_{\mathrm{alg}}(Y, \sigma^j(x^0), \ldots, \sigma^j(x^i)) \subseteq \mathrm{acl}_{\mathrm{alg}}(Y, x^0, \ldots, x^i)$. But now by 2.3.8 Part (iii) $\dim_{\mathrm{alg}}(x_0 z_0 / y) \leq n$, and so there must be some $i_0 \leq n-1$ such that $x^{i_0+1} = \sigma(x^{i_0}) \in \mathrm{acl}_{\mathrm{alg}}(Y, x^0, \ldots, x^{i_0})$. Now $\sigma(x^N) = \sigma^{N-i_0+1}(x^{i_0})$, and so $\sigma(x^N) \in \mathrm{acl}_{\mathrm{alg}}(Y, x^0, \ldots, x^{i_0}) \subseteq \mathrm{acl}_{\mathrm{alg}}(Y, x_0)$.

Next we show that $x_0 \in \mathrm{acl}_{\mathrm{alg}}(Y, z_0)$. This is almost identical to the converse we just proved: it suffices to show that $x^0 \in \mathrm{acl}_{\mathrm{alg}}(Y, z_0)$. For $i \geq 0$, if $\sigma^{-1}(z^{N-i}) \in \mathrm{acl}_{\mathrm{alg}}(Y, z^N, \ldots, z^{N-i})$, then inductively, for all $j \geq 0$ we have $\sigma^{-j}(z^{N-i}) \in \mathrm{acl}_{\mathrm{alg}}(Y, \sigma^{-j}(z^N), \ldots, \sigma^{-j}(z^{N-i})) \subseteq \mathrm{acl}_{\mathrm{alg}}(Y, z^N, \ldots, z^{N-i})$. Again, since $\dim_{\mathrm{alg}}(x_0 z_0 / y) \leq n$ there must be some $i_1 \leq n-1$ such that $z^{N-i_1-1} = \sigma^{-1}(z^{N-i_1}) \in \mathrm{acl}_{\mathrm{alg}}(Y, z^N, \ldots, z^{N-i_1})$. Now $x^0 = \sigma^{i_1-(1+N)}(z^{N-i_1})$, and so $x^0 \in \mathrm{acl}_{\mathrm{alg}}(Y, z^N, \ldots, z^{N-i_1}) \subseteq \mathrm{acl}_{\mathrm{alg}}(Y, z_0)$. **End of proof of claim**

Since V is defined over Y, we deduce that x_0 and z_0 each have transcendence degree d over Y, and $x_0 z_0 \in V \backslash \mathrm{Zeroes}(f)$. Also, it follows from the claim that π_1 and π_2 are generically finite fibre projections, and furthermore,

$$\dim_{\mathrm{alg}}(\overline{\pi_1(V \backslash \mathrm{Zeroes}(f))}) = \dim_{\mathrm{alg}}(\overline{\pi_2(V \backslash \mathrm{Zeroes}(f))}) = d$$

Since $V(x'z)$ is irreducible and defined over Y, we deduce that both $\overline{\pi_1(V \backslash \mathrm{Zeroes}(f))}$ and $\overline{\pi_2(V \backslash \mathrm{Zeroes}(f))})$ are also irreducible and defined over Y. It follows that (i) x_0 is generic in $\overline{\pi_1(V \backslash \mathrm{Zeroes}(f))}$ over Y, and (ii) z_0 is generic in $\overline{\pi_2(V \backslash \mathrm{Zeroes}(f))}$ over Y. From (i) it follows that $\sigma(x_0) = z_0$ is generic in $\sigma(\overline{\pi_1(V \backslash \mathrm{Zeroes}(f))})$ over $\sigma(Y) = Y$. So z_0 is generic in two irreducible varieties defined over Y: $\overline{\pi_2(V \backslash \mathrm{Zeroes}(f))}$ and $\sigma(\overline{\pi_1(V \backslash \mathrm{Zeroes}(f))})$. We deduce $\overline{\pi_2(V \backslash \mathrm{Zeroes}(f))} = \sigma(\overline{\pi_1(V \backslash \mathrm{Zeroes}(f))})$. $\square$

PROPOSITION 2.3.11 *Let $\theta(x,y)$ be a $\emptyset$-definable family of σ-closed sets of σ-degree n. There exists $r \in \mathbb{N}$ and a finite set $\{(B_j(w,v), f_j(w,v)) : 1 \leq j \leq r\}$ of 0-definable families of algebraic sets $B_j(w,v)$ and polynomials $f_j(w,v)$ with the following properties:*

For some $k \in \mathbb{N}$ there is a tuple of tuples $v = (v_1, v_2, \ldots, v_{2k+1})$, where each v_i is a tuple of the same length as y. For any ω_1-saturated model $(K,\sigma) \models ACFA$ and $y_0 \in P(\theta(K))$ let $v_0 = (\sigma^{-k}(y_0), \sigma^{1-k}(y_0), \ldots, \sigma^k(y_0))$. Then there is a subset $J \subseteq \{1,2,\ldots,r\}$ such that the following hold:

1. *$\triangle_n(\theta)(w,y_0) \subseteq \bigcup_{j\in J} B_j(w,v_0) \subseteq \mathrm{shift}_n(\theta)(w,y_0)$;*
2. *For each $j \in J$, $\dim_{\mathrm{alg}}(B_j(w,v_0)) = \dim_{\mathrm{alg}}(B_j(w,v_0) \backslash \mathrm{Zeroes}(f_j(w,v_0)))$.*
3. *For each $j \in J$, $B_j(w,v_0)$ contains a generic point over $\mathrm{acl}_\sigma(y_0)$ of the form $x_0 z_0$ where $z_0 = \sigma(x_0)$;*
4. *For each $j \in J$, π_2 is a quasi-finite projection on $B_j(w,v_0) \backslash \mathrm{Zeroes}((f_j(w,v_0))$.*
5. *There is a $j \in J$ such that $\dim_{\mathrm{alg}}(B_j(w,v_0)) = n$.*

PROOF Let $C := C(y) := \{\sigma^i(y) : i \in \mathbb{Z}\}$. Consider the list $\mathbb{L}_{\mathrm{alg}}$ of algebraic sets in variable w and parameters in C:

$$\mathbb{L}_{\mathrm{alg}} = \{C - \text{parameterised algebraic sets in variables } w\}$$

and the list $\mathbb{L}_{\mathrm{poly}}$ of polynomials in variable w and parameters in C:

$$\mathbb{L}_{\mathrm{poly}} = \{C - \text{parameterised polynomials in variables } w\}$$

Let $(B,f) \in \mathbb{L}_{\mathrm{alg}} \times \mathbb{L}_{\mathrm{poly}}$. We define $\mathrm{BAD}_{(B,f)}(w,y)$ by

$$\mathrm{BAD}_{(B,f)}(w,y) := \quad P(\theta)(y) \ \wedge \ \triangle_n(\theta)(w,y) \ \wedge \ (\Theta_{(B,f)}(w,y) \ \Rightarrow \ \Psi_{(B,f)}(w,y))$$

where

$$\begin{aligned}\Theta_{(B,f)}(w,y) := \qquad & v = (\sigma^{-k}(y), \sigma^{1-k}(y), \ldots, \sigma^k(y)) \ \wedge \\ & B(w,v) \ \wedge \ (\forall t)[B(t,v) \ \Rightarrow \ \mathrm{shift}_n(\theta)(t,y)] \ \wedge \\ & (\forall s)(s \in \pi_2(B(w,v) \backslash \mathrm{Zeroes}(f(w,v))) \Rightarrow \dim_{\mathrm{alg}}(\pi_2^{-1}(s)) = 0) \ \wedge\end{aligned}$$

$$\dim_{\text{alg}}(B(w,v)\backslash \text{Zeroes}(f(w,v))) = \dim_{\text{alg}}(B(w,v))$$

$$\Psi_{(B,f)}(w,y) := \quad v = (\sigma^{-k}(y), \sigma^{1-k}(y), \ldots, \sigma^{k}(y)) \ \wedge$$
$$\dim_{\text{alg}}(B(w,v) \cap \triangle_n(\theta)(w,y)) < \dim_{\text{alg}}(B(w,v))$$

Here, the $\dim_{\text{alg}}$ notation is from 2.3.2. Notice that $\text{BAD}_{(B,f)}(w,y)$ is definable in the language of difference rings by Corollary 2.3.9.

Now consider the collection of formulae $D(w,y) = \{\text{BAD}_{(B,f)}(w,y) : \ (B,f) \in \mathbb{L}_{\text{alg}} \times \mathbb{L}_{\text{poly}}\}$. We shall suppose D is a consistent collection of formulae, derive a contradiction, and then apply compactness to deduce parts 1 to 4 of the lemma.

If D is a consistent set of formulae, then extend D to a type $p(w,y)$, and choose $(w_0,y_0) \in K$ such that $(K,\sigma) \models p(w_0,y_0)$. Let $C_0 = \{\sigma^i(y_0) : \ i \in \mathbb{Z}\}$ and let $Y_0 = \text{acl}_\sigma(y_0)$. Let L_0 be the locus of w_0/Y_0, and let B_0 be the C_0-definable algebraic set which is the union of the conjugate varieties of L_0 over C_0. Since $\text{shift}_n(\theta)(w,y_0)$ may be considered as an algebraic set defined over C_0, it follows that $B_0 \subseteq \text{shift}_n(\theta)$. Since w_0 is generic in B_0 over Y_0, we deduce that $\dim_{\text{alg}}(B_0 \cap \triangle_n(\theta)(w,y_0)) = \dim_{\text{alg}}(B_0)$. Let $w = xz$. From Lemma 2.3.10, the projections π_1 and π_2 on $L_0(xz)$ are of generically finite fibre. Thus the projections π_1 and π_2 on $B_0(xz)$ are also of generically finite fibre. Since π_2 is generically finite, consider $S = \pi_2^{-1}(\{z \in \pi_2(B_0) : \ \dim_{\text{alg}}(\pi_2^{-1}(z)) > 0\})$. Then $\bar{S} \subseteq B_0$, has $\dim_{\text{alg}}(\bar{S}) < \dim_{\text{alg}}(B_0)$, and is defined over C_0. So there is polynomial f, with $\text{Zeroes}(f)$ of codimension 1 in B_0, with f defined over C_0, and such that $\bar{S} \subseteq \text{Zeroes}(f) \cap B_0$. This shows that $(K,\sigma) \not\models \text{BAD}_{(B_0,f)}(w_0,y_0)$, and this is a contradiction.

Thus we may deduce

$$\Big[\ P(\theta)(y) \ \wedge \ \triangle_n(\theta)(w,y) \ \wedge \bigwedge_{(B,f)\in \mathbb{L}_{\text{alg}}\times\mathbb{L}_{\text{poly}}} (\Theta_{(B,f)}(w,y) \Rightarrow \ \Psi_{(B,f)}(w,y))\ \Big] \vdash \perp \quad (2.22)$$

Applying compactness to 2.22 and manipulating the resulting formula using elementary logic, we obtain:

$$\text{For some } r \in \mathbb{N} \left[P(\theta)(y) \ \wedge \ \triangle_n(\theta)(w,y) \ \wedge \ \bigwedge_{j=1}^{r} (\Theta_{(B_j,f_j)}(w,y) \Rightarrow \ \Psi_{(B_j,f_j)}(w,y)) \right] \vdash \bot$$

$$\vdash \ [P(\theta)(y) \ \wedge \ \triangle_n(\theta)(w,y)] \ \Rightarrow \ \neg[\bigwedge_{j=1}^{r} (\Theta_{(B_j,f_j)}(w,y) \Rightarrow \ \Psi_{(B_j,f_j)}(w,y))]$$

$$\vdash \ [P(\theta)(y) \ \wedge \ \triangle_n(\theta)(w,y)] \ \Rightarrow \ \bigvee_{j=1}^{r} \neg(\Theta_{(B_j,f_j)}(w,y) \Rightarrow \ \Psi_{(B_j,f_j)}(w,y))$$

$$\vdash \ \forall yw([P(\theta)(y) \ \wedge \ \triangle_n(\theta)(w,y)] \ \Rightarrow \ \bigvee_{j=1}^{r} \Theta_{(B_j,f_j)}(w,y) \wedge \ \neg(\Psi_{(B_j,f_j)}(w,y)))$$

Parts 1-4 in the statement of the proposition are exactly the last formula written in $\mathcal{L}_{\text{diff}}$. Now by Lemma 2.3.8, there is $w_0 \in \triangle_n(\theta)(K, y_0)$ such that tr.deg(w_0/Y)=n. So it follows that some $B_j(w, v_0)$ has algebraic dimension at least n, and has a generic point in $\triangle_n(\theta)(K, y_0)$. But by Lemma 2.3.8, $n = \max_{w \in \triangle_n(\theta)(K,y_0)}(\text{tr.deg}(w/Y))$. So $\dim_{\text{alg}}(B_j(w, v_0)) = n$. □

LEMMA 2.3.12 *Suppose $(K, \sigma) \models ACFA$, $y_0 \in P(\theta_n)(K)$ and $B_j = B_j(w, v_0)$, $1 \leq j \leq r$, are as in Proposition 2.3.11. Let $V_{j_1} \subseteq B_{j_1}$ and $V_{j_2} \subseteq B_{j_2}$ be two different irreducible varieties, each of dimension $\leq n$, and each with a generic point over $\text{acl}_\sigma(y_0)$ of the form $(x, \sigma(x))$. Let $\triangle V = \{xz : \ xz \in V_{j_1} \cap V_{j_2} \ \wedge \ z = \sigma(x)\}$. Then $\deg_\sigma(\triangle V) < n$.*

PROOF Let $Y = \text{acl}_\sigma(y_0)$. Suppose $\deg_\sigma(\triangle V) \geq n$. Then we may pick $w_0 \in \triangle V$ such that $\deg_\sigma(w_0/Y) \geq n$. But $w_0 \in \triangle_n(\theta)(K, y_0)$, and thus by Lemma 2.3.8, $\dim_{\text{alg}}(w_0/Y) = n$. But $w_0 \in V_{j_1} \cap V_{j_2}$ and since V_{j_1} and V_{j_2} are irreducible, not equal and of dimension $\leq n$, $\dim_{\text{alg}}(V_{j_1} \cap V_{j_2}) < n$. This contradiction proves the lemma. □

PROPOSITION 2.3.13 *Let $\theta(x, y)$ be a family of σ-closed sets of σ-degree n. Suppose that $\{B_j(w, v), \ f_j(w, v) : \ 1 \leq j \leq r\}$ is as in 2.3.11. Suppose that $(K, \sigma) \models ACFA$ is ω_1-saturated and that $y_0 \in P(\theta_n)(K)$. Let the triple of natural numbers $(n_{\text{comp}}, n_{\text{deg}}, n_{\text{ins}})(y_0)$ denote the following:*

In the collection of irreducible components of the algebraic sets $B_j(w, v_0)$ $(1 \leq j \leq r)$ there are exactly n_{comp} distinct components with the following property: if we label

one as V, then $V\backslash\text{Zeroes}(f_j(w, v_0))$ has dimension n with a generic point of the form $(x, \sigma x)$, and on $V\backslash\text{Zeroes}(f_j(w, v_0))$ the projection π_1 is of degree n_{deg} and π_2 is a quasi-finite projection of inseparable degree n_{ins}.

Over all ω_1-saturated models $(K, \sigma) \models ACFA$ and $y_0 \in P(\theta_n)(K)$, there is a finite set of different triples $(n_{\text{comp}}, n_{\text{deg}}, n_{\text{ins}})(y_0)$. Every $\theta(x, y_0)$ has a non-empty collection of triples. $\theta_n(x, y)$ can be uniformly stratified according to the collection of triples of a member $\theta(x, y_0)$.

PROOF Let (K, σ) be an ω_1-saturated model of $ACFA$ and let $y_0 \in P(\theta_n(K))$. By Proposition 2.3.11 there is a j with $1 \leq j \leq r$ such that $B_j(xz, v_0)$ has an irreducible component $V(xz)$ of dimension n, and $V(xz)$ has a generic point over $\text{acl}_\sigma(y_0)$ of the form $z_0 = \sigma(x_0)$.

Since $B_j(xz, v_0)\backslash\text{Zeroes}(f_j(w, v_0))$ has π_2 quasi-finite, then so too does $V(xz)\backslash\text{Zeroes}(f_j(w, v_0))$. Furthermore, by Lemma 2.3.10 both projections π_1 and π_2 on V are generically of finite fibre. Thus the collection of triples for $\theta(xz, y_0)$ is non-empty.

Let $V(xz, v)$ be any family of absolutely irreducible algebraic sets. Then the set $S_{\text{generic}} := \{v : \dim_{\text{alg}}(V(xz, v)) = \dim_{\text{alg}}(V(xz, v) \cap \triangle_n(\theta)(xz, v))\}$ is uniformly definable as a corollary of Corollary 2.3.9. Each member of S_{generic} has a generic point of the form $z = \sigma(x)$, so we may apply Lemma 2.3.10. Suppose now the projections π_1 and π_2 on any member $V(xz, v_0)$ of a family $V(xz, v)$ are of generically finite fibre. By Lemma 2.2.11, $V(xz, v)$ can be uniformly stratified by the degree of π_1 or by the inseparable degree of π_2. By 2.2.2, $V(xz, v)$ may be simultaneously, uniformly stratified according to all these properties. The last statement of the lemma then follows from 2.2.14 Part 2.

Finally, since all the stratifications used stratify families into finitely many sub-families, there can only be finitely many triples. □

We now prove the main Theorem 2.1.1 for families of σ-closed sets. It will make strong use of Theorems 2.1.2 and 2.1.3:

THEOREM 2.3.14 *Let θ be a $\emptyset$-definable family of σ-closed sets. Then $\theta_n(x,y)$ can be partitioned into finitely many sub-families $\theta_{n,\mu_i}(x,y)$, ($\mu_i \in \mathbb{R}^+$), such that the following holds:*

There is a constant $C \in \mathbb{R}^+$ such that for all pairs of the form $(\tilde{\mathbb{F}}_p, \mathrm{Frob}^k)$ but finitely many, for any $y_0 \in \tilde{\mathbb{F}}_p$

$$P(\theta_{n,\mu_i})(y_0) \;\Rightarrow\; \big|\; |\,\theta(x,y_0)\,| \;-\; \mu_i p^{kn}\;\big| \leq C p^{k(n-\frac{1}{2})}$$

Here, we allow p to run over all primes and k to run over the natural numbers.

Proof We begin by defining the sub-families $\theta_{n,\mu_i}(x,y) = \theta_n(x,y) \wedge P(\theta_{n,\mu_i})(y)$. Let $N = \{(n_{\mathrm{comp}_l}, n_{\mathrm{deg}_l}, n_{\mathrm{ins}_l}) : 1 \leq l \leq m\}$ be a collection of triples of natural numbers. By Lemma 2.3.13, there is a finite set of such collections of triples $D = \{N_1, N_2, \ldots, N_e\}$, such that for any ω_1-saturated $(K,\sigma) \models ACFA$ and $y_0 \in P(\theta_n)(K)$, the collection of triples associated to $\theta(x,y_0)$ in the stratification defined in 2.3.13 is N_t, for some $1 \leq t \leq e$. Thus, by Proposition 2.3.13, $\theta_n(x,y)$ may be stratified into sub-families $\theta_{n,N_t}(x,y) = \theta_n(x,y) \wedge P(\theta_{n,N_t})(y)$. We define the function μ on finite collections of triples, and its definition on $N = \{(n_{\mathrm{comp}_l}, n_{\mathrm{deg}_l}, n_{\mathrm{ins}_l}) : 1 \leq l \leq m\}$ is

$$\mu(N) = \sum_{l=1}^{m} n_{\mathrm{comp}_l} \cdot \frac{n_{\mathrm{deg}_l}}{n_{\mathrm{ins}_l}}$$

We may define an equivalence relation $\approx$ on D by $N_t \approx N_s$ if and only if $\mu(N_s) = \mu(N_t)$. Let D_t be the $\approx$-equivalence class of N_t. For each $\approx$-equivalence class D_t we define a sub-family θ_{n,μ_t} by setting $\mu_t = \mu(N_t)$ and $P(\theta_{n,\mu_t})(y) := \bigvee_{N_s \in D_t} P(\theta_{n,N_s})(y)$.

Now we prove the theorem with respect to this choice of sub-families $\theta_{n,\mu_t}(x,y)$.

Recall Theorem 2.1.3: $ACFA$ is the almost theory of the set of difference fields $S = \{(\tilde{\mathbb{F}}_p, \mathrm{Frob}^k) : \; p \text{ a prime}, \; k \in \mathbb{N}\}$. Thus we have the principle that any first-order formula which holds for all ω_1-saturated models of $ACFA$, holds for all but finitely many members of S. The reader will notice that Propositions 2.3.11, 2.3.13 and Lemma 2.3.10 proved results for *all* ω_1-saturated models of $ACFA$, and so we begin applying this principle to that lemma and those two propositions:

Let $\{B_j(w,v),\ f_j(w,v) :\ 1 \leq j \leq r\}$ be as in 2.3.11. We deduce that for all $(K,\sigma) \in S\backslash E_\theta$, where E_θ is a finite collection of exceptional difference fields depending only on θ, the following hold:

1. $P(\theta_n)(K)$ is stratified into the sub-families $P(\theta_{n,N_t})(K)$. Also, $P(\theta_n)(K)$ is stratified into the sub-families $P(\theta_{n,\mu_t})(K)$.

2. Suppose now $y_0 \in P(\theta_{n,\mu_i})(K)$. Then there is $t \in \{1,2,\ldots,e\}$ such that $y_0 \in P(\theta_{n,N_t})(K)$, and $\mu(N_t) = \mu_i$. Without loss of generality we shall write $N_t = N = \{(n_{\mathrm{comp}_l}, n_{\mathrm{deg}_l}, n_{\mathrm{ins}_l}) :\ 1 \leq l \leq m\}$ and $\mu_i = \mu$. Let $v_0 = (\sigma^{-k}(y_0), \sigma^{1-k}(y_0), \ldots, \sigma^k(y_0))$, where this k is as in Proposition 2.3.11. Then there is a subset $J \subseteq \{1,2,\ldots,r\}$ such that

   (a) $\theta(K,y_0)$ is in $\emptyset$-definable bijection with $\triangle_n(\theta)(K,y_0)$.

   (b) $\triangle_n(\theta)(K,y_0) \subseteq \bigcup_{j\in J} B_j(K,v_0)$;

   (c) For each $j \in J,\ B_j(K,v_0) \subseteq \mathrm{shift}_n(\theta)(K,y_0)$;

   (d) For each $j \in J$, π_2 is a quasi-finite projection on $B_j(K,v_0)\backslash\mathrm{Zeroes}(f_j(K,v_0))$, and π_1 is a generically finite fibre projection on $B_j(K,V_0)$.

   (e) For each $j \in J$, $\dim_{\mathrm{alg}}(B_j(K,v_0)\backslash\mathrm{Zeroes}(f_j(K,v_0))) = \dim_{\mathrm{alg}}(B_j(K,v_0))$.

3. It follows from Lemma 2.2.14 and an application of Lemma 2.2.4 that there is a finite set of $\emptyset$-definable families of algebraic sets $\{W_k(w,u) :\ 1 \leq k \leq h\}$ such that for any algebraically closed field $\tilde{K}$, and j such that $1 \leq j \leq r$, and $v_1 \in P(B_j)(\tilde{K})$, the irreducible components of $B_j(w,v_1)$ are all of the form $W_k(w,u_1)$ for some $1 \leq k \leq h$ and $u_1 \in \tilde{K}$. Also, there is $G \in \mathbb{N}$ such that over all $\tilde{K}$ and for any selection of parameters $\{v_j \in P(B_j)(\tilde{K}) :\ 1 \leq j \leq r\}$, the total number of irreducible components in the collection of algebraic sets $\{B_j(w,v_j) :\ 1 \leq j \leq r\}$ is less than G.

   Returning to the specific case outlined in Item 2, we deduce (making additional use of Lemma 2.3.10 and Proposition 2.3.13) that there is a finite set of varieties $\{V_i(w,u_i) :\ 1 \leq i \leq g\}$ such that each $V_i(w,u_i)$ is of the form $W_k(w,u_i)$ for some $1 \leq k \leq h$, and $u_i \in K$, and

(a) $\triangle_n(\theta)(K, y_0) \subseteq \bigcup_{i=1}^{g} V_i(K, u_i)$;

(b) For each $1 \leq i \leq g$, $V_i(K, u_i) \subseteq \text{shift}_n(\theta)(K, y_0)$;

(c) For each $1 \leq i \leq g$, there is a j such that $1 \leq j \leq r$ and π_2 is a quasi-finite projection on $V_i(K, u_i) \backslash \text{Zeroes}(f_j(w, v_0))$, and π_1 is a generically finite fibre projection on $V_i(K, u_i)$. Also, $\dim_{\text{alg}}(V_i(K, u_i) \backslash \text{Zeroes}(f_j(w, v_0)))$ $=\dim_{\text{alg}}(V_i(K, u_i))$.

(d) For each $1 \leq i \leq g$, $\overline{\pi_2(V_i(w, u_i) \backslash \text{Zeroes}(f_j(w, v_0)))} = \sigma\overline{(\pi_1(V_i(w, u_i) \backslash \text{Zeroes}(f_j(w, v_0))))}$. This is specifically because of Lemma 2.3.10.

(e) For each $1 \leq l \leq m$ there are exactly n_{comp_l} numbers $i \in \{1, 2, \ldots, g\}$ such that $\dim_{\text{alg}}(V_i(w, u_i)) = n$, $V_i(w, u_i)$ has a generic point of the form $(x, \sigma(x))$, and $V_i(w, u_i)$ has π_1 of degree n_{deg_l} and π_2 of inseparable degree n_{ins_l}. Furthermore, every $V_i(w, u_i)$ such that $\dim_{\text{alg}}(V_i(w, u_i)) = n$ is counted exactly once in this way.

We now need to examine some consequences of Theorem 2.1.2:

Let us work with the families $W_k(w, u)$ $(1 \leq k \leq h)$ defined in Item 3. For given k, we may uniformly define the sub-family of $W_k(w, u)$ where $W_k(w, u)$ is absolutely irreducible, both π_1 and π_2 are generically finite fibre projections, and by Lemma 2.2.11 we may stratify the resulting sub-family by pairs (deg, ins), where deg is the degree of π_1 and ins the inseparable degree of π_2. Repeating this procedure for each $1 \leq k \leq h$, we obtain a finite set of such pairs (deg, ins). For each such pair we may consider the ratio $\frac{\text{deg}}{\text{ins}}$. Let μ_{low} be the minimum such ratio and μ_{high} the maximum such ratio.

Let us apply Hrushovski's correspondence estimates to a family $W_k(w, u)$. Consider an arbitrary $(\tilde{\mathbb{F}}_p, \text{Frob}^\gamma) \in S$ and $q = p^\gamma$. Suppose $u_1 \in \tilde{\mathbb{F}}_p$. Suppose that f is a polynomial such that $\dim_{\text{alg}}(W_k(w, u_1) \backslash f) = \dim_{\text{alg}}(W_k(w, u_1))$, and $W_k(w, u_1)$ is irreducible of dimension d with π_1 of generically finite fibre and degree δ, and π_2 quasi-finite of inseparable degree δ' on $W_k(w, u_1) \backslash \text{Zeroes}(f)$. We define $\triangle_q(W_k \backslash \text{Zeroes}(f)) = \{xz \in W_k \backslash \text{Zeroes}(f) : \ z = x^q\}$. Then by 2.1.2 there is a constant $C_k \in \mathbb{R}^+$ such that:

$$\left| |\triangle_q(W_k \backslash \text{Zeroes}(f))(\tilde{\mathbb{F}}_p)| - \frac{\delta}{\delta'} q^d \right| \leq C_k q^{d-1/2} \tag{2.23}$$

We may also deduce a cruder estimate; we express this for $V_i \backslash \text{Zeroes}(f_j)$ where f_j is as in 3c above, and V_i is of the form $W_k(w, u_1)$ as above:

$$\mu_{\text{low}} q^d - C_k q^{d-\frac{1}{2}} \leq |\triangle_q(V_i \backslash \text{Zeroes}(f_j))| \leq \mu_{\text{high}} q^d + C_k q^{d-\frac{1}{2}} \tag{2.24}$$

Inductive Proof of the theorem

The inductive hypothesis, which is on $n \in \mathbb{N}$, is:

Suppose that $\varphi(w, v)$ is a 0-definable family of σ-closed sets such that if (K, σ) is any ω_1-saturated model of $ACFA$ and $v_1 \in P(\varphi)(K)$, then $\deg_\sigma(\varphi(w, v_1)) < n$. Then the conclusion of the theorem is true for the family $\varphi(w, v)$.

We begin by applying the inductive hypothesis to get a rough estimate of cardinality for sets of σ-degree less than n. Suppose that $\varphi(w, v)$ is a 0-definable family of σ-closed sets. Suppose that if (K, σ) is any ω_1-saturated model of $ACFA$ and $v_1 \in P(\varphi)(K)$, then $\deg_\sigma(\varphi(w, v_1)) < n$. Then there is $m_\varphi \in \mathbb{R}^+$ such that for all $(\tilde{\mathbb{F}}_p, \text{Frob}^\gamma) \in S$ and $v_2 \in P(\varphi)(\tilde{\mathbb{F}}_p)$,

$$|\varphi(\tilde{\mathbb{F}}_p, v_2)| \leq m_\varphi q^{n-1} \quad (\text{where } q = p^\gamma) \tag{2.25}$$

Consider the family $\varphi_{\text{int},k_1,k_2} = W_{k_1}(w, u_{k_1}) \cap W_{k_2}(w, u_{k_2})$, where $1 \leq k_1 < k_2 \leq h$, and consider the definable sub-family $\varphi_{\text{int},k_1,k_2,<n}$ of members of σ-degree $< n$. Then we may define $m_{\text{int},k_1,k_2} = m_{\varphi_{\text{int},k_1,k_2,<n}}$ as we defined m_φ.

Now consider the family $\varphi_{\text{open},k_1,j_2} = W_{k_1}(w, u_{k_1}) \cap \text{Zeroes}(f_j(w, v_{j_2}))$, where $1 \leq k_1 \leq h$ and $1 \leq j_2 \leq r$, and consider the definable sub-family $\varphi_{\text{open},k_1,j_2,<n}$ of members of σ-degree $< n$. Then we may also define $m_{\text{open},k_1,j_2} = m_{\varphi_{\text{open},k_1,j_2,<n}}$ as we defined m_φ.

With reference to 2.25, 2.23 and 2.24, we let

$$\begin{aligned} T = \max(\quad & \{m_{\text{int},k_1,k_2} : \ 1 \leq k_1 < k_2 \leq h\}; \ \{m_{\text{open},k_1,j_2} : \ 1 \leq k_1 \leq h, \ 1 \leq j_2 \leq r\}; \\ & \mu_{\text{high}}; \ \{C_k : \ 1 \leq k \leq h\}) \end{aligned}$$

In the given set-up we estimate $\theta(K, y_0)$.

Case $n = 0$**:** For $n = 0$ the theorem follows by [8] Section 1.8; the reader can look at 2.1.3 for details.

Case $n > 0$**:** Each $V_i(w, u_i)$ is irreducible (see Item 3), has π_1 generically of finite fibre and π_2 quasi-finite on the open affine subvariety $V_i(w, u_i)\backslash\text{Zeroes}(f_j(w, v_1))$ for some $1 \leq j \leq r$ (see Item 3c). Also, $\pi_2 = \sigma \circ \pi_1$ (see Item 3d).

Thus we may apply Hrushovski's correspondence estimates 2.1.2 to each $V_i(w, u_i)\backslash\text{Zeroes}(f_j(w, v_1))$, for $1 \leq i \leq g$. We now also need to specify $(K, \sigma) = (\tilde{\mathbb{F}}_p, \text{Frob}^\gamma)$ and $q = p^\gamma$. For ease, we suppress the parameter u_i. We define $\triangle_q(V_i) = \{xz \in V_i : \ z = x^q\}$. Suppose first that $\dim_{\text{alg}}(V_i(w, u_i)) = d < n$. Then by the Hrushovski correspondence estimate 2.24 and the definition of T:

$$|\triangle_q(V_i)(K)| \leq Tq^d \tag{2.26}$$

For a component V_i of dimension n, and π_1 of degree n_{deg_i} and π_2 of inseparable degree n_{ins_i} we shall need to use the fine estimate 2.23. We begin by writing the obvious decomposition:

$$|\triangle_q(V_i)(K)| = |\triangle_q(V_i\backslash\text{Zeroes}(f_j))(K)| + |\triangle_q(V_i \cap \text{Zeroes}(f_j))(K)| \tag{2.27}$$

Since, by 3c, $\dim_{\text{alg}}(V_i \cap \text{Zeroes}(f_j)(K)) < n$, we have

$$|\triangle_q(V_i \cap \text{Zeroes}(f_j))(K)| \leq Tq^{n-1} \tag{2.28}$$

and we have by the fine estimate 2.23

$$\left||\triangle_q(V_i\backslash\text{Zeroes}(f_j))(K)| - \frac{\delta}{\delta'}q^n\right| \leq Tq^{n-\frac{1}{2}} \tag{2.29}$$

where $\delta = \deg(\pi_1)$ and $\delta' = \text{deg.ins}(\pi_2)$. With reference to Item 3e, let $\alpha = \sum_{l=1}^{m} n_{\text{comp}_l}$. There are exactly α of the V_i of dimension n. Amongst those α, there are exactly n_{comp_l} where $\delta = n_{\text{deg}_l}$ and $\delta' = n_{\text{ins}_l}$, for each l such that $1 \leq l \leq m$. Recall that $\mu = \sum_{l=1}^{m} n_{\text{comp}_l} \cdot \frac{n_{\text{deg}_l}}{n_{\text{ins}_l}}$.

By Items 2a, 3a, and 3b, $\theta(K, y_0)$ is in bijection with $\cup_{i=1}^{g} \triangle_q(V_i)(K)$. So we have the following upper-bound estimate for $|\theta(K, y_0)|$:

$$\begin{aligned}
|\theta(K,y_0)| &\leq \mu q^n + \alpha T q^{n-\frac{1}{2}} + \alpha T q^{n-1} + (g-\alpha)q^{n-1} + (g-\alpha)Tq^{n-\frac{3}{2}} \\
&\leq \mu q^n + \alpha T q^{n-\frac{1}{2}} + \alpha T q^{n-1} + (1+T)(g-\alpha)q^{n-\frac{1}{2}} \\
&\leq \mu q^n + (1+T)gq^{n-\frac{1}{2}} \\
&\leq \mu q^n + (1+T)Gq^{n-\frac{1}{2}} \qquad (2.30)
\end{aligned}$$

where G is an in Item 3.

Let us briefly describe the terms visible in the first line of Calculation 2.30. The first two terms are the asymptotic estimate and upper bound on the error for the contributions from the α sets $V_i \backslash \text{Zeroes}(f_j)$ of dimension n. The third term is an upper bound estimate for the contribution of the α sets $V_i \cap \text{Zeroes}(f_j)$ where each V_i is of dimension n. The last two terms are the asymptotic estimate and upper bound on the error for the contributions from the remaining $g - \alpha$ sets V_i.

A lower-bound estimate for $|\theta(K, y_0)|$ is given by the expression

$$\sum_{i=1}^{g} |\triangle_q(V_i \backslash \text{Zeroes}(f_j))(K)| - \sum_{1 \leq i < i^* \leq g} |\triangle_q(V_i)(K) \cap \triangle_q(V_{i^*})(K)| \qquad (2.31)$$

But notice that $\triangle_q(V_i)(K) \cap \triangle_q(V_{i^*})(K) = \triangle_q(V_i \cap V_{i^*})$. By Lemma 2.3.12 we may assume that $\deg_\sigma(\triangle_q(V_i \cap V_{i^*}) < n$. Thus by the inductive hypothesis, and by our discussion above, we may assume that $|\triangle_q(V_i \cap V_{i^*})| \leq m_{i,i^*} q^{n-1} \leq T q^{n-1}$. Thus we deduce a lower-bound estimate for $|\theta(K, y_0)|$:

$$\begin{aligned}
|\theta(K,y_0)| &\geq \mu q^n - \alpha T q^{n-\frac{1}{2}} - \begin{pmatrix} g \\ 2 \end{pmatrix} T q^{n-1} \\
&\geq \mu q^n - gT q^{n-\frac{1}{2}} - \begin{pmatrix} g \\ 2 \end{pmatrix} T q^{n-\frac{1}{2}} \\
&\geq \mu q^n - (G + \begin{pmatrix} G \\ 2 \end{pmatrix}) T q^{n-\frac{1}{2}} \qquad (2.32)
\end{aligned}$$

Again, let us briefly describe the terms visible in the first line of Calculation 2.32. The first two terms are the asymptotic estimate and upper negative bound on the error for

the contributions from the α sets $V_i \backslash \text{Zeroes}(f_j)$ of dimension n. We then assume (as we are looking for a lower bound) that the remaining $g - \alpha$ sets V_i make no contribution, so there is no term accounting for these. However, in the last term we subtract an upper bound estimate for the contribution of the intersection sets from Expression 2.31.

Thus, let $C = \max\big((T+1)G,\ (G + \begin{pmatrix} G \\ 2 \end{pmatrix})T\big)$. We deduce that

$$\mid \mid \theta(x, y_0) \mid - \mu q^n \mid \leq C q^{(n-\frac{1}{2})}$$

Again, these estimates are valid for all $(K, \sigma) = (\tilde{\mathbb{F}}_p, \text{Frob}^\gamma) \in S \backslash E$; the exceptions E result from transferring from definable stratifications that hold for *all* ω_1-saturated models of $ACFA$, to the the class S, where such stratifications hold *almost everywhere*. □

2.4 Estimates for all finite σ-degree sets

Theorem 2.3.14 establishes Theorem 2.1.1 for families of finite σ-degree, σ-closed sets. We need to extend this to all families of finite σ-degree sets. We now prove two lemmas that we apply here in conjunction with Theorem 2.3.14 in order to deduce Theorem 2.1.1, and in Chapter 2 in Theorem 3.5.8. The first lemma is a relativisation of Lemma 3.5 of [10] in the difference fields setting; similarly, the second is a relativisation of 3.7 of [10], also in the difference fields setting.

DEFINITION 2.4.1 Let $\mathcal{C}$ be a class of difference fields. Let $T_\infty(\mathcal{C})$ be the almost theory of $\mathcal{C}$. We say that the σ-degree of sets is definable in $\mathcal{C}$, if for every family $\theta(x, y)$, and for each $l \in \mathbb{N}$, there is a formula $\theta_l(y) \in \mathcal{L}_{\text{diff}}$ such that for any ω_1-saturated model $M \models T_\infty(\mathcal{C})$, then $y_0 \in \theta_l(M)$ if and only if $\deg_\sigma(\theta(x, y_0)) = l$.

We now need a more general version of Definition 1.2.7:

DEFINITION 2.4.2 Let $\mathcal{C}$ be a class of difference fields. Suppose $R(x) \in \mathcal{L}_{\text{diff}}$ is a formula in one variable, the *measuring stick* for $\mathcal{C}$. Let $\mathcal{E}$ be a class of families of

$\mathcal{L}_{\text{diff}}$-sets. Then we say $\mathcal{E}$ satisfies Elwes' definition of asymptotic sets with respect to R, if

(i) $R(M)$ is finite for each $M \in \mathcal{C}$.

(ii) for every $\mathcal{E}$ family $\varphi(x, \overline{y})$ where $length(\overline{y}) = m$, there exists finite $D \subset \{0, ..., N\} \times \mathbb{R}^{>0} \cup \{(0,0)\}$ and a partition $\{\Phi_{(d,\mu)} : (d,\mu) \in D\}$ of $\{\{M\} \times M^m : M \in \mathcal{C}\}$ so that for $(M, \overline{a}) \in \Phi_{(d,\mu)}$
we have

$$||\varphi(M, \overline{a})| - \mu |R(M)|^{\frac{d}{N}}|| = o(|R(M)|^{\frac{d}{N}})$$

as $|R(M)| \longrightarrow \infty$.

(iii) Moreover each $\Phi_{(d,\mu)}$ is definable, that is to say $\{\overline{a} \in M : (M, \overline{a}) \in \Phi_{(d,\mu)}\}$ is uniformly $\emptyset$-definable across $\mathcal{C}$.

In the following two lemmas, we assume that a measuring stick formula $R(x)$ is fixed and so we omit reference to it.

LEMMA 2.4.3 *Let $\mathcal{C}$ be a class of difference fields such that the σ-degree of sets is definable in $\mathcal{C}$, and suppose that any family of σ-closed sets of finite σ-degree satisfies Elwes' definition for asymptotic classes. Then any family of quantifier-free sets of finite σ-degree satisfies Elwes' definition for asymptotic classes.*

PROOF We transcribe the proof of Lemma 3.5 of [10] into our context:

Let $\theta(x, y)$ be a quantifier-free family of sets of finite σ-degree. By disjunctive normal form manipulations we see that θ is equivalent to a disjunction $\bigvee_{1 \leq v \leq N} (f_v(x, y) = 0 \ \wedge \ g_v(x, y) \neq 0)$, where f_v is a formula defining a σ-closed set, and g_v is a difference polynomial. Now let $y' = y_{r+1}, \ldots, y_{r+N}$. We define the formula

$$\theta'(xy', y) = \bigvee_{1 \leq v \leq N} [f_v(x, y) \ \wedge \ g_v(x, y) y_{r+v} = 1 \ \wedge \ \bigwedge_{\lambda \neq v} y_{r+\lambda} = 0] \tag{2.33}$$

Now, $\theta'(xy', y)$ is a formula defining a σ-closed set. Also, for fixed family parameter y, the solutions of $\theta'(xy', y)$ are in definable bijection with the solutions of $\theta(x, y)$ via

the map $xy' \mapsto x$. Thus $\theta'(xy', y)$ has finite σ-degree. It follows that $\theta'(xy', y)$ satisifes Elwes' definition for asymptotic classes, and thus so does $\theta(x, y)$. $\square$

LEMMA 2.4.4 *Let $\mathcal{C}$ be a class of difference fields such that the σ-degree of sets is definable in $\mathcal{C}$, and suppose that the quantifier-free sets of finite σ-degree satisfy Elwes' definition for asymptotic classes. Let $\theta(xt, y)$ be a quantifier-free family of sets of finite σ-degree, and suppose that there is an $e \in \mathbb{N}$ such that for any $(x_0, y_0) \in C$ for some $C \in \mathcal{C}$, the set $\theta(x_0 C, y_0)\}$ has cardinality less than e. Then $\exists t(\theta(xt, y))$ satisfies Elwes' definition for asymptotic classes.*

PROOF Let $(K, \sigma) \in \mathcal{C}$. Let $\varphi(x, y) := \exists t(\theta(xt, y))$. Define

$$\mathcal{F} := \varphi(K, y) \tag{2.34}$$

$$\mathcal{F}_j := \{x \in K : \ |\{t \in K : \ \theta(x, t, y)\}| = j\} \tag{2.35}$$

$$\mathcal{G} := \theta(K, y) \tag{2.36}$$

So, as in 3.7 of [17], we have the equations:

$$|\mathcal{F}| = |\mathcal{F}_1| + |\mathcal{F}_2| + \ldots + |\mathcal{F}_e| \tag{2.37}$$

$$|\mathcal{G}| = |\mathcal{F}_1| + 2 \cdot |\mathcal{F}_2| + \ldots + e \cdot |\mathcal{F}_e| \tag{2.38}$$

To get an estimate of $|\mathcal{F}_j|$, we consider the formula

$$\theta_j(xt_1 \ldots t_j, y) \ := \ \bigwedge_{i=1}^{j} \theta(xt_i, y) \ \wedge \ \bigwedge_{i_1 \neq i_2} t_{i_1} \neq t_{i_2} \tag{2.39}$$

where the t_i are new tuples of variables of the same length as t, and $t_{i_1} \neq t_{i_2}$ is the disjunction expressing that some coordinate of t_{i_1} differs from the corresponding coordinate of t_{i_2}. Let $\mathcal{K}_j := \theta_j(K, y)$. Then for each $0 \leq s \leq e - j$, each $x \in \mathcal{F}_{j+s}$ corresponds to $j![(\frac{(j+t)!}{j!t!}] = \frac{(j+t)!}{t!}$ points in $\mathcal{K}_j$. Thus we have:

$$|\mathcal{K}_j| = j! \cdot |\mathcal{F}_j| + \frac{(j+1)!}{1!} \cdot |\mathcal{F}_{j+1}| + \ldots + \frac{e!}{(e-j)!} \cdot |\mathcal{F}_e| \tag{2.40}$$

Using 2.40, we may solve for the $|\mathcal{F}_j|$ from the $|\mathcal{K}_j|$ to give

$$|\mathcal{F}| = r_1 \cdot |\mathcal{K}_1| + r_2 \cdot |\mathcal{K}_2| + \ldots + r_e \cdot |\mathcal{K}_e| \tag{2.41}$$

for some rationals $r_1, \ldots, r_e$ depending only on e. Now the $\mathcal{K}_j$ are defined using the quantifier-free families $\theta_j(xt_1 \ldots t_j, y)$. Since we have assumed $\theta(xt, y)$ is a family of

finite σ-degree sets, it follows by its definition that $\theta_j(xt_1 \dots t_j, y)$ is also a family of finite σ-degree sets. Thus, by assumption, the family of sets $\theta_j(xt_1 \dots t_j, y)$ satisfies Elwes' definition for asymptotic classes. Combining this with 2.41, we obtain the result.$\square$

We now deduce Theorem 2.1.1 from Theorem 2.3.14. Let $\mathcal{C} = \{(\tilde{\mathcal{F}}_p, \mathrm{Frob}^k) : p \text{ a prime}, k \in \mathbb{N}\}$. Let $R(x) := \sigma(x) = x$. Then 2.3.14 implies that $\mathcal{C}$ satisfies Elwes' definition for asymptotic classes with respect to $R(x)$ for all families of σ-closed sets of finite σ-degree. Then we may apply 2.4.3 to deduce that $\mathcal{C}$ satisfies Elwes' definition for asymptotic classes with respect to $R(x)$ for all quantifier-free families of sets of finite σ-degree. Then Theorem 2.1.1 follows from the elimination form for $ACFA$ (see Expression 2.15) and Lemma 2.4.4.

Chapter 3

Asymptotic Finite Difference Fields

3.1 Chapter Introduction

This chapter presents a family of asymptotic classes of finite difference fields. The results make strong use of Theorem 2.1.1. In order to to obtain the results it is necessary to develop the almost theory of finite difference fields equipped with fractional powers of the Frobenius. The almost theories under consideration are made precise below.

3.2 Notation and Key Definitions

A fractional power of the Frobenius $\mathrm{Frob}^{\frac{m}{n}}$ (m, n positive) should be exactly a solution to the equation $\mathrm{Frob}^{-m}\sigma^n = \mathrm{id}$. In the literature of $ACFA$, and also of Suzuki and Ree groups, the objects tend to be solutions of $\mathrm{Frob}^m\sigma^n = \mathrm{id}$, ($m, n$ positive). Although there is no real difference, since our eventual aim in Chapter 4 is to study Suzuki and Ree groups, our theory follows the latter convention, and strictly is the theory of fractional powers of the *inverse* of the Frobenius - but we are slack and ignore the distinction.

Throughout the chapter we work with a fixed triple $m, n, p \in \mathbb{N}$, with p a prime, $(m, n) = 1$, $m \geq 1$ and $n > 1$.

If F is a field, and σ an automorphism of F, we shall use the notation $\mathrm{Fix}(\sigma)$ to denote the subfield of F of fixed points of σ. The identity automorphism is referred to as id.

Algebraically closed fields are again denoted by a tilde: so $\tilde{K}$ is an algebraically closed field, and if K is a field then $\tilde{K}$ is its algebraic closure. For a field K, we denote by K^{ins} the purely inseparable closure of K.

For a perfect field K, $\mathrm{Gal}(K)$ denotes the automorphisms of $\tilde{K}$ that fix all elements of K.

The notions of $\mathrm{acl}_{\mathrm{alg}}(\cdot)$ and $\mathrm{acl}_\sigma(\cdot)$ are defined in sections 1.4.1 and 1.4.2 respectively. For either notion $\mathrm{acl}_{\mathrm{alg}}(A)$ or $\mathrm{acl}_\sigma(A)$, if the structure in which we are closing A is not clear, we shall denote it by a superscript. So if $(M, \sigma) \subseteq (K, \sigma)$ is a difference subfield,

and $A \subseteq M$, then $\mathrm{acl}_\sigma{}^M(A)$ denotes the closure in M. Similarly, if (K, σ) is a difference field, and $A \subseteq K$ then we write A_σ for the smallest difference subfield of (K, σ) which contains A.

For types, if we wish to specify the language in which we take a specific type as pure fields we write $\mathrm{tp}_{\mathrm{alg}}$, and for difference fields we write tp_σ.

We shall make use of ultrafilters and ultraproducts. An appropriate guide to the conventions we use is in Section 1.2.2.

3.3 Fractional powers of the Frobenius in finite fields

This first section is really an easy application of the hard results of [8] and [13]. All our lemmas are relative to a fixed characteristic determined by a choice of Frobenius automorphism; we often omit subscript reference to that characteristic.

3.3.1 Easy observations about finite fields

We begin with some simple observations about finite fields and finite cyclic groups. Our axiomatisation of the asymptotic theory of fractional powers of the Frobenius will be composed partly of a relativisation of the theory $ACFA$. The intuition for the additional ingredient comes largely from the observations and the lemma of this section.

The Set-up

- For $\alpha \in \mathbb{N}$, $\mathbb{Z}_\alpha$ shall mean the cyclic group of order α, and we shall *always* identify $\mathbb{Z}_\alpha$ with the numbers $0, 1, \ldots, \alpha - 1$. So in the sequel, we have the set of abelian groups $S_{\text{cyclic groups}} = \{\mathbb{Z}_\alpha : \alpha \in \mathbb{N}\} \bigcup \mathbb{Z}$.
- All epimorphisms considered, unless explicitly otherwise stated, are either
  - maps $\varphi_\alpha : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_\alpha$ for some $\alpha \in \mathbb{N}$, where φ_α is determined by mapping $1 \in \mathbb{Z}$ to $1 \in \mathbb{Z}_\alpha$, or

– maps $\varphi_{\alpha,\beta} : \mathbb{Z}_\alpha \twoheadrightarrow \mathbb{Z}_\beta$ for some $\alpha, \beta \in \mathbb{N}$ where $\beta|\alpha$ and $\varphi_{\alpha,\beta}$ is determined by mapping $1 \in \mathbb{Z}_\alpha$ to $1 \in \mathbb{Z}_\beta$.

So our set-up is tantamount to picking a coherent set of generators and epimorphisms for the set of groups $S_{\text{cyclic groups}}$.

- The map φ_α is commonly known as the modulus map or 'mod ' map. Let $\alpha \in \mathbb{N}$, and let the prime decomposition of α be $\alpha = p_1^{j_1} \cdot p_2^{j_2} \dots p_k^{j_k}$. The Kronecker decomposition of $\mathbb{Z}_\alpha$ is precisely the map

$$\begin{aligned} K_\alpha : \quad \mathbb{Z}_\alpha &\mapsto \prod_{i=1}^{k} \mathbb{Z}_{p_i^{j_i}} \\ X &\mapsto (\varphi_{\alpha,p_1^{j_1}}(X), \varphi_{\alpha,p_2^{j_2}}(X), \dots, \varphi_{\alpha,p_k^{j_k}}(X)) \end{aligned} \tag{3.1}$$

Now consider $g \in \mathbb{Z}_\alpha$, and for each $1 \leq i \leq k$, let $g_{p_i} = \varphi_{\alpha,p_i^{j_i}}(g)$. Then of course

$$K_\alpha : \ \langle g \rangle \cong \prod_{i=1}^{k} \langle g_{p_i} \rangle \tag{3.2}$$

- We fix notation: for prime q, the Kronecker q-component or just q-component of $\mathbb{Z}_\alpha$ will be the Sylow q-subgroup in $\mathbb{Z}_\alpha$. We may refer to this as K_q^α.

- The canonical projection from the Kronecker decomposition to the q-component will be π_q, and supposing that the Sylow q-subgroup has order q^n, then for $h \in \mathbb{Z}_\alpha$ we let $h_q = \pi_q \circ K_\alpha(h) = \varphi_{\alpha,q^n}$. We call h_q the q-coordinate of h.

- The Kronecker decomposition commutes with epimorphisms: suppose we have the prime decomposition $\alpha = p_1^{j_1} \cdot p_2^{j_2} \dots p_k^{j_k}$, and $\beta|\alpha$, so that we have the prime decomposition $\beta = p_1^{l_1} \cdot p_2^{l_2} \dots p_k^{l_k}$, with $l_i \leq j_i$ for $1 \leq i \leq k$. Then we have the tuple map

$$(\varphi_{p_1^{j_1},p_1^{l_1}}, \varphi_{p_2^{j_2},p_1^{l_2}}, \dots, \varphi_{p_k^{j_k},p_k^{l_k}}) : \ \prod_{i=1}^{k} \mathbb{Z}_{p_i^{j_i}} \mapsto \prod_{i=1}^{k} \mathbb{Z}_{p_i^{l_i}} \tag{3.3}$$

The commutation with epimorphisms is summarised by the equation

$$(\varphi_{p_1^{j_1},p_1^{l_1}}, \varphi_{p_2^{j_2},p_1^{l_2}}, \dots, \varphi_{p_k^{j_k},p_k^{l_k}}) \circ K_\alpha = K_\beta \circ \varphi_{\alpha,\beta} \tag{3.4}$$

We call the tuple map in Expression 3.3 the Kronecker decomposition of $\varphi_{\alpha,\beta}$. For q a prime , the 'q'th component of the Kronecker decomposition of $\varphi_{\alpha,\beta}$' will refer to the member map of the Kronecker decomposition which is the map of Sylow q-subgroups.

LEMMA 3.3.1 *Let n and m be coprime natural numbers. Let $\varphi_{\alpha\cdot\beta,\alpha} : \mathbb{Z}_{\alpha\cdot\beta} \mapsto \mathbb{Z}_\alpha$ be an epimorphism of finite cyclic groups. Let h be an element of $\mathbb{Z}_\alpha$. Suppose $\langle nh + m\rangle$ is a subgroup of $\mathbb{Z}_\alpha$ of cardinality S. Then there exists $g \in \mathbb{Z}_{\alpha\cdot\beta}$ such that $\varphi_{\alpha\cdot\beta,\alpha}(g) = h$ and $\langle ng + m\rangle$ is a subgroup of $\mathbb{Z}_{\alpha\cdot\beta}$ of cardinality $S \cdot \beta$.*

PROOF We work with the set-up of cyclic groups as described in the set-up section of 3.3.1, and we assume that for natural numbers $d_1|d_2$, epimorphisms φ_{d_2,d_1} are interpreted as in that set-up. There is no loss of generality in this. It suffices to let β be a prime p, and do one step, since it is clear that $\varphi_{\alpha\cdot\beta\cdot\gamma,\alpha} = \varphi_{\alpha\cdot\beta,\alpha} \circ \varphi_{\alpha\cdot\beta\cdot\gamma,\alpha\cdot\beta}$. We pick g by picking its Kronecker coordinates. Using Expression 3.2, we see that to prove the lemma we must pick g according to the following demands:

Demands on g

1. $\varphi_{\alpha\cdot p,\alpha}(g) = h$
2. For all Kronecker q-components of $\mathbb{Z}_\alpha$ with $p \neq q$, $|\langle ng_q + m\rangle| = |\langle nh_q + m\rangle|$
3. $|\langle ng_p + m\rangle| = p \cdot |\langle nh_p + m\rangle|$.

$1'$. By the commutation of Kronecker decomposition with epimorphisms (see expression 3.4), demand 1 is equivalent to the statement: for each Kronecker q-component of $\mathbb{Z}_{\alpha\cdot p}$, suppose the order of q in $\alpha\cdot p$ is N_1 and the order of q in α is N_2, then $\varphi_{q^{N_1},q^{N_2}}(g_q) = h_q$. We shall use $1'$ instead of 1.

Let us do two cases.

(Case 1: $p|\alpha$) In this case the Kronecker decomposition of $\varphi_{\alpha\cdot p,\alpha}$ is identity on all Kronecker q-components for $p \neq q$ and is φ_{p^{N+1},p^N} on the Kronecker p-component, where N is the order of p in α.

Since $\varphi_{\alpha\cdot p,\alpha}$ is identity on all q-components for $p \neq q$, for these, we may let $g_q = h_q$, and demand 2 is satisfied. Also, demand $1'$ is met on all Kronecker q-components with $p \neq q$.

For the p-component, let $0 \leq w \leq N$. Notice the following:

1. The restriction of the map φ_{p^{N+1},p^N} to the unique p^{w+1}-size subgroup of $\mathbb{Z}_{p^{N+1}}$ is the epimorphism φ_{p^{w+1},p^w}.

2. From (1) above and by counting, the preimage $\varphi^{-1}_{p^{w+1},p^w}(\mathbb{Z}_{p^w}) = \mathbb{Z}_{p^{w+1}}$.

3. The other fact we recall is that for an epimorphism of cyclic p-groups where the image is not the trivial group, the generators of the source are exactly the preimages of the generators of the image. We omit the proof of this, but it is straightforward, by counting, and the counting makes use of Euler's totient function.

Now begin by 'guessing' $g_p = h_p$ (see the set-up subsection at the beginning of 3.3.1 to see the specific meaning of this guess). Now, with this guess, $\varphi_{p^{N+1},p^N}(g_p) = h_p$, and so demand $1'$ is now satisfied on all Kronecker components, and so all we need to do is ensure demand 3. We have two cases:

If $nh_p + m$ is a non-trivial element of $\mathbb{Z}_{p^N}$ then suppose $\langle nh_p + m\rangle$ has size p^w with $w \neq 0$. By (2) above, $\varphi^{-1}_{p^{N+1},p^N}(\langle nh_p + m\rangle)$ is the unique $\mathbb{Z}_{p^{w+1}}$ subgroup of $\mathbb{Z}_{p^{N+1}}$. By (3) and (1) above, any preimage $\varphi^{-1}_{p^{N+1},p^N}(nh_p + m)$ is a generator for $\mathbb{Z}_{p^{w+1}}$. But $ng_p + m$ is such a preimage.

If $nh_p + m$ is the trivial element of $\mathbb{Z}_{p^N}$ then our guess may not be good enough. Now the preimages $\varphi^{-1}_{p^{N+1},p^N}(h_p)$ are exactly $\{h_p + \delta p^N : \ 0 \leq \delta < p\}$. So the preimages are coded by numbers δ with $0 \leq \delta < p$, and since we shall select g_p from these preimages by selecting a value for δ, demand $1'$ will be satisfied on all Kronecker components. We now work in $\mathbb{Z}_{p^{N+1}}$. We may suppose that for some $0 \leq \varepsilon < p$, that $nh_p + m$ is the element εp^N of $\mathbb{Z}_{p^{N+1}}$ We have $n \cdot (h_p + \delta p^N) + m = (\varepsilon + n\delta)p^N$. If $\varepsilon \neq 0$ then we may pick $\delta = 0$, and $nh_p + m$ generates the unique p size subgroup of $\mathbb{Z}_{p^{N+1}}$, which is what we desired. If $\varepsilon = 0$ and $(n, p) = 1$ we can pick any $\delta \neq 0$ and let $g_p = h_p + \delta p^N$. Then $ng_p + m$ generates the unique p-size subgroup of $\mathbb{Z}_{p^{N+1}}$, which was what we desired. Otherwise $(n, p) = p$. But then $(n, m) = 1$ so $(m, p) = 1$ and so $(nh_p + m, p) = 1$ and $nh_p + m$ cannot be the trivial element of $\mathbb{Z}_{p^N}$.

(Case 2: $(\alpha, p) = 1$) For $q \neq p$ we must pick $g_q = h_q$, and again, demand 2 is satisfied,

and demand $1'$ is satisfied for all Kronecker q-components with $p \neq q$. For demand 3, notice that we have that the Kronecker p-component of $\varphi_{\alpha\cdot p,\alpha}$ is $\varphi_{p,1} : \mathbb{Z}_p \mapsto 1$, and any choice for g_p in $0 \leq g_p < p$ extends h_p. So to satisfy demand 3, we require exactly a g_p such that $(ng_p + m, p) = 1$ where $0 \leq g_p < p$. Try $g_p = 0$. Either it works, or $(m, p) = p$. If $(m, p) = p$ then $(n, p) = 1$ and $(m + n, p) = 1$, so $g_p = 1$ suffices. $\square$

This tells us something quite specific about extensions of fractional powers of the Frobenius. This is because for q a prime power, and $l \in \mathbb{N}$, $\mathrm{Aut}(\mathbb{F}_{q^l}/\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q) \cong \mathbb{Z}_l$. So let p be a prime and $a, j, l \in \mathbb{N}$. Suppose σ is a solution in $\mathrm{Aut}(\mathbb{F}_{p^a})$ to the equation $\mathrm{Frob}^m X^n = \mathrm{id}$. Say $\mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^{aj}} \subseteq \mathbb{F}_{p^{ajl}}$ is a containment of fields, and suppose $\sigma' \in \mathrm{Aut}(\mathbb{F}_{p^{aj}})$ is an extension of σ. Further suppose that $\mathrm{Frob}^m(\sigma')^n$ is a generator of $\mathrm{Gal}(\mathbb{F}_{p^{aj}}/\mathbb{F}_{p^a})$. Now let $\alpha = aj$ and $\beta = l$ and apply Lemma 3.3.1 to the data: $\mathbb{Z}_\alpha = \mathrm{Aut}(\mathbb{F}_{p^{aj}})$; $\mathbb{Z}_{\alpha\cdot\beta} = \mathrm{Aut}(\mathbb{F}_{p^{ajl}})$; $h = \sigma'$; and F is the restriction epimorphism of automorphism groups. The conclusion of the Lemma is the existence of $\sigma'' \in \mathrm{Aut}(\mathbb{F}_{p^{ajl}})$ such that σ'' extends σ' and $\mid \langle \mathrm{Frob}^m(\sigma'')^n \rangle \mid = l \cdot \mid \langle \mathrm{Frob}^m(\sigma')^n \rangle \mid$. But $\langle \mathrm{Frob}^m(\sigma')^n \rangle = \mathrm{Gal}(\mathbb{F}_{p^{aj}}/\mathbb{F}_{p^a})$, so we deduce $\mathrm{Frob}^m(\sigma'')^n$ is a generator for $\mathrm{Gal}(\mathbb{F}_{p^{ajl}}/\mathbb{F}_{p^a})$.

We enshrine this conclusion in a definition and lemma:

DEFINITION 3.3.2 *Consider an extension of perfect difference fields $(F, \sigma) \subseteq (G, \sigma')$ with $\mathrm{Frob}^m\sigma^n = \mathrm{id}$. We say the extension is generic over F if $\mathrm{Fix}(\mathrm{Frob}^m\sigma'^n) = F$.*

PROPOSITION 3.3.3 *Let p be a prime and $a, j, l \in \mathbb{N}$. Consider an extension of finite difference fields $(\mathbb{F}_{p^a}, \sigma) \subseteq (\mathbb{F}_{p^{aj}}, \sigma')$ with $\mathrm{Frob}^m\sigma^n = \mathrm{id}$. Suppose the extension is generic over $\mathbb{F}_{p^a}$. Then for any finite extension $\mathbb{F}_{p^{aj}} \subseteq \mathbb{F}_{p^{ajl}}$, σ' has an extension $\sigma'' \in \mathrm{Aut}(\mathbb{F}_{p^{ajl}})$ which is generic over $\mathbb{F}_{p^a}$.* $\square$

Here is an example of the Lemma in action:

EXAMPLE 3.3.4 Consider the field $\mathbb{F}_{3^9}$, the automorphism $\mathrm{Frob} = x \mapsto x^3$ and the automorphism of $\mathbb{F}_{3^9}$, $\sigma = \mathrm{Frob}^3 = x \mapsto x^{27}$. Then in $\mathbb{F}_{3^9}$, σ is a solution of $\mathrm{Frob}^3 \circ X^5 = \mathrm{id}$. Consider $\mathbb{F}_{3^9} \subseteq \mathbb{F}_{3^{18}}$ and let us find a generic extension of σ to $\mathbb{F}_{3^{18}}$ over $\mathbb{F}_{3^9}$. Recall that $\mathrm{Aut}(\mathbb{F}_{3^{18}}/\mathbb{F}_3) \cong \mathbb{Z}_{18} \cong \mathbb{Z}_9 \times \mathbb{Z}_2$. Thus we have two choices for the Kronecker 2-coordinate. Keeping $\sigma = \mathrm{Frob}^3$ is picking 2-coordinate 1. But this is not generic as the fixed field of $\mathrm{Frob}^3 \circ (\mathrm{Frob}^3)^5$ in $\mathbb{F}_{3^{18}}$ is $\mathbb{F}_{3^{18}}$. But pick 2-Kronecker

coordinate 0, and this yields an extension of σ, $\sigma' = \text{Frob}^{12} = x \mapsto x^{3^{12}}$. Now in $\mathbb{F}_{3^{18}}$, $\text{Fix}(\text{Frob}^3 \circ (\text{Frob}^{12})^5) = \text{Fix}(\text{Frob}^{63}) = \text{Fix}(\text{Frob}^9) = \mathbb{F}_{3^9}$.

3.3.2 Axiomatisation and quantifier elimination results

In this section, unless stated otherwise, we work in $\mathcal{L}_{\text{diff}}$, the language of rings with a unary function symbol σ. Let $\mathcal{L}_{\text{diff},c}$ be the augmentation of $\mathcal{L}_{\text{diff}}$ by distinguished constants $(c_{ij} : i \in \mathbb{N},\ 0 \leq j \leq i)$. Similarly, let the language $\mathcal{L}_{\text{rings},c}$ be the language of rings augmented by constants c. A field K is augmented to an $\mathcal{L}_{\text{rings},c}$-structure simply by interpreting the constants c, and is denoted K_c. Recall that distinguished constants are used in [10] to produce model-complete expansions of pseudo-finite fields. They will play a similar role in what follows.

Let p be a prime. For V a variety over the field K and σ an automorphism of K, we shall use the notion of the conjugate variety $\sigma(V)$, which is explained in Section 1.4.1. The following axioms express properties of an $\mathcal{L}_{\text{diff}}$-structure (K, σ). It will be called the theory $PSF_{(m,n,p)}$:

(i) K is a pseudo-finite field of characteristic p.

(ii) σ is an automorphism of K with $\text{Frob}^m \circ \sigma^n = \text{id}$.

(iii) Suppose $U = U(x_{11}x_{21} \ldots x_{n1} \ldots x_{1N}x_{2N} \ldots x_{nN})$ is an absolutely irreducible variety over K and $\sigma(U) = \sigma(U)(y_{11}y_{21} \ldots y_{n1} \ldots y_{1N}y_{2N} \ldots y_{nN})$. Suppose $V \subseteq U \times \sigma(U)$ is an absolutely irreducible variety over K including the equations $y_{ij} = x_{i+1j}$ and $y_{nj}^{p^m} = x_{1j}$ for $i = 1$ to $n-1$ and $j = 1$ to N. Suppose V projects generically onto U and $\sigma(U)$, and suppose W is a K-algebraic set properly contained in V. Then there is a point $x \in V(K) \backslash W(K)$ such that $x = ab$ where $a = (a_{ij} : 1 \leq i \leq n,\ 1 \leq j \leq N)$, $b = (b_{ij} : 1 \leq i \leq n,\ 1 \leq j \leq N)$, $a \in U$, $b \in \sigma(U)$ and $b_{ij} = \sigma(a_{ij})$ for each i, j.

(iv) Let $K \subseteq L \subseteq H$ be a tower of finite extensions. Suppose $(K, \sigma) \subseteq (L, \sigma')$ is an extension of difference fields generic over K. Then there is an extension of difference fields $(L, \sigma') \subseteq (H, \sigma'')$ with σ'' generic over K.

In the language $\mathcal{L}_{\text{diff},c}$, let $PSF_{(m,n,p,c)}$ be the theory obtained from the axioms above with axiom (i) replaced by (i') saying K_c is a model of the theory of enriched pseudo-finite fields. Let us describe this enrichment briefly: let $P_i(X)$ be the polynomial $P_i(X) = c_{i0} + c_{i1}X + c_{i2}X^2 \ldots + c_{ii}X^i$. The enriched theory of pseudo-finite fields is the theory of pseudo-finite fields augmented by sentences stating the $P_i(X)$ are irreducible polynomials. Thus in a containment $K_c \subseteq L_c$ of enriched pseudo-finite fields, it follows that $L_c \cap \tilde{K}_c = K_c$. This implies $K_c \prec L_c$ as enriched fields, by the characterisation of elementary equivalence of pseudo-finite fields (see [6] Theorem 5.12). Thus the theory of enriched pseudo-finite fields is model-complete. See [10] Section 2, and [6] Section 5 for more details.

LEMMA 3.3.5 *The theories $PSF_{(m,n,p)}$ and $PSF_{(m,n,p,c)}$ are first order and consistent. Furthermore, for any $(M,\sigma) \models ACFA_p$, $(\text{Fix}(\text{Frob}^m \circ \sigma^n)(M), \sigma|_{\text{Fix}(\text{Frob}^m \circ \sigma^n)(M)}) \models PSF_{(m,n,p)}$.*

PROOF It is enough to prove these results for $PSF_{(m,n,p)}$, since a model of $PSF_{(m,n,p,c)}$ is obtained from a model of $PSF_{(m,n,p)}$ by an appropriate assignment of the constants.

We show that $PSF_{(m,n,p)}$ is first-order. Axioms (i) to (iii) are clearly first-order since (i) is known and (iii) is just a fragment of $ACFA$. As to (iv) we can quantify over a finite extension of K-(see for instance the axiomatisation of a pseudo-finite field in [6]). So let L be a finite extension of K. Since K is perfect (this is in the axiomatisation of pseudo-finite fields) we may write $L = K(l)$ where l is a primitive element for L/K. An automorphism τ of L, such that τ extends σ, is determined exactly by two things: by the action of σ on K and by the image $\tau(l)$. Thus all automorphisms τ, which are extensions of σ to L, are interpretable. Thus (iv) is first-order too.

Proving the last statement of the lemma also suffices to prove consistency, so pick a model (M,σ) of $ACFA_p$ and look at $K = \text{Fix}(\text{Frob}^m \circ \sigma^n)$. Now I claim $(K, \sigma|_K) \models PSF_{(m,n,p)}$. Axiom (i) is a basic fact about the theory $ACFA$- see [8] 1.2 and 1.12. Axiom (ii) is clear. Axiom (iii) is just a fragment of the theory $ACFA$ satisfied by $(K, \sigma|_K)$.

Now for axiom (iv): the elementary equivalence theorem for $ACFA$ (one of the main theorems of [13], and presented in this thesis as Theorem 2.1.3) states that $ACFA_p$ is the theory of all non-principal ultraproducts of all difference fields of the form $(\tilde{\mathbb{F}}_p, \mathrm{Frob}^k)$ where $k \in \mathbb{N}$. Thus, we suppose

$$(M, \sigma) \equiv \prod_{i \in \mathbb{N}} (\tilde{\mathbb{F}}_p, \mathrm{Frob}^{t_i}) / \sim_{\mathcal{U}}$$

for some choice of $\mathcal{U}$, and t_i.

Notice that for any characteristic p difference field (K_1, σ_1) the formula $\mathrm{Frob}^m \sigma^n(x) = x$ defines the underlying set of a difference subfield, which we denote by $(K_1)_{m,n}$. If (K_1, σ_1) and (K_2, σ_2) are elementarily equivalent difference fields, then it follows that the difference subfields $(K_1)_{m,n}$ and $(K_2)_{m,n}$ are elementarily equivalent too. It follows that

$$(K, \sigma|_K) \equiv \prod_{i \in \mathbb{N}} (\mathbb{F}_{p^{nt_i+m}}, \mathrm{Frob}^{t_i}) / \sim_{\mathcal{U}}$$

By $\mathcal{L}$os's Theorem, an extension $(K, \sigma) \subseteq (L, \sigma')$, with $[L : N] = j < \infty$, satisfies

$$(L, \sigma') \equiv \prod_{i \in \mathbb{N}} (\mathbb{F}_{p^{(nt_i+m)j}}, \mathrm{Frob}^{s_i}) / \sim_{\mathcal{U}},$$

for some collection s_i where $0 \leq s_i \leq (nt_i + m)j - 1$, and $s_i = t_i \bmod (nt_i + m)$. Similarly, if $L \subseteq H$ and $[H : L] = l < \infty$, then

$$H \equiv \prod_{i \in \mathbb{N}} (\mathbb{F}_{p^{(nt_i+m)jl}}) / \sim_{\mathcal{U}},$$

Since axiom (iv) is first-order, $\mathcal{L}$os's Theorem implies that there is σ'', an extension of σ' on H which is generic over K, if and only if there are extensions of Frob^{s_i} on $\mathbb{F}_{p^{(nt_i+m)jl}}$ which are generic over $\mathbb{F}_{p^{nt_i+m}}$ on 'ultrafilter-many' components i (see section 1.2.2 for an explanation of this term). This is so by 3.3.3. □

LEMMA 3.3.6 *Let $(K, \sigma) \models PSF_{(m,n,p)}$. Then there is an automorphism τ of $\tilde{K}$ such that $\tau|_K = \sigma$ and* $\mathrm{Fix}(\mathrm{Frob}^m \circ \tau^n) = K$.

PROOF Clear by axiom scheme (iv).

THEOREM 3.3.7 *(a) Every $\mathcal{L}_{\mathrm{diff},c}$-model (K_c, σ) of axioms (i'), (ii) and (iv) embeds in a model of $PSF_{(m,n,p,c)}$. Considered as an embedding of the reduct enriched pseudo-finite fields, the embedding is elementary.*
(b) $PSF_{(m,n,p,c)}$ is model-complete.

PROOF (a) Since (K, σ) models axiom scheme (iv), there is an extension of difference fields $(K, \sigma) \subseteq (\tilde{K}, \sigma^+)$ with $\mathrm{Fix}(\mathrm{Frob}^m(\sigma^+)^n) = K$. Now $ACFA$ is the model companion of difference fields so $(\tilde{K}, \sigma^+)$ embeds in $(M, \tau) \models ACFA$. Look at $\mathrm{Fix}(\mathrm{Frob}^m \circ \tau^n)(M)$. Observe firstly that K is algebraically closed inside $\mathrm{Fix}(\mathrm{Frob}^m \circ \tau^n)(M)$ (see Section 1.4.1 for an explanation), and secondly, that if E and F are two pseudo-finite fields with a common subfield K then $E \equiv_K F \Leftrightarrow E \cap \tilde{K} \cong F \cap \tilde{K}$. (The reader may find a detailed proof of this in section 5 of [6].) Thus $K \prec \mathrm{Fix}(\mathrm{Frob}^m \circ \tau^n)(M)$, and this shows that $K_c \prec \mathrm{Fix}(\mathrm{Frob}^m \circ \tau^n)_c(M)$. This was what was required.

(b) Now we apply the Robinson test: 'If T is a consistent theory in a language $\mathcal{L}$, then T is model complete if and only if for any pair of models $U, B \models T$ with $U \subseteq B$, then every existential sentence in $\mathcal{L}(U)$ which holds in B also holds in U' (see [5] pp. 187). An existential sentence is a sentence $\exists(x_1, x_2, \ldots, x_r)\theta(x_1, x_2, \ldots, x_r)$ where θ is quantifier-free.
Let $(K, \sigma, c) \models PSF_{(m,n,p,c)}$. Let $\psi(\bar{x})$ be a quantifier-free formula with parameters in K, in variables $\bar{x} = (x_1, \ldots, x_{r-1})$, and which has a solution $\bar{a}_0 = (a_1, \ldots, a_{r-1})$ in some $(L, \sigma', c) \models PSF_{(m,n,p,c)}$, such that $(K_c, \sigma) \subseteq (L_c, \sigma')$. It suffices to assume that for some $k, s \in \mathbb{N}$, $\psi(\bar{x})$ is of the form

$$f_1(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^k(\bar{x})) = f_2(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^k(\bar{x})) = \ldots = f_s(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^k(\bar{x})) = 0$$
$$\wedge\, g(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^k(\bar{x})) \neq 0$$

where the f_i's and g are polynomials with coefficients in K. We may 'hyperbolise': that is, let x_r be a new variable, let $\bar{x}' = (x_1, x_2, \ldots, x_r)$, so that $\bar{x}$ is the sub-tuple of $\bar{x}'$ of its first $r-1$ elements, and consider the formula $\psi'(\bar{x}')$:

$$\psi'(\bar{x}') =_{\mathrm{def}} \; f_1(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^k(\bar{x})) = f_2(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^k(\bar{x})) = \ldots = f_s(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^k(\bar{x})) = 0$$
$$\wedge\, x_r \cdot g(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^k(\bar{x})) - 1 = 0$$

Notice that $\bar{a} = (\bar{a}_0, \frac{1}{g(\bar{a}_0,\sigma(\bar{a}_0),\ldots,\sigma^k(\bar{a}_0))})$ is a solution to ψ'. Also notice that the subtuple of the first $r-1$ elements of a solution to ψ' is always a solution to ψ. So it suffices to find a tuple $\bar{b}$ of elements from K such that $\psi'(\bar{b})$ holds.

We use axiom scheme (iii). For a matrix $\overline{\mathrm{Mat}}$ of elements of a difference field (K,σ), let $\sigma(\overline{\mathrm{Mat}})$ be the matrix obtained by applying σ component-wise. Relabel $\bar{x}'$ as $\bar{x}$. Let $\overline{\mathrm{Mat}}_0(\bar{x})$ be an $n \times r$ matrix with $\overline{\mathrm{Mat}}_0(\bar{x})_{ij} = \sigma^i(x_j)$ where $0 \leq i \leq n-1$ and $1 \leq j \leq r$. Let $\overline{\mathrm{Mat}}_q(\bar{x}) = \sigma^q(\overline{\mathrm{Mat}}_0(\bar{x}))$ for $0 \leq q \leq k$, and finally, let $\overline{\mathrm{Mat}}(\bar{x}) = \overline{\mathrm{Mat}}_0(\bar{x})\overline{\mathrm{Mat}}_1(\bar{x})\ldots\overline{\mathrm{Mat}}_k(\bar{x})$ be the matrix obtained by right juxtaposition of the $\overline{\mathrm{Mat}}_q(\bar{x})$.

So suppose that $\bar{a} \in L$ and $\psi'(\bar{a})$ holds in the extension (L,σ',c). Then consider the algebraic-geometric locus: $V = \mathrm{locus}(\overline{\mathrm{Mat}}(\bar{a})\sigma(\overline{\mathrm{Mat}}(\bar{a}))/\tilde{K})$. Then V has dominant projections into each of $U = \mathrm{locus}(\overline{\mathrm{Mat}}(\bar{a})/\tilde{K})$ and $\sigma(U)$. Clearly $V \subseteq U \times \sigma(U)$. It also satisfies the equational constraints of axiom (iii).

Also I claim that both V and U are definable over K. To show this, first recall a fact about algebraically closed fields: Let $C \subseteq \tilde{L}$. Then $\mathrm{tp}_{\mathrm{alg}}(\overline{\mathrm{Mat}}(\bar{a})\sigma(\overline{\mathrm{Mat}}(\bar{a}))/(\mathrm{acl}(C) \cap \mathrm{dcl}(C, \overline{\mathrm{Mat}}(\bar{a})\sigma(\overline{\mathrm{Mat}}(\bar{a})))))$ is stationary (see, for instance, Section 1, and Proposition 1.1 in particular, of [15]). So let $C = K$; we write $\mathrm{acl}(K)$ as $\tilde{K}$. Since K is algebraically closed in L, we have $\tilde{K} \cap \mathrm{dcl}(K, \overline{\mathrm{Mat}}(\bar{a})\sigma(\overline{\mathrm{Mat}}(\bar{a}))) \subseteq \tilde{K} \cap L = K$, and so $\mathrm{tp}(\overline{\mathrm{Mat}}(\bar{a})\sigma(\overline{\mathrm{Mat}}(\bar{a}))/K$ is stationary, and so V is definable over K. Similarly, so too are U and $\sigma(U)$. We can now apply axiom scheme (iii): there is a tuple $\bar{b} \in K$ such that $\overline{\mathrm{Mat}}(\bar{b})\sigma(\overline{\mathrm{Mat}}(\bar{b})) \in V$. However the construction of $\overline{\mathrm{Mat}}(\bar{b})$ was a typical correspondence coding of a σ-closed set, similar to the constructions of 2.3.1. Similar to Lemma 2.3.7, there is a bijection between the points $x\sigma(x) \in V(K)$ and the points of $\psi'(K)$. Chasing through the construction of $\overline{\mathrm{Mat}}(\bar{b})$, the reader can verify that $\psi'(\bar{b})$ holds. □

LEMMA 3.3.8 *Let T_0 be the $\mathcal{L}_{\mathrm{diff}}$-theory of a field of characteristic p with automorphism σ satisfying* $\mathrm{Frob}^m \circ \sigma^n = \mathrm{id}$. *Every model of T_0 embeds into a model of $PSF_{(m,n,p)}$.*

PROOF Let $(M_0, \sigma_0) \models T_0$. Then (M_0, σ_0) embeds into some $(M, \tau) \models ACFA$, because $ACFA$ is the model companion of difference fields. Now this shows that M_0 embeds into $\mathrm{Fix}(\mathrm{Frob}^m \circ \tau^n)(M)$. In Lemma 3.3.5 it is shown that $(\mathrm{Fix}(\mathrm{Frob}^m \circ \tau^n)(M), \tau|_{\mathrm{Fix}(\mathrm{Frob}^m \circ \tau^n)(M)}) \models PSF_{(m,n,p)}$. □

We needed the following lemma. We have been informed subsequently that it is Theorem 7 of [3].

LEMMA 3.3.9 *Let $K \subseteq L$ be such that L is pseudo-finite and $L \cap \tilde{K} = K$. Then K has at most one finite extension of each degree.*

PROOF Firstly K must be perfect by the assumption that K is relatively algebraically closed in L. So suppose K has two extensions of degree r, witnessed by primitive elements α_1 and α_2. Let their minimal polynomials over K be denoted M_{α_i}. Since their compositum is a finite separable extension of K, it is primitively generated by an element α whose minimal polynomial over K is denoted by M_α. Now fix i for $i = 1$ or $i = 2$. If $[L(\alpha_i) : L] < r$, then M_{α_i} factorises partially over the field L. Suppose $P \in L[X]$ and P is a non-trivial factor of M_{α_i}. The coefficients of P are rational functions of the roots of M_{α_i} and at least one of these must live in $L \backslash K$. But then $L \cap \tilde{K} \neq K$. The same argument applies to $[L(\alpha) : L]$. So

$$(*) \quad [L(\alpha) : L] = [K(\alpha) : K] > [K(\alpha_i) : K] = [L(\alpha_i) : L] = r$$

Now by the uniqueness of degree-r extensions for pseudo-finite fields $L(\alpha_1) = L(\alpha_2)$. So $L(\alpha) = L(\alpha_i)$ and this contradicts (*). □

THEOREM 3.3.10 *Let (F, σ) and (E, τ) both be models of $PSF_{(m,n,p)}$ containing a common substructure K- i.e. $\sigma|_K = \tau|_K$. Then $(F, \sigma) \equiv_K (E, \tau) \Leftrightarrow (F \cap \tilde{K}, \sigma|_{F \cap \tilde{K}}) \cong_K (E \cap \tilde{K}, \tau|_{E \cap \tilde{K}})$.*

PROOF For the left to right we use results on pseudo-finite fields. We assume saturated models exist and take saturated elementary extensions $(F, \sigma, K) \prec (M, \mu, K)$ and $(E, \tau, K) \prec (N, \nu, K)$. By (F, σ, K), we mean the difference field (F, σ) with constants for the subfield K; similarly, by (F, K) we mean the field F with constants for the subfield K. We may suppose there is an isomorphism $i : (M, \mu, K) \cong (N, \nu, K)$. But

$(F,\sigma,K) \prec (M,\mu,K)$ means that for (F,K) we have $(F,K) \prec (M,K)$. So by the version of our Theorem for pseudo-finite fields (see [7] 5.12), $M \cap \tilde{K}{=}F \cap \tilde{K}$. Similarly $N \cap \tilde{K}{=}E \cap \tilde{K}$. So i gives us the necessary isomorphism.

Now the other direction. It is harmless to relabel K as the intersection $E \cap \tilde{K}$, and using an isomorphism we may assume that K is algebraically closed in both E and F, and that $\tau|_K = \sigma|_K$.

Claim: There are difference fields $(\tilde{F},\tilde{\sigma})$ and $(\tilde{E},\tilde{\tau})$ such that $\tilde{F}$ and $\tilde{E}$ are the algebraic closures of F and E respectively, $(F,\sigma) \subseteq (\tilde{F},\tilde{\sigma})$ and $(E,\tau) \subseteq (\tilde{E},\tilde{\tau})$, and

$$(i)\ \tilde{\tau}|_{\tilde{K}} = \tilde{\sigma}|_{\tilde{K}}$$
$$(ii)\ \mathrm{Fix}(\mathrm{Frob}^m\tilde{\sigma}^n) = F \text{ and } \mathrm{Fix}(\mathrm{Frob}^m\tilde{\tau}^n) = E$$

Proof of right to left direction of lemma assuming claim: Embed $(\tilde{E},\tilde{\tau}) \subseteq (A,\tilde{\tau}')$ where the latter is a model of $ACFA$. Similarly embed $(\tilde{F},\tilde{\sigma}) \subseteq (B,\tilde{\sigma}')$ where the latter is a model of $ACFA$. Notice that by [8] Theorem 1.3 $(A,\tilde{\tau}') \equiv_{\tilde{K}} (B,\tilde{\sigma}')$. So, in particular, we have for the reducts

$$(\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n), \tilde{\tau}'|_{\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n)}) \equiv_K (\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n), \tilde{\sigma}'|_{\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n)})$$

and by Lemma 3.3.5

$$(\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n), \tilde{\tau}'|_{\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n)}) \models PSF_{(m,n,p)}$$
$$(\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n), \tilde{\sigma}'|_{\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n)}) \models PSF_{(m,n,p)}$$

By the claim, F is algebraically closed in $\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n)$, and E is algebraically closed in $\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n)$. Thus by Theorem 3.3.7 (b)

$$(F,\sigma) \prec (\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n), \tilde{\sigma}'|_{\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n)})$$

$$(E,\tau) \prec (\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n), \tilde{\tau}'|_{\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n)})$$

and so we have the chain

$$(F,\sigma) \equiv_K (\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n), \tilde{\sigma}'|_{\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\sigma}')^n)}) \equiv_K (\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n), \tilde{\tau}'|_{\mathrm{Fix}(\mathrm{Frob}^m(\tilde{\tau}')^n)}) \equiv_K (E,\tau)$$

End of proof of right to left direction assuming claim

Proof of claim: Let $\mathcal{H} = \mathrm{Gal}(F) \times \mathrm{Gal}(E)$. Thus $\mathcal{H}$ is naturally a compact topological group. Pick $\sigma_1 \in \mathrm{Aut}(\tilde{F})$ such that $\sigma_1|_F = \sigma$, and $\tau_1 \in \mathrm{Aut}(\tilde{E})$ such that $\tau_1|_E = \tau$. Then $\mathcal{J} = \{(x, y) \in \mathrm{Aut}(\tilde{F}) \times \mathrm{Aut}(\tilde{E})$: x extends σ and y extends $\tau\}$= $\sigma_1\mathrm{Gal}(F) \times \tau_1\mathrm{Gal}(E)$, and this choice of representatives σ_1 and τ_1 identifies a structure of a compact topological space on $\mathcal{J}$ induced from the topology of $\mathcal{H}$.

For a pseudo-finite field P we denote by P_r its unique degree-r extension.

Now let

$$S_r = \quad \{(x, y) \in \mathcal{J} : \mathrm{Fix}(\mathrm{Frob}^m(x|_{F_r})^n) = F \text{ and } \mathrm{Fix}(\mathrm{Frob}^m(y|_{E_r})^n) = E \text{ and } x|_{\tilde{K}\cap F_r} = y|_{\tilde{K}\cap E_r}\}$$

To conclude the proof of the claim it suffices to show that for any $r \in \mathbb{N}$, S_r is closed and non-empty. Let us demonstrate this: since for any $i \in \mathbb{N}$, we have $\emptyset \neq S_{r_1\cdot r_2\ldots\cdot r_{i-1}\cdot r_i}$ and since $S_{r_1\cdot r_2\ldots\cdot r_{i-1}\cdot r_i} \subseteq S_{r_1} \cap S_{r_2} \ldots \cap S_{r_{i-1}} \cap S_{r_i}$, so the collection of sets $\{S_i : i \in \mathbb{N}\}$ has the finite intersection property. By compactness, $\bigcap_{i\in\mathbb{N}} S_i$ is non-empty. Thus we are reduced to the following subclaim:

Subclaim: For any $r \in \mathbb{N}$, S_r is closed and non-empty.

Proof that any S_r is closed: Any set S_r is closed in $\mathcal{J}$ because it is a finite union of sets of the form $\sigma_1 Y \times \tau_1 X$ where Y is a coset of $\mathrm{Gal}(F_r)$ in $\mathrm{Gal}(F)$ and X is a coset of $\mathrm{Gal}(E_r)$ in $\mathrm{Gal}(E)$.

Proof that any S_r is not empty: This is more complicated. Principally, we use axiom scheme (iv): using that axiom scheme, pick some x extending σ on F_r with $\mathrm{Fix}(\mathrm{Frob}^m(x)^n) = F$. We shall restrict x to $F_r \cap \tilde{K}$ and then try to lift the restriction to some $y \in$Aut$(\tilde{E})$ so that $(x, y) \in S_r$.

To begin, let $K_{r'} = \tilde{K} \cap F_r$ and $x' = x|_{K_{r'}}$ where $r' = [K_{r'} : K]$. Then notice $r' \leq r$. If not, then there is some $h \in F_r$ which generates a finite extension of K of finite degree r^*

with $r^* > r$. But then let us make a similar argument to that in 3.3.9: let $m_h \in K[X]$ be the minimal polynomial for h over K. Since m_h must partially factorise over F, say with factor m_h^*, then $m_h^* \in F[X] \cap (\tilde{K}[X] \backslash K[X]) = \emptyset$, since K is relatively algebraically closed in F. This contradiction proves $r' \leq r$. Also, since K is algebraically closed in E, a similar argument shows that $E_{r'} = EK_{r'}$.

Now let us show that x' extends to $x'' \in \mathrm{Aut}(E_{r'})$ with (a) $x''|_E = \tau$ and (b) $\mathrm{Fix}(\mathrm{Frob}^m(x'')^n) = E$.

For (a), $E_{r'} = E(a)$ for some $a \in K_{r'}$. Let M_a be a minimal polynomial for a/E. We assume $M_a \in K[X]$. Denote by $\tau(M_a)$ the polynomial obtained by applying τ to the coefficients of M_a. The automorphisms of $E_{r'}$ extending τ are exactly those obtained by picking any root R of $\tau(M_a)$ and mapping a to R: on the one hand, clearly it is necessary that under any automorphism extending τ, that a be mapped to a root of $\tau(M_a)$. On the other hand, let R be a root of $\tau(M_a)$. Then $\tau(M_a)$ must be irreducible over E and by the uniqueness of r'-degree extensions result (3.3.9) it follows that $R \in K(a)$. Let $E[X]$ be the polynomial ring in one variable. So τ extends to an automorphism of $E[X]$, and we have, for any $\alpha \in \tilde{E}$, the homomorphism $f_\alpha : E[X] \mapsto E[\alpha]$, where $f_\alpha(X) = \alpha$, and $f|_E =$id. So, consider the map $f_R \circ \tau : E[X] \mapsto E_{r'}$. The kernel of the map is $\langle M_a \rangle$, and so there is an isomorphism $g_1 : E[X]/\langle M_a \rangle \cong E_{r'}$, where $g_1(X + \langle M_a \rangle) = R$, and $g_1|_E = \tau$. Now f_a induces an isomorphism $g_2 : E[X]/\langle M_a \rangle \cong E_{r'}$ with $g_2|_E$ the identity and $g_2(X + \langle M_a \rangle) = a$. The unique automorphism of $E_{r'}$ extending τ and mapping a to R is then $g_1 g_2^{-1}$. Let us apply this: since $\sigma|_K = \tau|_K$ we may find an automorphism x'' of $E_{r'}$ such that $x''(a) := x'(a)$. Then x'' satisfies (a).

For (b), by 3.3.9, $K_{r'}/K$ is a normal extension. It is also finite and since K is perfect, it is separable; so it is Galois. Also, we quote the following lemma which is proved in [6] pp.34: 'Suppose G is a finite group, and suppose that for any $m|\mathrm{order}(G)$, that G has at most one subgroup of order m. Then G is cyclic.' By this lemma, and by the Galois correspondence, $\mathrm{Gal}(E_{r'}/E)$ and $\mathrm{Gal}(K_{r'}/K)$ are both cyclic groups of order r'. Again, by the elementary Galois correspondence, the subfield lattices for the extensions $E_{r'}/E$ and $K_{r'}/K$ are identical, so that every subfield E' with $E \subseteq E' \subseteq E_{r'}$,

has the form $E' = EK'$ where $K \subseteq K' \subseteq K_{r'}$. So if x'' does not satisfy (b), then let $E' = \mathrm{Fix}(\mathrm{Frob}^m(x'')^n)$. Then $E' = EK'$ and $K' \neq K$. But on K', $x'' = x'$, and that contradicts our choice of x'.

Now we must lift x'' to some y on E_r so that the $\mathrm{Fix}(\mathrm{Frob}^m y^n) = E$. This is a direct application of axiom scheme (iv). Note that x'' is an automorphism of $E_{r'}$ generic over E. So by axiom scheme (iv) there is $y \in \mathrm{Aut}(E_r)$ extending x'' such that y is generic over E. So S_r is not empty.

End of proof of Subclaim and proof of Claim □

3.3.3 Deducing an Elimination Form

Having proved Theorem 3.3.10 we show that, as in pseudo-finite fields, we can deduce an *almost* $\exists_1$ form for formulas: we show that, analogously to pseudo-finite fields, every definable set $\theta(\bar{x})$ is a boolean combination of projections of σ-closed sets in variables $\bar{x}, y$, where y is a single variable. This places our theory in the middle of pseudo-finite fields and $ACFA$.

In this section, we shall present general logical results modulo an arbitrary theory T in a language $\mathcal{L}$, and then we shall present further results after specifying both $\mathcal{L}$ and T. Generally, suppose Δ is a set of formulas over $\emptyset$ and for any type p over $\emptyset$ let us define $p_\Delta = p \cap \Delta$. Let conj/disj(Δ) be the collection of all finite conjunctions and disjunctions of Δ-formulas - that is, formulas in Δ.

Most general assumption: T is an arbitrary theory in an arbitrary language $\mathcal{L}$.

We begin with a very standard type of result:

LEMMA 3.3.11 *Suppose that $p_\Delta \vdash p$ for any consistent type p over $\emptyset$. Let $\theta \in \mathcal{L}$. Then there is $\varphi_\theta \in$ conj/disj(Δ) such that*

$$T \vdash \theta \Leftrightarrow \varphi_\theta$$

PROOF Clearly any formula θ consistent with T lies in some type p, and since $p_\Delta \vdash p$,

then by compactness θ is implied by a conjunction of Δ-formulas. Let $\Phi \subseteq \text{conj/disj}(\Delta)$ be the subset of conj/disj(Δ) of formulas that imply θ. Suppose θ implies no member of Φ. Clearly Φ is closed under disjunctions, so by compactness the partial type $p_0 = \{\neg\varphi : \varphi \in \Phi\} \cup \theta$ is consistent. Extending p_0 to a type p, we can apply the hypothesis: $p_\Delta \vdash p$. In particular, there is a formula $\varphi_\theta \in \text{conj/disj}(\Delta) \cap p$ such that $\varphi_\theta \Rightarrow \theta$. But our construction forbids that and we have a contradiction.□

More specific assumption on T and $\mathcal{L}$: Now suppose $\mathcal{L} = \mathcal{L}_{\text{diff}}$ and T is a theory in $\mathcal{L}$ such that

1. $T \models$'σ is an automorphism'.
2. If (M, σ) and (N, τ) are both models of T, and K is an $\mathcal{L}$-substructure of each, then $M \equiv_K N \Leftrightarrow (M \cap \tilde{K}, \sigma) \cong_K (N \cap \tilde{K}, \tau)$.

LEMMA 3.3.12 *Let K be a substructure of both $M \models T$ and $N \models T$. Let $\bar{a} \in M$ and $\bar{b} \in N$ be tuples of elements. Then* $\text{tp}(\bar{a}/K) = \text{tp}(\bar{b}/K)$ *as $\mathcal{L}_{\text{diff}}(K)$-types, iff there is a difference field K-isomorphism* $\text{acl}_\sigma^M(K(\bar{a})) \mapsto \text{acl}_\sigma^N(K(\bar{b}))$ *sending $\bar{a}$ to $\bar{b}$.*

PROOF ($\Leftarrow$) Let $i_0 : \text{acl}_\sigma^M(K(\bar{a})) \mapsto \text{acl}_\sigma^N(K(\bar{b}))$ be the given isomorphism. By elementary model theory, there is an $\mathcal{L}_{\text{diff}}$-structure M' containing $\text{acl}_\sigma^N(K(\bar{b}))$ such that we may extend i_0 to an isomorphism of $\mathcal{L}_{\text{diff}}$-structures $i : M \mapsto M'$. Then by (2) in the assumptions above, $M' \equiv_{K(\bar{b})} N$. So $\text{tp}(\bar{b})$ in M' is the same as $\text{tp}(\bar{b})$ in N. Now pulling back by the K-isomorphism i_0, we have $\text{tp}(\bar{b}/K)$=$\text{tp}(\bar{a}/K)$.

($\Rightarrow$) The assumption allows us to extend M and N elementarily to saturated enough models M' and N' of the same cardinality, so that there is an isomorphism $i : M' \mapsto N'$ taking $\bar{a}$ to $\bar{b}$ and such that i is the identity on K. We get the desired isomorphism of substructures by restricting i. □

Even more specific assumption on T and $\mathcal{L}$: Now we let $T = PSF_{(m,n,p)}$.

REMARK 3.3.13 We describe a set Δ of $\mathcal{L}_{\text{diff}}$-formulae over $\emptyset$, and a set Δ_c of $\mathcal{L}_{\text{diff},c}$-formulae over $\emptyset$ (see Section 3.3.2). We shall refer to polynomial equations: by this we mean equations with the left hand side of some specific polynomial/difference polynomial type, and the right hand side set to be 0.

1. A δ_0-formula $\delta(y, \bar{x})$ is just a σ-polynomial equation in σ-iterates of both y and $\bar{x}$, where y is a single variable.

2. A δ_1'-formula $\delta_1'(y, \bar{x})$ is a difference polynomial in y and $\bar{x}$, but a pure algebraic polynomial equation (i.e with no use of σ-iterates) in y, with y a single variable.

3. Consider a δ_1'-formula as a polynomial equation in y whose coefficients are difference polynomial expressions of $\bar{x}$. Assume an index J on the coefficient polynomials. Then a δ_1-formula is a formula $\delta_1'(y, \bar{x}) \wedge C_I(\bar{x})$ such that $I \subseteq J$ and $C_I(\bar{x})$ states that the coefficient difference polynomials indexed by I are not all identically zero. If the coefficient expressions are $C_i(\bar{x})$ $(i \in J)$, $C_I(\bar{x})$ can be expressed as $\exists t \prod_{i \in I}(C_i \cdot t - 1) = 0$. A non-trivial δ_1-formula is one where $I \neq \emptyset$.

4. A δ-formula is $\delta(\bar{x}) = \exists y(\delta_0(y, \bar{x}) \wedge \delta_1(y, \bar{x}))$, where the δ_1-conjunct is non-trivial. Notice that the existential quantifier inside the δ_1-conjunct can be brought outside: the result is that a δ-formula is an existential formula $\exists yt(\theta(yt, \bar{x}))$ where θ is a conjunction of a single difference equation in variables $y\bar{x}$, a single algebraic equation in variable y with coefficient difference polynomial expressions in $\bar{x}$, and a conjunction of difference algebraic equations in variables $t\bar{x}$; the latter difference algebraic equations ensure that the map $\theta(yt, \bar{x}) \mapsto \bar{x}$ has finite fibres bounded by some natural number N_θ.

5. We let Δ be the set of formulas boolean(δ) (boolean combinations of δ-formulas).

6. We can also consider the theory $T_c = PSF_{(m,n,p,c)}$ in the language $\mathcal{L}_{\text{diff},c}$, as described in the beginning of Se ction 3.3.2. For T_c, we can define a δ-formula similarly. The only difference is that the constants c and their σ-iterates are allowed in the δ_0,$\delta_1^{'}$ and C_I formulae. In this case we are more interested in Δ_c, the set of *positive* boolean combinations of δ-formulas.

7. There is a simplification of quantifiers result for pure pseudo-finite fields (see [6] 5.11 through 5.17). That simplification implies that there is a sub-type Δ^* of the pure field type $\text{tp}_{\text{field}}(\bar{a})$ such that $\Delta^* \vdash \text{tp}_{\text{field}}(\bar{a})$, and $\Delta^* \subseteq \text{tp}(\bar{a})_\Delta$. Similarly, let $\text{tp}_{\text{field},c}(\bar{a})$ be the type of $\bar{a}$ in the language $\mathcal{L}_{\text{rings},c}$. Then [6] 5.17 implies that there is a sub-type Δ_c^* of the type $\text{tp}_{\text{field},c}(\bar{a})$ such that $\Delta_c^* \vdash \text{tp}_{\text{field},c}(\bar{a})$, and $\Delta_c^* \subseteq \text{tp}(\bar{a})_{\Delta_c}$.

8. The quantifier-free type of $\bar{a}$ is determined by the difference polynomial equations $\varphi(\bar{x})$ which $\bar{a}$ satisfies, and by the difference polynomial equations $\varphi(\bar{x})$ which $\bar{a}$ does not satisfy. Take any difference polynomial equation $\varphi(\bar{x})$: it is a δ_0-formula. Also, if $\bar{x} = x_1, \ldots, x_k$, then consider the algebraic equation $f(\bar{x}, y) =_{\text{def}} \ y - x_1 = 0$. Since the coefficient of y in this algebraic equation is 1, we have the δ_1'-formula $f^*(\bar{x}, y) =_{\text{def}} \ f(\bar{x}, y) \wedge \exists t(t \cdot 1 - 1 = 0)$. Notice that the δ-formula $\exists y(\varphi(\bar{x}) \wedge f^*(\bar{x}, y))$ is equivalent to $\varphi(\bar{x})$, and thus, $\neg\exists y(\varphi(\bar{x}) \wedge f^*(\bar{x}, y))$ is equivalent to $\neg\varphi(\bar{x})$. Since Δ is the set of boolean combinations of δ-formulas, we have $\text{tp}(\bar{a})_\Delta \vdash \text{tp}_{\text{quantifier free}}(\bar{a})$.

   Even though Δ_c is defined as the positive boolean combinations of δ-formulas in $\mathcal{L}_{\text{diff},c}$, we still have $\text{tp}(\bar{a})_\Delta = \text{tp}(\bar{b})_\Delta$ only if $\text{tp}_{\text{quantifier free}}(\bar{a}) = \text{tp}_{\text{quantifier free}}(\bar{b})$, since the assumption that $\text{tp}(\bar{a})_\Delta = \text{tp}(\bar{b})_\Delta$ implies that $\text{tp}(\bar{a})$ and $\text{tp}(\bar{b})$ must agree on all boolean combinations of δ-formulas.

THEOREM 3.3.14 *(i) Let $\mathcal{L}=\mathcal{L}_{\text{diff}}$ and Δ be as in remark 3.3.13. For any $\mathcal{L}$-formula $\theta(\bar{x})$ there is $\delta \in \Delta$ and $PSF_{(m,n,p)} \vdash \theta \Leftrightarrow \delta$.*

(ii) In the expansion $\mathcal{L}_c$ there is $\delta \in \Delta_c$ and $PSF_{(m,n,p,c)} \vdash \theta \Leftrightarrow \delta$. We call this $\exists_1'$ form.

PROOF We will prove (i). The proof for (ii) is a simple relativisation of that for (i); if there is an important detail required for the relativisation we mention it.

The set of formulae Δ is closed under conjunctions and disjunctions. Thus, by 3.3.11 it suffices to show that Δ-formulae determine $\mathcal{L}_{\text{diff}}$-types modulo $PSF_{(m,n,p)}$. Suppose (M, σ) and (N, τ) are two models of $PSF_{(m,n,p)}$. Suppose that K is the prime field of both M and N (for the relativisation of the proof to (ii), suppose that $K_c(M)$ and $K_c(N)$ are the difference subfields of M and N generated by the distinguished constants c). Suppose we have tuples $\bar{a} \in M$ and $\bar{b} \in N$ of the same length. Then by 3.3.12 and by 3.3.10, if there is a K-isomorphism of difference fields between $\text{acl}_\sigma^M(K(\bar{a}))$ and $\text{acl}_\tau^N(K(\bar{b}))$ taking $\bar{a}$ to $\bar{b}$, then $\text{tp}(\bar{a}) = \text{tp}(\bar{b})$. So it is sufficient to

show that $\mathrm{tp}(\bar{a})_\Delta = \mathrm{tp}(\bar{b})_\Delta$ only if there is a K-isomorphism of difference fields between $\mathrm{acl}^M_\sigma(K(\bar{a}))$ and $\mathrm{acl}^N_\tau(K(\bar{b}))$ taking $\bar{a}$ to $\bar{b}$.

Firstly, by 3.3.13 (8), $\mathrm{tp}_{\text{quantifier free}}(\bar{a}) = \mathrm{tp}_{\text{quantifier free}}(\bar{b})$, (and also in the relativisation to (ii) this is true for the quantifier-free $\mathcal{L}_{\mathrm{diff},c}$-types), so there is a unique isomorphism $f : (K(\bar{a})_\sigma, \sigma) \cong (K(\bar{b})_\tau, \tau)$ that takes $\bar{b}$ to $\bar{a}$, and is identity on K. Thus, we can assume $K(\bar{a})_\sigma = K(\bar{b})_\tau$, and by extending f^{-1} we can identify $\mathrm{acl}^N_\tau(K(\bar{b}))$ with a subfield of $\widetilde{K(\bar{a})_\sigma}$ denoted K_2. We do this, and we also let $K_1 = \mathrm{acl}^M_\sigma(K(\bar{a}))$. Expand K_1 to a difference field by equipping it with the restriction of σ. Expand $\mathrm{acl}^N_\tau(K(\bar{b}))$ to a difference field by equipping it with τ, and then expand K_2 to a difference field by equipping it with the automorphism $f(\tau) = f^{-1}\tau f$.

Relabelling and setting notation, the problem is now reduced to exhibiting an isomorphism between the difference fields (K_1, σ) and (K_2, τ), where

- (K_1, σ) and (K_2, τ) share a common difference subfield (B, σ_B), where $B = K(\bar{a})_\sigma = f(K(\bar{b})_\tau$, and σ_B is the restriction of σ to B.
- $K_1 = \mathrm{acl}^M_\sigma(K(\bar{a}))$, $K_2 = \mathrm{acl}^N_\sigma(K(\bar{a}))$ with (M, σ), $(N, \tau) \models PSF_{(m,n,p)}$
- $\mathrm{tp}(\bar{a})_\Delta = \mathrm{tp}(\bar{b})_\Delta$.

By 3.3.13 (7) it follows that K_1 and K_2 are isomorphic over B as fields. For the relativisation of the proof to (ii), also by 3.3.13 (7), there is an isomorphism between K_{1c} and K_{2c} over B_c as fields with constants.

By this isomorphism, we must have the equality $K_1 \cap B^{\mathrm{ins}} = K_2 \cap B^{\mathrm{ins}}$ (see the preliminary section to this chapter for notation). In algebraic, purely inseparable extensions of difference fields, the difference operator extends uniquely. So there is a unique extension of σ_B to $K_1 \cap B^{\mathrm{ins}}$; σ and τ must both restrict to this unique extension. So we let $B^* = K_1 \cap B^{\mathrm{ins}} = K_2 \cap B^{\mathrm{ins}}$, and see that τ and σ agree on B^*. Both extensions K_i/B^* ($i = 1$ or 2) are separable.

For L a Galois extension of B^* we let $S_L = \{g \in \mathrm{Gal}(B^*)$: g gives an isomorphism from $L \cap K_1$ *onto* $L \cap K_2$ and $\forall x \in L \cap K_1$ $g\sigma(x) = \tau g(x)\}$. Then S_L is closed in $\mathrm{Gal}(B^*)$,

since it is a union of cosets of $\mathrm{Gal}(L)$. We aim to show that the set of all S_L has the finite intersection property.

Since we have shown that $K_1 \cong_{B^*} K_2$, by restriction we have $L \cap K_1 \cong_{B^*} L \cap K_2$, for any Galois L/B. Denote the isomorphic fields $L \cap K_1$ and $L \cap K_2$ as L_1 and L_2 respectively. Since L_i/B^* is separable for $i = 1$ or 2, we have primitive elements: $L_1 = B^*(\alpha)$, $L_2 = B^*(\beta)$ and $\alpha,\ \beta$ are roots of some irreducible $f(X) \in B^*[X]$.

To prove the finite intersection property, we aim to show that for each L, $S_L \neq \emptyset$.

Claim: The composite fields $\langle L_1, \sigma(L_1)\rangle$ and $\langle L_2, \tau(L_2)\rangle$ are isomorphic over B^*.

Proof of Claim: Take an isomorphism $\gamma :\ K_1 \cong_{B^*} K_2$. Under γ a root of $\sigma^j(f(X))$ $(0 \leq j \leq 1)$ goes to a root of $\sigma^j(f(X))$. L_1 is the unique subfield of K_1 generated over B^* by a root of $f(X)$: for any such field is contained in L, and $L \cap K_1 = L_1$, so it must be unique. By applying the difference operator, we see $\sigma^j(L_1)$ $(0 \leq j \leq 1)$ is the unique subfield of K_1 generated over B^* by a root of $\sigma^j(f(X))$. Analogously, $\tau^j(L_2)$ $(0 \leq j \leq 1)$ is the unique subfield of K_2 generated over B^* by a root of $\tau^j(f(X)) = \sigma^j(f(X))$. Thus $\gamma(L_1) = L_2$ and $\gamma(\sigma(L_1)) = \tau(L_2)$ and so γ witnesses the claim. **End of proof of claim**

Consider the algebraic-geometric type of the pair $(\alpha, \sigma(\alpha))/B^*$. It is isolated by the monic minimal polynomial (Min_α) equation of α/B^* and the monic minimal polynomial equation $(\mathrm{Min}_{\sigma(\alpha)})$ of $\sigma(\alpha)/B^*(\alpha)$. Now Min_α and $\mathrm{Min}_{\sigma(\alpha)}$ can be seen as a pair of difference equations in α with coefficients from B^*. It follows that

$$(K_1, \sigma) \models \exists y\ (\mathrm{Min}_\alpha(y) \wedge\ \mathrm{Min}_{\sigma(\alpha)}(\sigma(y))) \tag{3.5}$$

Ostensibly, this formula makes use of parameters in $B^* \backslash B$. However, since $B^* \subseteq B^{\mathrm{ins}}$, it follows that there is $l \in \mathbb{N}$ such that there are difference polynomials $M_\alpha = (\mathrm{Min}_\alpha)^{p^l}$ and $M_{\sigma(\alpha)} = (\mathrm{Min}_{\sigma(\alpha)})^{p^l}$ where M_α is a purely algebraic, monic polynomial in y, where the coefficients of M_α and $M_{\sigma(\alpha)}$ are over B, and such that modulo the theory of

characteristic-p fields

$$\forall y[(\mathrm{Min}_\alpha(y) \wedge \ \mathrm{Min}_{\sigma(\alpha)}(\sigma(y))) \Leftrightarrow \ (M_\alpha(y) \wedge \ M_{\sigma(\alpha)}(\sigma(y))] \tag{3.6}$$

Notice that we may now see $\exists y \ (M_\alpha(y) \wedge \ M_{\sigma(\alpha)}(y))$ as a sentence in parameters $\bar{a}$. Substituting $\bar{x}$ for $\bar{a}$, we have a formula $\theta(\bar{x}) =_{\mathrm{def}} \ \exists y \ (M_\alpha(y) \wedge \ M_{\sigma(\alpha)}(y))$, where $\theta(\bar{x}) \in \mathrm{tp}_\sigma(\bar{a})$. For the relativisation to (ii), $\theta(\bar{x})$ only uses parameters in the field K_c generated by the distinguished constants. Either way, $\theta(\bar{x})$ is definable without parameters. Since $M_\alpha(y, \bar{x})$ is purely algebraic and monic as a y-polynomial equation, it follows that $\theta(\bar{x})$ can be assumed to be a formula in $\mathrm{tp}(\bar{a})_\Delta$. So, by assumption, $\theta(\bar{x})$ is in $\mathrm{tp}(\bar{a})_\Delta$ as measured in K_2. So, by expression 3.6

$$(K_2, \tau) \models \exists y \ (\mathrm{Min}_\alpha(y) \wedge \ \mathrm{Min}_{\sigma(\alpha)}(\sigma(y))) \tag{3.7}$$

Let β be a witness for $\exists y \ (\mathrm{Min}_\alpha(y) \wedge \mathrm{Min}_{\sigma(\alpha)}(\sigma(y)))$ in K_2. By the uniqueness described in the claim above, $L_2 = B^*(\beta)$ and $\tau(L_2) = B^*(\tau(\beta))$. The isomorphism $L_1 \mapsto L_2$ given by sending α to β over B^*, maps $\mathrm{Min}_{\sigma(\alpha)}$ to an irreducible polynomial over L_2 satisfied by $\tau(\beta)$. So there is an embedding of $\langle L_1, \sigma(L_1)\rangle$ into $\langle L_2, \tau(L_2)\rangle$. But it is onto because the image contains B^*, β and $\tau(\beta)$. Lift this isomorphism to an element g of $\mathrm{Gal}(B^*)$. So $g \in S_L$.

The rest is standard. Let $L_1, L_2, \ldots, L_k$ be an arbitrary collection of finite extensions of B^*. Let L be the normal closure of the composite $L_1 L_2 \ldots L_k$ over B^*. Since $\emptyset \neq S_L$ and $S_L \subseteq S_{L_1} \cap S_{L_2} \cap \ldots \cap S_{L_k}$ this set of closed sets has the finite intersection property, and by compactness of $\mathrm{Gal}(B^*)$ there is $g^* \in \bigcap_{L/B^* \text{ normal}} S_L$. Thus g^* is the isomorphism we sought. $\square$

3.3.4 Theory of almost all fractional powers of the Frobenius

In this section we show that $PSF_{(m,n,p)}$ is the theory of almost all finite difference fields of a specific kind. For completeness we also recall the decidability results.

THEOREM 3.3.15 *Let n and m be coprime natural numbers and p a prime. $PSF_{(m,n,p)}$ is the asymptotic theory of the class of finite difference fields $\mathcal{C}_{(m,n,p)} = \{(\mathbb{F}_{p^{kn+m}}, \mathrm{Frob}^k) : k \in \mathbb{N}\}$. That is, every model of $PSF_{(m,n,p)}$ is elementarily equivalent to a non-principal ultraproduct of members of $\mathcal{C}_{(m,n,p)}$, and every non-principal ultraproduct of members*

of $\mathcal{C}_{(m,n,p)}$ is a model of $PSF_{(m,n,p)}$.

PROOF Let $\mathcal{D}$ =$\{$non-principal ultraproducts of members of $\mathcal{C}_{(m,n,p)}\}$. We start by showing that every member $D \in \mathcal{D}$ is a model of $PSF_{(m,n,p)}$. Recall that by Lemma 3.3.5, in any $(M,\sigma) \models ACFA$, the substructure $(\mathrm{Fix}(\mathrm{Frob}^m \circ \sigma^n), \sigma|_{\mathrm{Fix}(\mathrm{Frob}^m \circ \sigma^n)})$ is a model of $PSF_{(m,n,p)}$. So consider $D \in \mathcal{D}$. Suppose $D = \prod_{i\in\mathbb{N}}(\mathbb{F}_{p^{nk_i+m}}, \mathrm{Frob}^{k_i})/\sim \mathcal{U}$ where $\mathcal{U}$ is a non-principal ultrafilter on $\mathbb{N}$. Let $(M,\sigma) = \prod_{i\in\mathbb{N}}(\tilde{\mathbb{F}}_p, \mathrm{Frob}^{k_i})/\sim_{\mathcal{U}}$. By the elementary equivalence theorem for $ACFA$, $(M,\sigma) \models ACFA$. But $D = (\mathrm{Fix}(\mathrm{Frob}^m \circ \sigma^n)(M), \sigma|_{\mathrm{Fix}(\mathrm{Frob}^m \circ \sigma^n)(M)})$. So $D \models PSF_{(m,n,p)}$.

Now we need only show that every model of $PSF_{(m,n,p)}$ is elementarily equivalent to some model in $\mathcal{D}$. Take an arbitrary model $(M,\sigma) \models PSF_{(m,n,p)}$. Then by Lemma 3.3.6 we may extend $(M,\sigma) \subseteq (\tilde{M},\tilde{\sigma})$ such that $\mathrm{Fix}(\mathrm{Frob}^m\tilde{\sigma}^n)(\tilde{M}) = M$. Since $ACFA$ is the model companion of difference fields we may embed $(\tilde{M},\tilde{\sigma}) \subseteq (K,\tau)$ where $(K,\tau) \models ACFA$. Let $(K',\tau') = (\mathrm{Fix}(\mathrm{Frob}^m\tau^n)(K), \tau|_{\mathrm{Fix}(\mathrm{Frob}^m\tau^n)(K)})$. It is clear by the elementary equivalence theorem for $ACFA$ (see Theorem 2.1.3) that $(K',\tau') \equiv D$ for some $D \in \mathcal{D}$. Notice that M is algebraically closed in K'. So by 3.3.10 we have $(M,\sigma) \equiv (K',\tau') \equiv D$. $\square$

As to the decidability, there is not much to say. It is proved in [8] that the theory $ACFA$ is decidable. The proof there can be directly translated to a proof of the decidability of $PSF_{(m,n,p)}$. One can also see it this way: by the theorem above, $PSF_{(m,n,p)}$ is interpretable in $ACFA_p$, and so its decidability follows from the decidability of $ACFA_p$ (a proof of the decidability of $ACFA_p$ may be found in [8] 1.6).

3.3.5 Tools: analogues for theorems about $ACFA$

This section relativises results from $ACFA$ to $PSF_{(m,n,p)}$. The statements may be useful for a reader.

Suppose $(M,\sigma) \models PSF_{(m,n,p)}$. Let Θ be the $\mathcal{L}_{\mathrm{diff}}$-formula defining the substructure $\mathrm{Fix}(\mathrm{Frob}^m\sigma^n)$. Notice that Θ is quantifier-free. By Theorem 3.3.15 there is a model $(K,\tau) \models ACFA$ such that $(M,\sigma) \equiv ((\Theta(K), \tau|_{\Theta(K)})$. We may assume

(K, τ) is $|M|$-saturated, and this yields $|M|$-saturation for the definable substructure $(\Theta(K), \tau|_{\Theta(K)})$. Thus we may assume that (M, σ) embeds elementarily into $(\Theta(K), \tau|_{\Theta(K)})$. For ease of notation, in the following lemmas let us just use the symbol σ for the automorphism, ignoring the domain in question: we assume the elementary embedding $(M, \sigma) \prec (\Theta(K), \sigma) \subset (K, \sigma)$ with $(K, \sigma) \models ACFA$ for the following lemmas. We also assume ω_1-saturation of (K, σ).

PROPOSITION 3.3.16 *The model-theoretic and algebraic notions of algebraic closure over a substructure coincide in models of $PSF_{(m,n,p)}$.*

PROOF Let $(E, \sigma) \subseteq (M, \sigma)$ be a substructure that is algebraically closed inside M, in the sense of fields. Say $a \in M \backslash E$. But then $a \in K \backslash \tilde{E}$, and $(\tilde{E}, \sigma)$ is an algebraically closed substructure of (K, σ) in the sense of fields. By [8] Proposition 1.7, a is not model-theoretically algebraic over $\tilde{E}$ in (K, σ). Thus a is not model-theoretically algebraic over E in (M, σ). $\square$

So, as in $ACFA$, we can identify the model-theoretic algebraic closure of a set $A \subseteq M$ with $\mathrm{acl}_\sigma^M(A)$ (see 3.2 for a definition of $\mathrm{acl}_\sigma^M(A)$).

Let $\bar{X} = (X_1, X_2, \ldots X_k)$ be indeterminates. We let $\mathbb{Z}\langle \bar{X} \rangle$ be the free commutative σ-algebra generated by the X_i over $\mathbb{Z}$.

PROPOSITION 3.3.17 *Given $\psi(\bar{x}, y)$ with $\bar{x}$ a tuple and y a single variable, there are difference polynomials $f_1(\bar{X}, Y), \ldots, f_m(\bar{X}, Y)$, with each $f_i \in \mathbb{Z}\langle \bar{X} \rangle[Y]$, such that for every model M of $PSF_{(m,n,p)}$ and tuple $\bar{a}$ from M, if $\psi(\bar{a}, M)$ is finite, then it is included in the set of zeroes of $f_i(\bar{a}, Y)$, for some i such that $f_i(\bar{a}, Y)$ is a non-trivial polynomial in Y.*

PROOF The statement is exactly the same as the statement in [8] 1.8 for $ACFA$. The proof follows from [8] 1.8, because $PSF_{(m,n,p)}$ is interpretable in $ACFA_p$, and the quantifier-free $f_i(\bar{X}, Y)$ are interpreted as themselves. $\square$

In the following, we briefly describe the model-theoretic theory of independence for $PSF_{(m,n,p)}$. We make use of the general theory of independence, in particular, the

relation $\downarrow$, the notion of supersimplicity, Morley sequences, and the notion of model-theoretic *dividing*. A good general reference for this theory is [29]; in particular, section 2.2 and chapter 5.

PROPOSITION 3.3.18 *Let independence in the sense of $(\Theta(K), \sigma)$ be $\downarrow$. Let independence in the sense of (K, σ) be $\downarrow^{ACFA}$. Let independence in the sense of algebraically closed fields be $\downarrow^{\mathrm{acf}}$. Let $\bar{a}$ and $\bar{b}$ be tuples from $\Theta(K)$, and let $(E, \sigma) \subseteq (\Theta(K), \sigma)$ be an algebraically closed substructure such that K is $(|E| + \omega_1)$-saturated. Then*

1. *$\bar{a} \downarrow_E \bar{b}$ if and only if $\bar{a} \downarrow_E^{ACFA} \bar{b}$*

2. *$\bar{a} \downarrow_E \bar{b}$ if and only if $\mathrm{acl}_\sigma(\bar{a}E) \downarrow_E^{\mathrm{acf}} \mathrm{acl}_\sigma(\bar{b}E)$*

PROOF 1. We recall that $\mathrm{Th}(\Theta(K))$ is supersimple, because any model is elementarily equivalent to a definable substructure of a model of $ACFA$. Thus we may use *dividing* as our notion of forking.

($\Leftarrow$) A witness to dividing on the left-hand-side is a k-inconsistent set of formulas $\{\theta(\bar{x}, \bar{b}_i\bar{e}) : i \in \omega\}$ such that $\bar{b}_0 = \bar{b}$, $\bar{e} \in E$, the $\bar{b}_i$ are distinct, and for each $i \in \omega$ we have that $\mathrm{tp}(\bar{b}_i/E) = \mathrm{tp}(\bar{b}/E)$ and $(\Theta(K), \sigma) \models \theta(\bar{a}, \bar{b}_i\bar{e})$. By compactness and the assumption of $|E|$-saturation, we may assume that for each $i \in \omega$ we have that $\mathrm{tp}^{ACFA}(\bar{b}_i/E) = \mathrm{tp}^{ACFA}(\bar{b}/E)$. Here, tp^{ACFA} denotes a type in (K, σ). Now $PSF_{(m,n,p)}$ is 0-interpretable in $ACFA$. So suppose the formula $\theta(\bar{x}, \bar{y}z)$ is interpreted in $ACFA$ as $\theta'(\bar{x}, \bar{y}z)$. Then $\{\theta'(\bar{x}, \bar{b}_i\bar{e}) : i \in \omega\}$ witnesses dividing on the right-hand-side.

($\Rightarrow$) If $\bar{a} \not\downarrow_E^{ACFA} \bar{b}$, then σ-degree decreases: $\deg_\sigma(\bar{a}/\mathrm{acl}_\sigma^K(E\bar{b})) < \deg_\sigma(\bar{a}/\mathrm{acl}_\sigma^K(E))$ (see [8] 2.2 Remark (2)). Since these two bases are algebraic closures of $\Theta(K)$-subsets, this inequality is equivalent to there being some $l \in \mathbb{N}$ such that:

$$\deg_\sigma(\bar{a}/E\bar{b}\widetilde{(\sigma\bar{b})\ldots(\sigma^{l-1}\bar{b})}) < \deg_\sigma(\bar{a}/\tilde{E}) \tag{3.8}$$

So suppose that $\{a_1, a_2, \ldots a_s\} \subseteq \cup_{i=1}^{l-1}\sigma^i(\bar{a})$ is a transcendence base for $\mathrm{acl}_\sigma(E\bar{a})/E$. Then from expression 3.8, we see that there is some $1 \leq i \leq s-1$ such that a_{i+1}

is algebraic over $(E\bar{b}(\sigma\bar{b})\dots(\sigma^{l-1}\bar{b})a_1\dots a_i)$. Let $\hat{b} = \bar{b}\sigma(\bar{b})\dots\sigma^{l-1}(\bar{b})$ and let $\hat{a} = \bar{a}\sigma(\bar{a})\dots\sigma^{l-1}(\bar{a})$. So in terms of algebraically closed fields $\hat{a} \not\downarrow^{\text{acf}}_{E} \hat{b}$. So we can choose a formula $\psi(\hat{x}, \hat{b}\bar{e}) \in \mathcal{L}_{\text{rings}}(\Theta(K))$ with $\bar{e} \in E$, witnessing dividing in algebraically closed fields. Since we are now working over algebraically closed fields, we can choose ψ to be quantifier free. Also, there is a quantifier-free formula $\psi^*(\bar{x}, \bar{b}, \bar{e}) \in \mathcal{L}_{\text{diff}}(\Theta(K))$ such that if $\hat{x} = \bar{x}\sigma(\bar{x})\dots\sigma^{l-1}(\bar{x})$, then $\psi^*(\bar{x}, \bar{b}, \bar{e}) = \psi(\hat{x}, \hat{b}\bar{e})$. I claim that ψ^* is the formula witnessing dividing in the difference field $(\Theta(K), \sigma)$.

We work by assuming the contrary, so in $(\Theta(K), \sigma)$, suppose that $\psi^*(\bar{x}, \bar{b}, \bar{e})$ does not divide over E. Then let us quote [29] Theorem 2.4.7 (6) (changing notation to put the result in our context):

'If T is simple then a formula $\psi^*(\bar{x}, \bar{b}\bar{e})$ does not divide over E if and only if for some Morley sequence I^* in type $\bar{b}/E$ the set $H^* = \{\psi^*(\bar{x}, \bar{b}'\bar{e}) : \bar{b}' \in I^*\}$ is consistent.'

By the saturation we have assumed, there is an $\bar{a}' \in \Theta(K)$ that satisfies all formulas of H^*. We have the Morley sequence I^*; consider the sequence $I = \{\hat{b}' = \bar{b}'\dots\sigma^{l-1}(\bar{b}') : \bar{b}' \in I^*\}$. Then I must be an $\mathcal{L}_{\text{rings}}$-Morley sequence. Let $H = \{\psi(\hat{x}, \hat{b}'\bar{e}) : \hat{b}' \in I\}$. Then $\hat{a}' = \bar{a}'\sigma(\bar{a}')\dots\sigma^{l-1}(\bar{a}')$ must satisfy all formulas of H. But then we can reapply [29] Theorem 2.4.7 (6) to show that $\psi(\hat{x}, \hat{b}\bar{e})$ does not divide over E, and that is a contradiction.

2. This now follows from 1:

$$\bar{a} \underset{E}{\downarrow} \bar{b} \;\Leftrightarrow\; \bar{a} \overset{ACFA}{\underset{E}{\downarrow}} \bar{b} \;\Leftrightarrow\; \text{acl}_\sigma(\bar{a}E) \overset{\text{acf}}{\underset{E}{\downarrow}} \text{acl}_\sigma(\bar{b}E) \qquad \square$$

Having established the notion of independence to be what is expected, we may ask whether imaginaries are eliminated in $PSF_{(m,n,p)}$. In $ACFA$, imaginaries are eliminated. There, full elimination of imaginaries followed from the generalised independence theorem, and in particular, the independence theorem holds over algebraically closed sets in $ACFA$. However, inspecting the proof of the generalised independence theorem in [8] 1.9, we cannot obviously deduce the independence theorem over algebraically closed sets in $PSF_{(m,n,p)}$. Since $PSF_{(m,n,p)}$ is a simple theory, we certainly

have the independence theorem over a model (see [29] 2.5). Using the independence theorem, Proposition 3.2 and Corollary 3.3 of [15] hold in $PSF_{(m,n,p)}$:

PROPOSITION 3.3.19 *Let (M,σ) be a model of $PSF_{(m,n,p)}$, and let $(N,\sigma|_N) \prec (M,\sigma)$ be an elementary submodel. Then $(M,\sigma,a)_{a\in N}$ eliminates imaginaries.*

PROOF The independence theorem over a model is the necessary ingredient to transcribe the proofs of [15] Propositions 3.2 and Corollary 3.3: the PAC set F there is replaced with the structure (M,σ) in our context. With this replacement, Corollary 3.3 of [15] is exactly our statement. □

DEFINITION 3.3.20 Let $\mathcal{L}$ be a language and N be an $\mathcal{L}$-structure and $U \subseteq N$ an $\mathcal{L}$-substructure. Let Def(N) be the set of all sets in cartesian powers of N definable in Th(N), and let Def(U) be the set of all sets in cartesian powers of U definable in Th(U). Let Def(U,N) be the set of traces of Def(N) sets in U. So Def(U,N) = $\cup_{n\in\mathbb{N}}\{X \subseteq U^n : X = Y \cap U^n \wedge Y \in \text{Def}(N)\}$. Then we say U is completely embedded in N, if Def(U)=Def(U,N).

We also need the notion of *stable embeddability*. We transcribe part of the definition from the Appendix of [8], changing notation slightly. The reader will find a much more thorough treatment there.

DEFINITION 3.3.21 Let $T = T^{eq}$ be a complete theory in a countable language, and let U be an uncountable saturated model of T. Let p be a partial r-type over the empty set and let $P = P(U)$ be the set of realisations of p in U, together with the structure induced from U, i.e. the $\emptyset$-definable subsets of P^s are the traces on P^s of $\emptyset$-definable subsets of U^{rs}. Then we say P is stably embedded if for every s, if $D \subseteq U^{rs}$ is definable, then $D \cap P^s$ is definable with parameters from P. In Lemma 1 of the Appendix of [8], various equivalent conditions for stable embeddability are presented. We note one in particular: P is stably embedded if every automorphism of P lifts to an automorphism of U.

LEMMA 3.3.22 $(\Theta(K),\sigma)$ *is completely embedded in* (K,σ).

PROOF Since $\Theta(K)$ is definable without parameters in (K, σ), it follows that Def$((\Theta(K), \sigma))$ $\subseteq$Def$((\Theta(K$

Thus we need to show that if θ is a (K, σ)-definable subset of $\Theta(K)^r$, then $\theta(\Theta(K))$ is definable in the $\mathcal{L}_{\text{diff}}$-structure $(\Theta(K), \sigma)$.

Step 1 The big step is done for us: Proposition 7.1 (5) of [9] tells us that $\Theta(K)$ is stably embedded in (K, σ). Thus we may assume that θ is definable with parameters from $\Theta(K)$.

Step 2 Consider the elimination form for $ACFA$ described in 2.3.1. By that form we may also assume that $\theta = \bigvee_{i=1}^{k} \exists t\ \theta_i(x, b, t)$ with $b \in \Theta(K)$, and t a single variable and each θ_i a quantifier-free $\mathcal{L}_{\text{diff}}$-formula in parameters b. Clearly it suffices to assume that $k = 1$. Next, we can put θ_1 in conjunctive-disjunctive form ($\bigvee \wedge$); at this stage it is clear that it suffices to assume that θ_1 consisists of a single disjunct. Now we recall the additional feature of the elimination form in 2.3.1: there is an $r \in \mathbb{N}$ such that if $x_0 \in K$ then $\theta_1(x_0, b, t)$ has at most r solutions in t. This means that for $\theta_1(\Theta(K))$, all such solutions must lie in the unique r-degree extension of $\Theta(K)$. But the unique r-degree extension of $\Theta(K)$ and the extension of σ to any particular automorphism of that extension are parameter definable in $(\Theta(K), \sigma)$. So it follows that $\theta_1(x, b, t)(\Theta(K))$ may be defined by a formula in $(\Theta(K), \sigma)$, and then so too can $\exists t(\theta_1(x, b, t))(\Theta(K))$. □

3.4 Definable automorphisms of a perfect bounded PAC field

Let us remind ourselves that K is pseudo-algebraically closed (PAC) if every absolutely irreducible variety defined over K has a K-rational point. K is said to be bounded if its absolute Galois group Gal(K) is *small*, namely has, for any $n \in \mathbb{N}$, only finitely many open subgroups of index n. Equivalently, K has only finitely many extensions of degree n for any n (see [17] Definition 1.4).

This section is devoted to showing the following:

PROPOSITION 3.4.1 *Let K be a pure, perfect, bounded PAC field. Then K has no definable automorphisms apart from integer powers of the Frobenius automorphism $x \mapsto x^p$. In characteristic 0 there is only the trivial automorphism.*

At the end of the section, we use this result to characterise all infinite difference fields interpretable in a pseudo-finite field K. The proposition shows that our fractional powers of the Frobenius are genuine extensions of the theory of pseudo-finite fields. This was not immediately clear: in [9] proposition 7.1 it is shown that a model of $PSF_{(m,n,p)}$ embedded as a fixed field of a model of $ACFA$, considered with all the induced structure, has SU-rank 1. So the reduct theory $PSF_{(m,n,p)}$ that we consider also has SU-rank 1. However, the theorem we shall prove shows that the automorphism must add complexity. The proof makes use of only a few facts about algebraic groups.

In this section, we let K be a perfect, bounded PAC field. We shall use a dimension dim, as is used in [17]. For V an algebraic set with a definable subset of $X \subseteq V$, we denote the Zariski closure of X in V by $\bar{V}$. Also, an arbitrary definable set X in r variables may be seen as a subset of $\mathbb{A}^r$. We define $\dim(X)$ to be the algebraic-geometric dimension of the Zariski closure $\bar{X}$ in $\mathbb{A}^r$. Thus we may refer to the 'dimension' of a definable set, and dim is what is meant. Throughout this section we work under the assumption that σ is a definable automorphism in the language of rings (with parameters) of K. Eventually we will see that σ is a power of Frobenius. Originally this proof was seen for pseudo-finite fields, but the proof only depends on the following fact about perfect, bounded PAC fields. It is stated in [17] Fact 1.6(i):

FACT 3.4.2 Let F be a perfect, bounded PAC field. If $X \subseteq F^n$, $Y \subseteq F^m$ are definable in F, $f : X \mapsto Y$ is a definable surjection and $\dim(f^{-1}(a)) = d$ for all $a \in Y$, then $\dim(X) = \dim(Y) + d$.

This fact will eventually allow us to extend the definable automorphism σ of K to a definable automorphism of $\tilde{K}$.

DEFINITION 3.4.3 An algebraic group, G , will be an abstract variety over $\tilde{K}$ with two morphisms $\mu : G \times G \mapsto G$, and $\iota : G \mapsto G$, and an identity, e, which make G a group.

We state a well-known lemma:

LEMMA 3.4.4 *Let G be an algebraic group and $H \subseteq G$ a subgroup. Then $\bar{H}$ is an algebraic subgroup.*

DEFINITION 3.4.5 Let G_a denote the algebraic group $(\mathbb{A}^1, +)$. Let G_m denote the algebraic group $(\mathbb{A}^1 \backslash \{0\}, \cdot)$. Recall that G_a and G_m are varieties over $\tilde{K}$. Let J_a be the definable group $(\{(x, \sigma(x)) : x \in K\}, +) \subseteq G_a \times G_a$. Let J_m be the definable group $(\{(x, \sigma(x)) : x \in K \wedge x \neq 0\}, \cdot) \subseteq G_m \times G_m$. Let H_a be the closure of J_a in $G_a \times G_a$. Let H_m be the closure of J_m in $G_m \times G_m$. $\square$

LEMMA 3.4.6 *H_a and H_m both have algebraic-geometric dimension 1.*

PROOF By Fact 3.4.2, the dimension of the closure of a set defined in a perfect, bounded PAC field is preserved under a definable bijection. But either of the coordinate projections of J_a or J_m gives a bijection to a dense subset of the affine line. $\square$

LEMMA 3.4.7 *The Zariski topology on $G_m \times G_m$ is the subspace topology induced by the inclusion $G_m \times G_m \subseteq G_a \times G_a$.*

PROOF The Zariski topology on $G_m \times G_m$ is just the affine Zariski topology given by the coordinate ring $K[x, y]_{(xy)}$. The inclusion $G_m \times G_m \subseteq G_a \times G_a$ induces the inclusion of coordinate rings $K[x, y] \subseteq K[x, y]_{(xy)}$. Thus a Zariski closed set of $G_m \times G_m$ is the set of zeros of a function on the right-hand side of this inclusion, and equally well the set of zeros of its numerator, which is an element of the left-hand side, considered in $G_m \times G_m$. $\square$

LEMMA 3.4.8 *Let π_{1a} and π_{2a} denote the left and right projections of $H_a \subseteq G_a \times G_a$ into G_a, and similarly π_{1m} and π_{2m} of $H_m \subseteq G_m \times G_m$ into G_m. Then the following hold:*

1. *All the projections are onto.*

2. *For each projection, the fibres above any point are finite and equal.*

3. For $x \neq 0 \in \mathbb{A}^1$, $\mid \pi_{1a}^{-1}(x) \mid = \mid \pi_{1m}^{-1}(x) \mid$ *and* $\mid \pi_{2a}^{-1}(x) \mid = \mid \pi_{2m}^{-1}(x) \mid$.

PROOF (1) Both these projections are in fact projections of algebraic groups, so fibres are cosets or are empty. So all fibres have the same dimension and multiplicity. Because K is infinite, J_a has infinite π_{ia}-images and J_m has infinite π_{im}-images for $1 \leq i \leq 2$, and so too H_a and H_m. We have that H_a and H_m are dimension 1 (Lemma 3.4.6), so their respective π_{ia} and π_{im}-images ($1 \leq i \leq 2$) are dimension 1 subgroups of G_a and G_m respectively. A dimension 1 subgroup of a connected algebraic group is of course the group itself.

(2) Since both source and image of a given projection are dimension 1, generically the fibres must be finite. But the fibres are all cosets with natural definable bijections between them, so all fibres then have the same finite size.

(3) Firstly we show $H_m = H_a \cap G_m \times G_m$. By Lemma 3.4.7, there is a closed subset M of $G_a \times G_a$ such that $H_m = M \cap G_m \times G_m$. But then

$$H_m = M \cap G_m \times G_m = (M \cup \{0,0\}) \cap G_m \times G_m \supseteq H_a \cap G_m \times G_m \supseteq H_m \quad (3.9)$$

In expression 3.9, the first inclusion arises because $M \cup \{0,0\} \supseteq H_m \cup \{0,0\} \supseteq J_m \cup \{0,0\} = J_a$; since $M \cup \{0,0\}$ is closed in $G_a \times G_a$, it must thus contain $\bar{J_a} = H_a$. Expression 3.9 implies $H_m = H_a \cap G_m \times G_m$. This means that H_m is obtained from H_a by discarding the π_{1a} fibre over 0 and the π_{2a} fibre over 0- that is, by discarding a finite number of points. So above any generic point of $\mathbb{A}^1$ we have the stated equalities. By the fibre uniformity the equalities hold everywhere. □

LEMMA 3.4.9 *Let* $x \in \mathbb{A}^1$. *Then* $\mid \pi_{ia}^{-1}(x) \mid = 1$, ($i =$ 1 or 2). *If* $x \neq 0$ *then* $\mid \pi_{im}^{-1}(x) \mid = 1$, ($i = 1$ or 2). *Also,* H_m *is obtained from* H_a *by the removal of* $\{0,0\}$.

PROOF Consider H_a, π_{1a}, say, and the fibre above 0. It is isomorphic to a finite additive subgroup of a field, i.e. an abelian p-group of size p^r, where in the characteristic 0 case, $r = 0$. On the other hand, consider H_m, π_{1m} and the fibre above 1. It is isomorphic to a finite multiplicative subgroup of a field, i.e a group of roots of unity. In the characteristic p case its order must be coprime to p. By the uniformity of fibre

size we deduce that r=0, and the fibre size is 1. Now it follows that only the point {0,0} could have been deleted in the passage from J_a to J_m, otherwise we would have a contradiction to fibre size. The same arguments apply for π_{2a} and π_{2m}. □

Thus, Lemma 3.4.9 shows that H_a and H_m represent a definable automorphism of algebraically closed fields extending the automorphism represented by J_a and J_m.

To complete the proof of Proposition 3.4.1 we must show that the only definable automorphisms of an algebraically closed field in the language of fields are integral powers of the Frobenius automorphism. I could not find a reference.

PROPOSITION 3.4.10 *The only definable automorphisms of an algebraically closed field are powers of the Frobenius.*

PROOF Again, we suppose σ is a definable automorphism of an algebraically closed field. Let x be generic over a base of definition, B. Then $\sigma(x)$ lies in $\mathrm{dcl}(x, B)$. Since $\mathrm{dcl}(x, B)$ is the purely inseparable closure of the field generated by (x, B), then

$$\sigma(x) = (\frac{f(x)}{g(x)})^{p^{-r}},$$

where f and g are some polynomials with coefficients in the field generated by B, $r \in \mathbb{N}$, p is the characteristic of the algebraically closed field, and if $p = 0$ then $r = 0$. Letting $\sigma' = \mathrm{Frob}^r\sigma$ we relabel $\sigma = \sigma'$, and now

$$\sigma(x) = \frac{f(x)}{g(x)} \tag{3.10}$$

We assume that $f(x)$ and $g(x)$ are in lowest common form.

Suppose that H_a is the graph of the automorphism σ. Suppose it has coordinates (x, y). Then equation 3.10 shows that on H_a, $f(x) - yg(x) = 0$ holds generically. So it holds on the whole of H_a. Say $x \in \mathbb{A}^1$ and $g(x)$=0. Then $f(x) = 0$, so $g(x)$ and $f(x)$ share a root. But they are in lowest common form, so we may assume that $g(x) = 1$. Now it is clear that $y = f(x)$ defines an absolutely irreducible variety. And it is clear that in this case it has dimension 1 and contains H_a, also absolutely irreducible and of dimension 1. So $y = f(x)$ defines H_a. Let $y = 0$. There must be a unique solution to

$f(x) = 0$. So $f(x) = x^s$ for some $s \in \mathbb{N}$. Letting y=1, s is seen to be a power of the characteristic. □

Of course, it is interesting to characterise all interpretable difference fields in K. We have the following:

PROPOSITION 3.4.11 *Let (L', τ') be a difference field interpretable in the pseudo-finite field K. Then in K there is a definable difference field (L, τ) and a definable isomorphism of difference fields $i : (L', \tau') \cong (L, \tau)$, such that L is a finite extension of K, and $\mathrm{Frob}^r\tau \in \mathrm{Gal}(L/K)$ for some $r \in \mathbb{Z}$.*

PROOF By [15] Theorem 9.1, every infinite interpretable field in K is definably isomorphic to a finite extension of K. So there is a definable, finite field extension L of K and a definable isomorphism of fields $i : L' \mapsto L$. Then define $\tau = i\tau' i^{-1}$.

We may suppose that K is elementarily equivalent to an ultraproduct of finite fields: $K \equiv K_*$ where $K_* = \prod_{i\in\mathbb{N}} \mathbb{F}_{p^{d_i}} / \sim$. Supposing that $[L : K] = s$, we may also assume that $L \equiv L_*$ where $L_* = \prod_{i\in\mathbb{N}} \mathbb{F}_{p^{d_i s}} / \sim$. So we may assume that L_* is a definable extension of K_*. Using $\mathcal{L}$os's Theorem, and the fact that if $F_1 \subseteq F_2$ is a containment of finite fields then any automorphism of F_2 restricts to an automorphism of F_1, we see that any definable automorphism of L_* restricts to an automorphism of K_*. By elementary equivalence it follows that the restriction $\tau|_K$ is an automorphism of K. By Proposition 3.4.1, $\tau|_K = \mathrm{Frob}^{-r}|_K$ for some $r \in \mathbb{Z}$. Thus $(\mathrm{Frob}^r\tau)|_K$ =id. □

We presented the proof using [15] Theorem 9.1, because that theorem is applicable to all perfect, bounded PAC fields. The above theorem should, thus, generalise to the perfect, bounded PAC context.

3.5 An Asymptotic theory for finite difference fields

In this section, let m and l be coprime natural numbers with $l > 1$, and let p be a prime. We show that the class of structures $\mathcal{C}_{(m,l,p)} = \{(\mathbb{F}_{p^{kl+m}}, \mathrm{Frob}^k) : k \in \mathbb{N})\}$ forms a 1-dimensional asymptotic class.

We begin with an important remark:

REMARK 3.5.1 Lemma 2.3.9 holds for the theory $PSF_{(m,l,p)}$. The reader may verify that the proof transfers. Furthermore, suppose that $\theta(x,y)$ is a formula in $\mathcal{L}_{\text{diff}}$, and length$(x)$=$n$. The reader may verify that for any (M,σ) an ω_1-saturated model of $PSF_{(m,l,p)}$, and $y_0 \in P(\theta)(M)$, then $\deg_\sigma(\theta(x,y_0)) \leq n \cdot l$. This follows from the fact that for any single element $y_1 \in M$, then $\sigma^l(y_1) = y_1^{p^{-m}}$, and so $\text{acl}_\sigma(y_1) \subseteq \text{acl}_{\text{alg}}(y_1, \sigma(y_1), \ldots, \sigma^{l-1}(y_1))$. It is a simple corollary that σ-degree is uniformly definable in $PSF_{(m,l,p)}$. $\square$

DISCUSSION/DEFINITION 3.5.2 There is an operator Fix from difference fields (K,σ) to difference fields (M,τ) whose automorphism satisfies $\text{Frob}^m\tau^l$=id:

$$M = \{x : \ x \in K \ \wedge \ \sigma^l(x) = x^{p^{-m}}\}$$

$$\text{Fix}((K,\sigma)) = (M, \sigma|_M)$$

In the consistency proof for $PSF_{(m,l,p)}$, it was shown that if $(K,\sigma) \models ACFA_p$ then $\text{Fix}((K,\sigma)) \models PSF_{(m,l,p)}$.

We may specify specific subdomains of the domain of all difference fields where we may define an inverse to Fix:

Let $\mathcal{D}_p$ be the class of difference fields $\{(\tilde{\mathbb{F}}_p, \text{Frob}^k) : k \in \mathbb{N}\}$. The class $\mathcal{C}_{(m,l,p)}$ is uniformly interpretable in $\mathcal{D}_p$ by the formula $\text{Fix}(\text{Frob}^m\sigma^l) : \ \ \sigma^l(x) = x^{p^{-m}}$. Moreover, there is a perfect matching $\text{Fix} : \mathcal{D}_p \mapsto \mathcal{C}_{(m,l,p)}$ such that $\text{Fix}((\tilde{\mathbb{F}}_p, \text{Frob}^k)) = (\mathbb{F}_{p^{lk+m}}, \text{Frob}^k)$. Let Fix^{-1} denote the inverse of this matching Fix on the subdomain $\mathcal{D}_p$ of difference fields. For convenience, we may abuse notation and also let Fix^{-1} denote the embedding Fix^{-1}: $\mathbb{F}_{p^{lk+m}} \subset \tilde{\mathbb{F}}_p$.

Let us consider the subdomain of the class of difference fields given by non-principal ultraproducts $\mathcal{D}_{p,\text{npu}} = \{\prod_{k\in\mathbb{N}}(\tilde{\mathbb{F}}_p, \text{Frob}^k)/\sim : \sim \text{ a non-principal ultrafilter on } \mathbb{N}\}$. Then $\text{Fix}(\prod_{k\in\mathbb{N}}(\tilde{\mathbb{F}}_p, \text{Frob}^k)/\sim) = \prod_{k\in\mathbb{N}}(\mathbb{F}_{p^{lk+m}}, \text{Frob}^k)/\sim$, and so if we let $\mathcal{C}_{m,l,p,\text{npu}} = \{\prod_{k\in\mathbb{N}}(\mathbb{F}_{p^{lk+m}}, \text{Frob}^k)/\sim : \sim \text{ a non-principal ultrafilter on } \mathbb{N}\}$, then Fix is a perfect matching between $\mathcal{D}_{p,\text{npu}}$ and $\mathcal{C}_{m,l,p,\text{npu}}$. So we may define Fix^{-1} on this sub-domain

of difference fields, and again, abusing notation, also let Fix^{-1} denote the containment Fix^{-1}: $\prod_{k\in\mathbb{N}} \mathbb{F}_{p^{lk+m}}/\sim \subset \prod_{k\in\mathbb{N}} \tilde{\mathbb{F}}_p/\sim$.

There is a map $^{\mathrm{Fix}} : \mathcal{L}_{\mathrm{diff}} \mapsto \mathcal{L}_{\mathrm{diff}}$ such that: either (i) let $(M,\sigma) \in \mathcal{C}_{(m,l,p)}$ and $(K,\sigma) \in \mathcal{D}_p$ be such that $\mathrm{Fix}((K,\sigma)) = (M,\sigma)$, or (ii) let $(M,\sigma) \in \mathcal{C}_{m,l,p,\mathrm{npu}}$ and let $(K,\sigma) \in \mathcal{D}_{p,\mathrm{npu}}$ be such that $\mathrm{Fix}((K,\sigma)) = (M,\sigma)$. Then, for any formula $\varphi(y) \in \mathcal{L}_{\mathrm{diff}}$, and any tuple $a \in M$

$$(M,\sigma) \models \varphi(a) \iff \mathrm{Fix}^{-1}((M,\sigma)) \models \varphi^{\mathrm{Fix}}(\mathrm{Fix}^{-1}(a))$$

In particular, there is a bijection between $\varphi(a)$ in (M,σ) and $\varphi^{\mathrm{Fix}}(\mathrm{Fix}^{-1}(a))$ in $\mathrm{Fix}^{-1}((M,\sigma))$. The operator $^{\mathrm{Fix}}$ is defined inductively on complexity. If $\varphi(x)$ is a quantifier-free formulae, then $\varphi^{\mathrm{Fix}}(x) = \varphi(x) \wedge (x \in \mathrm{Fix}(\mathrm{Frob}^m\sigma^l))$. For a formula $\varphi(x) = \exists z(\psi(x,z))$, then $\varphi^{\mathrm{Fix}}(x) = \exists z(z \in \mathrm{Fix}(\mathrm{Frob}^m\sigma^l) \wedge \psi^{\mathrm{Fix}}(x,z))$; for a formula $\varphi(x) = \neg\psi(x)$, then $\varphi^{\mathrm{Fix}}(x) = \neg\psi^{\mathrm{Fix}}(x)$.

PROPOSITION 3.5.3 *The first criterion for asymptotic classes is satisfied by the class $\mathcal{C}_{(m,l,p)}$.*

PROOF Let $\varphi(x,y)$ be a $\emptyset$-definable family of sets in $\mathcal{L}_{\mathrm{diff}}$. By Remark 3.5.1, the sub-family of $\varphi(x,y)$ given by $\varphi_n(x,y) : \varphi(x,y) \wedge \deg_\sigma(\varphi(x,y)) = n$ is uniformly definable in $PSF_{(m,l,p)}$. Also, the bound in 3.5.1 shows that there are only finitely many such sub-families $\varphi_n(x,y)$. Theorem 2.1.1 shows that for each $\varphi_n(x,y)$ the class $\mathcal{C}_{(m,l,p)}$ has asymptotic estimates that satisfy the first criterion for asymptotic classes: to obtain a set of asymptotic estimates over $\mathcal{C}_{(m,l,p)}$ for $\varphi_n(x,y)$ one may use the estimates over $\mathcal{D}_p$ for $\varphi_n^{\mathrm{Fix}}(x,y)$ obtained in 2.1.1. Since there are only finitely many sub-families $\varphi_n(x,y)$, there are in total a finite number of dimension/measure estimates over $\mathcal{C}_{(m,l,p)}$ for the family $\varphi(x,y)$. We deduce that the first criterion for asymptotic classes is satisfied by $\mathcal{C}_{(m,l,p)}$. $\square$

REMARK 3.5.4 The estimates obtained in 2.1.1 are shown there to be uniformly definable over the class $\mathcal{D}_p$. That is, the second criterion for asymptotic classes is satisfied over $\mathcal{D}_p$. It is not immediate that the second criterion is satisfied over $\mathcal{C}_{(m,l,p)}$.

DEFINITION 3.5.5 *Suppose* $(M,\sigma) \models PSF_{(m,l,p)}$, $(K,\sigma) \models ACFA_p$, *and* $\mathrm{Fix}((K,\sigma)) = (M,\sigma)$. *We call* (M,σ) *an embedded model of* $PSF_{(m,l,p)}$, *or say that* M *is embedded in* K.

REMARK 3.5.6 Let T be a completion of $PSF_{(m,l,p)}$. Then by Theorem 3.3.15, there is a model (M,σ) of T of the form $(M,\sigma) = \prod_{k\in\mathbb{N}}(\mathbb{F}_{p^{lk+m}}, \mathrm{Frob}^k)/\sim$, where the right hand side is a non-principal ultraproduct of finite difference fields. Let $(K,\sigma) = \prod_{k\in\mathbb{N}}(\tilde{\mathbb{F}}_p, \mathrm{Frob}^k)/\sim$, Then $(M,\sigma) = \mathrm{Fix}((K,\sigma))$. So, for any completion T of $PSF_{(m,l,p)}$ there is an embedded model of T, where the embedded model $(M,\sigma) \in \mathcal{C}_{m,l,p,\mathrm{npu}}$, and the corresponding $(K,\sigma) \in \mathcal{D}_{p,\mathrm{npu}}$.

PROPOSITION 3.5.7 *Let* $\varphi(x,y)$ *be a* $\emptyset$*-definable family of* σ*-closed sets. Then the second criterion for asymptotic classes is satisfied in* $\mathcal{C}_{(m,l,p)}$ *with respect to the family* $\varphi(x,y)$.

PROOF Let $\theta(x,y) = \varphi^{\mathrm{Fix}}(x,y)$. Now suppose that θ_{n,μ_i} are from Theorem 2.1.1 relative to this choice of $\theta(x,y)$.

Consider the statement:

(*) there is a formula φ_{n,μ_i} definable without parameters such that for any $(K,\sigma) \in \mathcal{D}_{p,\mathrm{npu}}$, and $(M,\sigma) = \mathrm{Fix}((K,\sigma))$, then

$$\varphi^{\mathrm{Fix}}_{n,\mu_i}(K) = \theta_{n,\mu_i}(K) \tag{3.11}$$

Suppose we can show (*): by Remark 3.5.6, we know that there are embedded models $(M,\sigma) \in \mathcal{C}_{m,l,p,\mathrm{npu}}$ for every completion of $PSF_{(m,l,p)}$. Since $PSF_{(m,l,p)}$ is the almost theory of the class $\mathcal{C}_{(m,l,p)}$ we may then deduce that equation 3.11 is satisfied in all but finitely many $(M,\sigma) \in \mathcal{C}_{(m,l,p)}$, with $(K,\sigma) = \mathrm{Fix}^{-1}((M,\sigma))$ (considering Fix as a bijection between $\mathcal{D}_p$ and $\mathcal{C}_{(m,l,p)}$). Thus to prove the proposition it suffices to show (*).

To ease notation, we let $(K,\sigma) \in D_{p,\mathrm{npu}}$ and we let $(M,\sigma) = \mathrm{Fix}((K,\sigma))$ be an embedded model of $PSF_{(m,l,p)}$. We shall also quantify over all 'pairs (K,M)'; this means to

quantify over all pairs where $(M,\sigma) \in \mathcal{C}_{m,l,p,\mathrm{npu}}$ is embedded in $(K,\sigma) \in \mathcal{D}_{p,\mathrm{npu}}$.

Now examine the 'construction' of θ_{n,μ_i}: the construction depends only on the fact that a finite set of properties of algebraic sets and σ-closed sets are uniformly stratifiable across algebraically closed fields and models of $ACFA$. Suppose $\Gamma = \{\gamma_1(v_1), \gamma_2(v_2), \ldots \gamma_s(v_s)\}$ is the set of formulae defining the necessary uniform stratifications to construct θ_{n,μ_i}.

Over all pairs (K,M), the families of algebraic sets/σ-closed sets that are stratified by the formulae in Γ in order to construct θ_{n,μ_i} are all families of the form $A(x,y)$ where we may uniformly, definably specify that $y \in M$ (see Propositions 2.3.11 and 2.3.13). So it follows that we may assume that uniformly over pairs (K,M), for each $1 \leq r \leq s$, $\gamma_r(K)$ takes its values in M. Thus, it suffices to show that for each $1 \leq r \leq s$, there is a formula $\delta_r(v_r)$ such that over all pairs (K,M), $\gamma_r(K) = \delta_r^{\mathrm{Fix}}(K)$.

The first Γ-formula is $\theta_n(x,y)$. Let $\varphi_n(x,y)$ be the sub-family of $\varphi(x)$ of σ-degree n, where σ-degree is measured in $PSF_{(m,l,p)}$. For a pair (K,M) and a notion of model theory or notion we have defined in this chapter, let us denote by superscript K if the notion is taken to be relative to (K,σ), and by superscript M, if it is taken to be relative to (M,σ). Let $X \subseteq M$. The reader may verify that $\mathrm{acl}_\sigma{}^K(X) = \mathrm{acl}^K_{\mathrm{alg}}(\mathrm{acl}^M_\sigma(X))$, and it follows that for $y \in M$ $\deg^M_\sigma(y/X) = \deg^K_\sigma(y/X)$. Thus $\theta_n(x,y) = \varphi_n^{\mathrm{Fix}}(x,y)$.

Relative to $\theta_n(x,y)$, the formulae in 2.3.3, $\mathrm{ext}_n(\varphi)$, $\mathrm{alg}_n(\varphi)$, $\mathrm{shift}_n(\varphi)$ and $\triangle_n(\varphi)$ are quantifier-free and without parameters. Since $\theta_n(x,y)$ is uniformly a family of sets in M with M-parameters, the reader may verify that the proofs of Propositions 2.3.11 and 2.3.13 with respect to θ_n work equally well relative to the sets $\mathrm{ext}_n^M(\varphi)$: $\mathrm{ext}_n(\varphi) \wedge (\sigma^l(x) = x^{p^{-m}})$, $\mathrm{alg}_n^M(\varphi)$: $\mathrm{alg}_n(\varphi) \wedge (\sigma^l(x) = x^{p^{-m}})$, and $\mathrm{shift}_n^M(\varphi)$: $\mathrm{shift}_n(\varphi) \wedge (\sigma^l(x) = x^{p^{-m}})$. Now $\mathrm{ext}_n^M(\varphi)$, $\mathrm{alg}_n^M(\varphi)$ and $\mathrm{shift}_n^M(\varphi)$ are relevant sets in Γ, and clearly they are all $^{\mathrm{Fix}}$-images.

The reader may verify that there is a $G \in \mathbb{N}$ such that the proofs of Propositions 2.3.11 and 2.3.13 work equally well with the L-rational points of the algebraic sets B_j of Proposition 2.3.11, where L is the extension of M of a fixed finite degree G. Note

that G is chosen so that uniformly over all pairs (K, M), the irreducible components of the B_j are all definable over L. In Propositions 2.3.11 and 2.3.13, the B_j are made use of in the following way:

(i) to uniformly count the number of irreducible components V_i of the B_j which are of algebraic dimension n, and contain a generic point of the form $(x, \sigma(x))$.

(ii) to stratify the irreducible components counted in (i) by the degree of π_1 and the inseparable degree of π_2.

There are formulae γ_i and γ_{ii} in Γ that achieve (i) and (ii). We must find their $^{\text{Fix}}$-preimages:

For (i) we may parameter interpret the degree G extension of any $M \models PSF_{(m,l,p)}$. Call such an extension L. We may then interpret the set of L-rational points of V_i. Using parameters, we may define any generic extension τ of σ to L. Then we may parameter define an embedding $\triangle_n \cap V_i(L) \subseteq V_i(L)$, where $\triangle_n$ is with respect to τ. By Remark 3.5.1, we may then parameter define the set of components V_i where $\dim_{\text{alg}}(\triangle_n(\varphi) \cap V_i(L)) = n$, and this serves to parameter define those irreducible components V_i which have a generic point of the form $(x, \tau(x))$. Now, we must get rid of parameters:

Claim: Suppose $M \in \mathcal{C}_{m,l,p,\text{npu}}$, and L is its degree G-extension. Suppose that τ is an extension of σ, generic over M. Then any point $(x_0, \tau(x_0)) \in V_i(L)$ is in fact, $(x_0, \tau(x_0)) \in V_i(M)$.

Proof of Claim: $\theta(x, y)$ is a family of M-rational sets. This is by construction; concretely, we may assume that if $x = (x_1 \dots x_r)$, then $\theta(x, y)$ contains the conjuncts $\sigma^l(x_i) = x_i^{p^{-m}}$ for each $1 \leq i \leq r$. The reader verifies, by chasing the definitions of $\text{shift}_n(\varphi)$ and $\triangle_n(\varphi)$, and by noting that $\text{Fix}(\text{Frob}^m\tau^l(L)) = M$, that this directly implies the claim. **End of Proof of Claim**

Thus, it does not matter how we extend σ to τ, as long as τ is a generic extension. The set of generic extensions of σ to L is $\emptyset$-definable. As soon as counting the components is independent of the parameters we choose to interpret the degree-G extension L of M, and the extension of σ to an automorphism of L, the reader may easily verify that we may dispense with parameters in our stratifications of (i). Thus there is a δ_i such that $\gamma_i(K) = \delta_i^{\mathrm{Fix}}(K)$.

For (ii), these stratifications count the numbers of irreducible components of the B_j which have particular ACF-stratifiable properties. Since these are properties in algebraically closed fields, the formulae involved are quantifier-free. We deduce that there is a δ such that $\gamma_{ii}(K) = \delta_{ii}^{\mathrm{Fix}}(K)$. $\square$

THEOREM 3.5.8 *$\mathcal{C}_{(m,l,p)}$ is a 1-dimensional asymptotic class.*

PROOF Propositions 3.5.7 and 3.5.3 show that $\mathcal{C}_{(m,l,p)}$ forms an asymptotic class relative to families of σ-closed sets. In terms of Definition 2.4.2 we let $R(x) := x = x$. Then $\mathcal{C}_{(m,l,p)}$ satisfies Elwes' definition for asymptotic classes (Definition 2.4.2) with respect to $R(x)$ for all families of σ-closed sets. We may immediately apply Lemma 2.4.3 to deduce that $\mathcal{C}_{(m,l,p)}$ satisfies Elwes' definition for asymptotic classes with respect to $R(x)$ for all families of quantifier-free sets.

Analogously to methods used in [10] Theorem 3.7, Theorem 3.3.14 part (ii) reduces proving that $\mathcal{C}_{(m,l,p)}$ is an asymptotic class to proving the theorem for families $\theta(x, y)$ where

$$\theta(x,y) \ := \ \bigvee_{i=1}^{r} \bigwedge_{j=1}^{r_i} \exists t(f_{ij}(x,t,y)) \tag{3.12}$$

t is a single variable, $f_{ij}(x, t, y)$ is quantifier-free, and there is an $e \in \mathbb{N}$ such that for any $M \in \mathcal{C}$ and $x_0, y_0 \in M$ we have $|f_{ij}(x_0, M, y_0)| \leq e$. Now, by the inclusion-exclusion principle, it suffices to prove the theorem for any conjunction $\bigwedge_{j=1}^{r} \exists t(f_j(x, t, y))$. But then let $s = t_1, \ldots, t_r$. We have

$$\bigwedge_{j=1}^{r} \exists t(f_j(x,t,y)) \iff \exists s(\bigwedge_{j=1}^{r} f_j(x,t_j,y)) \tag{3.13}$$

But let $\psi(xs, y) := \bigwedge_{j=1}^{r} f_j(x, t_j, y)$. Then there is an $b \in \mathbb{N}$ such that for any $M \in \mathcal{C}$ and $x_0, y_0 \in M$, $|\{s \in M : \ M \models \psi(x_0 s, y_0)\}| \leq b$. So we may now apply Lemma 2.4.4

to deduce that $\mathcal{C}_{(m,l,p)}$ is an asymptotic class relative to *all* families of sets. All that remains is to compute the dimension of the asymptotic class $\mathcal{C}_{(m,l,p)}$.

Let $\mathcal{D}_p = \{(\tilde{\mathbb{F}}_p, \mathrm{Frob}^k) : \ k \in \mathbb{N}\}$. Inspection of 2.1.1 and 2.1.2 shows that for any $\mathcal{L}_{\mathrm{diff}}$-formula $\theta_n(x,y)$, and for all $(\tilde{\mathbb{F}}_p, \mathrm{Frob}^k) \in \mathcal{D}_p$ with finitely many exceptions, for any $y_0 \in P(\theta)(\tilde{\mathbb{F}}_p)$ the asymptotic estimate for $|\theta_n(x,y_0)|$ chosen by Theorem 2.1.1 is $\mu \mid \mathrm{Fix}(\mathrm{Frob}^k)(\tilde{\mathbb{F}}_p) \mid^n$. Here, $\mathrm{Fix}(\mathrm{Frob}^k)(\tilde{\mathbb{F}}_p)$ is the fixed field in $\tilde{\mathbb{F}}_p$ of the automorphism Frob^k, and it has cardinality p^k; also, μ is one of a finite number of measure constants.

Proposition 3.5.7 shows that the estimates on $\mathcal{C}_{(m,l,p)}$ arise from the estimates on $\mathcal{D}_p$ from 2.1.1; in turn, the latter arise as combinations of estimates from Theorem 2.1.2. That is, for any $\mathcal{L}_{\mathrm{diff}}$-formula $\theta(x,y)$, and for all $(\mathbb{F}_{p^{kl+m}}, \mathrm{Frob}^k) \in \mathcal{C}_{(m,l,p)}$, for any $y_0 \in P(\theta)(\mathbb{F}_{p^{kl+m}})$, the estimate we choose for $|\theta(\mathbb{F}_{p^{kl+m}}, y_0)|$ is the estimate chosen in 2.1.1 for $|\theta^{\mathrm{Fix}}(\tilde{\mathbb{F}}_p, \mathrm{Fix}^{-1}(y_0)|$. Since $\mid \mathbb{F}_{p^{lk+m}} \mid = p^{lk+m} = p^m \cdot \mid \mathrm{Fix}(\mathrm{Frob}^k) \mid^l$, by analogy with the algebraically closed case, we might guess that the field $\mathbb{F}_{p^k}$ was uniformly definable inside $(\mathbb{F}_{p^{lk+m}}, \sigma)$ as the fixed field of σ, and consequently the dimension of the asymptotic class is l. But in fact $\mid \mathrm{Fix}(\mathrm{Frob}^k)(\tilde{\mathbb{F}}_p) \cap \mathbb{F}_{p^{lk+m}} \mid \leq p^m$, so things are not so simple.

The dimension of the class is 1. For suppose there was a 0-definable $\theta(x,y)$ with x one variable, and a stratification formula $\theta_{j,\mu}(y)$ with $j < l$. Then we can choose a non-principal ultraproduct $(M,\sigma) = \prod_{i\in\mathbb{N}}(\mathbb{F}_{p^{lk_i+m}}, \mathrm{Frob}^{k_i})/\sim_{\mathcal{U}}$, and a tuple $a \in M$ such that $\theta_{j,\mu}(a)$ holds. So $\theta(x,a) \subseteq M$ and $\deg_\sigma(\theta(x,a)) = j < l = \deg_\sigma(M)$. Also, (M,σ) embeds into the ultraproduct $(K,\sigma) = \prod_{i\in\mathbb{N}}(\tilde{\mathbb{F}}_p, \mathrm{Frob}^{k_i})/\sim_{\mathcal{U}}$, and $(K,\sigma) \models ACFA_p$. We then have $\deg_\sigma(\theta^{\mathrm{Fix}}(K, \mathrm{Fix}^{-1}(a))) = j < l$ and $\theta^{\mathrm{Fix}}(K, \mathrm{Fix}^{-1}(a)) \subseteq \mathrm{Fix}(\mathrm{Frob}^m\sigma^l)(K)$. But this contradicts the result [9] Proposition 7.1 (1). $\square$

Chapter 4

Bi-interpretations and Asymptotic Classes

4.1 Chapter Introduction

This chapter is divided into two principal sections. The first section is devoted to defining uniform parameter bi-interpretations, strongly uniform parameter bi-interpretations, and proving a transfer result: a class of structures which is strongly, uniformly parameter bi-interpretable with an asymptotic class is itself an asymptotic class. Intuitively, part (i) of 1.2.7 should hold for a class of structures $\mathcal{C}$, if $\mathcal{C}$'s members are bi-interpretable structure by structure with the members of an asymptotic class $\mathcal{D}$. Part (ii) of 1.2.7 is harder to transfer, and we need uniformity in the family of bi-interpretations between the members of $\mathcal{C}$ and the members of $\mathcal{D}$ in order to obtain a result. The necessary uniformities are the basis of what is called 'uniform parameter bi-interpretations' and 'strongly uniform parameter bi-interpretations'.

The second section provides technical tools for generating interpretations in the context of groups. These tools are then applied in the following chapter.

4.2 Uniformly Parameter-Definable Bi-interpretations

.

NOTATION 4.2.1 To ease notation, all variable and constant references will be to tuples. We need to specify what this means: in this section, from Definition 4.2.2 onwards, we treat parameter bi-interpretations. We use constant tuple variables such as x and w throughout. This might seem peculiar since various parts of a bi-interpretation require different length tuples: for instance, the interpretation of an n-ary relation requires tuples of length n, but the isomorphism from the underlying set to its re-interpretation within itself requires a $1 + k$-length tuple, where k is the tuple-length of the set in which this re-interpretation occurs. But we simply think of x as a large enough 'bank' of free variables to code all possible parts of the bi-interpretation. There is no need for a particular part to use all of the elements of x.

In this section, we shall be in the following situation: $\mathcal{L}$ is a language; $\mathcal{C}$ is a class of $\mathcal{L}$-structures and $\theta(x, y)$ is a formula in $\mathcal{L}$. What will be important is to distinguish between the free variable y which parameterises the family of sets $\theta(x, y)$ throughout $\mathcal{C}$,

and a particular set $\theta(x, a_y)$ for some $a_y \in \mathcal{C}$. We need to carefully distinguish between these two. For clarity, our notation will be as presented: a_y will be a specific parameter (and by our convention, in fact a tuple of parameters) in some member $C \in \mathcal{C}$, where its subscript y indicates the free variable in $\theta(x, y)$.

DEFINITION 4.2.2 Suppose $\mathcal{D}$ is a class of $\mathcal{L}$-structures and suppose we have a system of subsets $S = \{X_D \subseteq D^m : D \in \mathcal{D}\}$. We say S is 'uniformly parameter-definable' or UPD if there is a 0-definable $\mathcal{L}$-formula $X(x, y)$ such that $\forall D \in \mathcal{D}$, $X_D = X(x, a_y)$ for some tuple $a_y \in D$. In such a situation we refer to the variable y as the witnessing variable, and the variable x as the free variable. In the text we will refer to UPD in several ways: an object is UPD (uniformly parameter-definable); we give a UPD (uniform parameter definition); we UPD (uniformly parameter define).

DEFINITION 4.2.3 Suppose $\mathcal{C}$ is a class of $\mathcal{L}_1$-structures and $\mathcal{D}$ is a class of $\mathcal{L}_2$-structures. The following define a uniform parameter bi-interpretation between $\mathcal{D}$ and $\mathcal{C}$:

1. $\mathcal{L}_1$ and $\mathcal{L}_2$ are finite languages. By this we mean that both $\mathcal{L}_1$ and $\mathcal{L}_2$ have a finite number of relations and functions.

2. There is a perfect matching m from $\mathcal{C}$ to $\mathcal{D}$.

3. There is a finite set $J_1 = \{\theta_{1i}(x, y) : \ 1 \leq i \leq n_1\}$ of $\mathcal{L}_1$-formulas, and a finite set $J_2 = \{\theta_{2i}(w, z) : \ 1 \leq i \leq n_2\}$ of $\mathcal{L}_2$-formulas, an $\mathcal{L}_1$-definable function $i_1(x, y)$ and an $\mathcal{L}_2$-definable function $i_2(w, z)$, such that:

   let L_1 be a finite list of the functions, relations, and constants of $\mathcal{L}_1$, and let L_2 be a finite list of the functions, relations, and constants of $\mathcal{L}_2$. We demand there be bijections $f_1 : J_1 \equiv L_2$ and $f_2 : J_2 \equiv L_1$ and that for each matched pair $C \in \mathcal{C}$, $D \in \mathcal{D}$ such that $D = m(C)$, there be a parameter bi-interpretation $\Omega_{C,D}$ between D and C, where there are tuples $a_y \in C$ and $a_z \in D$ such that

   (a) for each $1 \leq i \leq n_1$, $\theta_{1i}(x, a_y)$ defines the interpretation of $f_1(\theta_{1i}(x, y))$ in the bi-interpretation $\Omega_{C,D}$.

   (b) for each $1 \leq i \leq n_2$, $\theta_{2i}(w, a_z)$ defines the interpretation of $f_2(\theta_{2i}(w, z))$ in the bi-interpretation $\Omega_{C,D}$.

(c) $i_1(x, a_y)$ is the isomorphism between C and its re-interpretation C^{**} in $\Omega_{C,D}$.

(d) $i_2(w, a_z)$ is the isomorphism between D and its re-interpretation D^{**} in $\Omega_{C,D}$.

In this context we shall say that $a_y \in C$ is a witness to the interpretation of $m(C)$ in C inside the uniform interpretation of $\mathcal{D}$ in $\mathcal{C}$, and we denote this particular interpretation $m(C)(a_y)$. We shall say that the pair a_y, a_z is witness to the bi-interpretation between D and C inside the uniform bi-interpretation between $\mathcal{C}$ and $\mathcal{D}$.

DEFINITION 4.2.4 Let $D = m(C)$. Suppose that a_y is a witness to the interpretation of D inside C. Any such witness induces an interpretation of the language $\mathcal{L}_2$ inside $\mathrm{Def}(C)$. Let us describe some well-defined maps:

1. Any interpretation $m(C)(a_y)$ induces a map $\mathrm{Int}_{a_y} : \mathcal{L}_2 \mapsto \mathcal{L}_1(C)$.

2. Let $\mathcal{L}_{1,c}$ be the language $\mathcal{L}_1$ augmented by constant symbols for the uniform interpretation of $\mathcal{D}$ in $\mathcal{C}$. For a tuple $a_y \in C$, let $\mathrm{Sub}_{a_y} : \mathcal{L}_{1,c} \mapsto \mathcal{L}_1(C)$ be the map obtained by setting the constant symbols c to be the tuple a_y. Notice in addition that Sub_{a_y} has a natural inverse defined on its image inside $\mathcal{L}_1(C)$; the inverse is obtained simply by replacing any occurence of the tuple a_y with the constant symbols c.

3. Similarly, we have the map P from $\mathcal{L}_{1,c}$ to the zero definable parsed families of $\mathcal{L}_1$. The map P simply replaces the tuple c with a tuple y and treats the resulting y as a family parameter, and not a free variable.

4. There is a natural embedding as sets $B : \mathcal{L}_2 \hookrightarrow \mathcal{L}_{1,c}$, such that for any witness $a_y \in C$ to the interpretation of D in C, the equation $\mathrm{Int}_{a_y} = \mathrm{Sub}_{a_y} \circ B$ holds.

5. We also have the map $I_1 := P \circ B$. We note that for any witness a_y we have $I_1 = P\mathrm{Sub}_{a_y}^{-1}\mathrm{Int}_{a_y}$. Notice that these various maps can be taken to respect formula parsings.

6. All of the above was done with respect to an interpretation $m(C)(a_y)$. We could describe the same maps relative to $C(a_z)$, $a_z \in D$, and d a tuple of constant symbols adjoined to $\mathcal{L}_2$. We obtain:

   (a) $\mathrm{Sub}_{a_z} : \mathcal{L}_{2,d} \mapsto \mathcal{L}_2(D)$;

   (b) P_2, which is a map from $\mathcal{L}_{2,d}$ to the zero definable parsed families of $\mathcal{L}_2$.

   (c) $B_2 : \mathcal{L}_1 \hookrightarrow \mathcal{L}_{2,d}$, such that for any witness $a_z \in D$ to the interpretation of C in D, the equation $\mathrm{Int}_{a_z} = \mathrm{Sub}_{a_z} \circ B_2$ holds.

   (d) $I_2 := P_2 \circ B_2$, such that for any witness a_z we have $I_2 = P_2 \mathrm{Sub}_{a_z}^{-1} \mathrm{Int}_{a_z}$.

NOTATION 4.2.5 We adopt the following notation for the rest of the section. Suppose, as in Chapter 2, that the parameter set of a definable family $\theta(x, y)$ in a structure C is denoted by $P(\theta)(C)$. Also, inside a parameter bi-interpretation between structures C and D, denote by C^* the interpreted version of C living in D and by D^* the interpreted version of D living in C. In these circumstances, call the actual witnessing isomorphisms $\alpha : D \mapsto D^*$ and $\beta : C \mapsto C^*$.

REMARK 4.2.6 Let us informally describe the purpose of the following Definition 4.2.7. Uniform parameter bi-interpretations are not natural in one striking sense. For each pair of matched structures we need to specifically pick the parameters that make the bi-interpretations. It would be convenient if we had a definable mechanism for picking those parameters. Practically, we shall require such a mechanism in 4.2.10, which is central to the thesis. With this purpose in mind, Definition 4.2.7 is natural.

In the following definition we inherit the notation of 4.2.3 and 4.2.5:

DEFINITION 4.2.7 Suppose $\mathcal{C}$ are $\mathcal{D}$ are uniformly parameter bi-interpretable. Then they are strongly uniformly parameter bi-interpretable if additionally there is an $\mathcal{L}_1$-formula $\Gamma(y, t)$, where for any $C \in \mathcal{C}$ and $D = m(C)$:

1. $C \models \exists yt(\Gamma(y, t))$

2. For $a_y, a_t \in C$, we have $C \models \Gamma(a_y, a_t)$ if and only if there is a tuple of witnesses a_y, a_z to the bi-interpretation between C and D such that $\alpha(a_z) = a_t$.

We call $\Gamma(y, t)$ a defining formula for the strongly uniform parameter bi-interpretation.

EXAMPLE 4.2.8 We now build up a very easy, informal example of a uniform and strongly uniform parameter bi-interpretation. We do not give all the details, but focus on the intuition. We begin with two very similar classes of structures: $\mathcal{C} = \{$ pure sets of size $n^2 + n : \ n \in \mathbb{N}\}$ and $\mathcal{D} = \{$ pure sets of size $n^2 : \ n \in \mathbb{N}\}$, both in the language $\mathcal{L}$ of pure sets. We shall denote by c_n the member of $\mathcal{C}$ with $n^2 + n$ elements, and by d_n the member of $\mathcal{D}$ with n^2 elements. Then there is a natural matching $m : \mathcal{C} \equiv \mathcal{D}$ such that $m(c_n) = d_n$. At this stage there is no uniform parameter bi-interpretation between the classes. As we progress we enrich the language $\mathcal{L}$ in various ways and augment the $\mathcal{C}$ and $\mathcal{D}$ classes accordingly. Once we have augmented, then henceforth the class and all references to the class suppose it to be in the richer language.

Suppose that we add two unary predicates B (for blue) and G (for green) to the language of pure sets to make $\mathcal{L}_{B,G}$, and we augment $\mathcal{C}$ to be a class of $\mathcal{L}_{B,G}$-structures. We do this so that for each $n \in \mathbb{N}$, c_n has exactly n^2 green elements and exactly n blue elements, and no element is both blue and green. At this stage it is possible to uniformly interpret $\mathcal{D}$ in $\mathcal{C}$ with our matching m. We simply interpret d_n as the green elements of c_n. However there is no way of uniformly interpreting $\mathcal{C}$ in $\mathcal{D}$.

Suppose now that we add a single binary relation $E(x, y)$ to the language of pure sets to make $\mathcal{L}_E$ and we augment $\mathcal{D}$ to be a class of $\mathcal{L}_E$ structures. We do this so that for each $n \in \mathbb{N}$, E is an equivalence relation on d_n with exactly two equivalence classes: one of size n, and the other of size $n^2 - n$. Then consider the following formula in $\mathcal{L}_E$, in the single variables y, x_1 and x_2:

$$\theta_{\text{blue}}(x_1, x_2, y) =_{\text{def}} x_1 = y \ \wedge \ \neg E(x_2, y) \tag{4.1}$$

$$\theta_{\text{green}}(x_1, x_2, y) =_{\text{def}} x_2 = y \tag{4.2}$$

$$\theta(x_1, x_2, y) =_{\text{def}} \theta_{\text{blue}}(x_1, x_2, y) \ \vee \ \theta_{\text{green}}(x_1, x_2, y) \tag{4.3}$$

For each d_n let $a_y \in d_n$ be an element such that the equivalence class $E(a_y)$ has size $n^2 - n$. Then we may define c_n in d_n via the formula $\theta(x_1, x_2, a_y)$, the green elements being interpreted by $\theta_{\text{green}}(x_1, x_2, a_y)$, and the blue elements by $\theta_{\text{blue}}(x_1, x_2, a_y)$. If we had picked a_y such that $E(a_y)$ has size n, then we cannot interpret c_n in this way. Is our uniform parmater bi-interpretation complete? No, we have new considerations.

Firstly, how can we now uniformly interpret $\mathcal{D}$ in $\mathcal{C}$? I cannot see a natural way to do so that yields a uniform parameter bi-interpretation. Roughly speaking, this is because from the point of view of the uniform bi-interpretation, we shall need a uniformly definable bijection between the green elements of c_n and the underlying set used in the interpretation of d_n. Since there are effectively no uniformly definable maps from blue elements to green elements without bounded domain, essentially green elements need to form the domain of the intepretation of d_n. But then it becomes very difficult to interpret the equivalence class of size $n^2 - n$.

Secondly, the interpretation is not strongly uniform in the sense of 4.2.7. This is because we have no zero definable mechanism to distinguish between the two equivalence classes.

To solve the first issue we augment $\mathcal{L}_{B,G}$ by a binary predicate $s(x, y)$, to make $\mathcal{L}_{B,G,s}$, where s stands for 'section'. We augment $\mathcal{C}$ to a class of $\mathcal{L}_{B,G,s}$-structures by interpreting s in each c_n as an injective function from the blue elements into the green elements. To solve the second problem, let us add to $\mathcal{L}_E$ a unary predicate R (for red), and augment $\mathcal{D}$ to be a class of $\mathcal{L}_{E,R}$-structures. Let us do this so that for each d_n, exactly 3 elements of d_n, all in the equivalence class of size $n^2 - n$, are coloured red; this is a bit arbitrary, but is merely an example of what can work. We may now exhibit a strong uniform bi-interpretation between $\mathcal{C}$ as a class of $\mathcal{L}_{B,G,s}$-structures, and $\mathcal{D}$ as a class of $\mathcal{L}_{E,R}$ structures:

- We interpret d_n in c_n via the following $\mathcal{L}_{B,G,s}$-formulae, where the parameter $y = y_1y_2y_3$ is a tuple of 3 elements:

$$\text{Underlying set} =_{\text{def}} G(x) \tag{4.4}$$

$$\begin{aligned} E(x_1, x_2, y) =_{\text{def}} \; & G(x_1) \wedge G(x_2) \wedge [(\exists wz(x_1 = s(w) \wedge x_2 = s(z))) \\ \vee \; & (\nexists w(x_1 = s(w)) \wedge \nexists z(x_2 = s(z)))] \end{aligned} \tag{4.5}$$

$$R(x, y) =_{\text{def}} \nexists v[y_1 = s(v) \vee y_2 = s(v) \vee y_3 = s(v)] \wedge \vee_{i=1}^{3} x = y_i \tag{4.6}$$

- We interpret c_n in d_n via $\mathcal{L}_{E,R}$-formulae given in expressions 4.1, 4.2, 4.3, and

the following formula to interpret the section s:

$$s: \ \theta_{\text{blue}} \mapsto \theta_{\text{green}}: \ (y, x, y) \mapsto (x, y, y) \tag{4.7}$$

- We include the uniform isomorphisms for completeneness. On the $\mathcal{C}$-side the uniform isomorphism is

$$i_{\mathcal{C},\text{ green elements}}: \ x \mapsto (x, y, y) \tag{4.8}$$

$$i_{\mathcal{C},\text{ blue elements}}: \ x \mapsto (y, s(x), y) \tag{4.9}$$

On the $\mathcal{D}$-side the uniform isomorphism is

$$i_{\mathcal{D}}: \ x \mapsto (x, y, y) \tag{4.10}$$

All that remains is to give the formula giving the strong uniform parameter bi-interpretation. In the uniform parameter bi-interpretation, the parameters are used only in defining c_n in d_n. The parameters are the three red elements of d_n; these are always going to be interpreted in the complement of the s-image of the blue elements in the green elements of c_n. But any such three elements will suffice to construct the parameter bi-interpretation. Thus, the formula, in y empty and $t = t_1t_2t_3$, is:

$$\Gamma(y, t) =_{\text{def}} t_1 \neq t_2 \ \wedge \ t_1 \neq t_3 \ \wedge \ t_2 \neq t_3 \wedge \ \nexists t[\vee_{i=1}^{3} t_i = s(t)] \tag{4.11}$$

REMARK 4.2.9 It is not obvious that Definition 4.2.7 is symmetric. Nor do we require it to be symmetric. The exact direction of the uniform parameter bi-intepretation would always be clear from the language of the formula $\Gamma(y, t)$. However, for clarity, where necessary we shall say explicitly 'strongly uniformly parameter bi-intepretable on the $\mathcal{C}$-side', to mean that the formula $\Gamma(y, t)$ is in $\mathcal{L}_1$. We shall *always* use this definition in connection with Proposition 4.2.10 and Lemma 4.2.11 below. To understand the nature of the definition it is important to consider it in relation to those two results:

In Proposition 4.2.10, we see that if $\mathcal{D}$ is an asymptotic class, and $\mathcal{C}$ is strongly uniformly parameter bi-interpretable with $\mathcal{D}$ on the $\mathcal{C}$-side, then $\mathcal{C}$ is an asymptotic class. Here, we see the lack of symmetry. We know that $\mathcal{D}$ is asymptotic; since we have a

sequence of parameter bi-interpretations, we know that asymptotic estimates for definable sets in $\mathcal{C}$ exist in some form or another. We need additional uniformities in order that part (ii) of Definition 1.2.7 is satisfied for families of sets in $\mathcal{C}$. A uniform parameter bi-interpretation almost does the trick: now families of sets $\theta(x, y)$ in $\mathcal{C}$ are interpreted inside families of sets $\theta^*(w, zy_1)$ in $\mathcal{D}$. At this stage, we attempt to define the asymptotic estimates on $\mathcal{C}$ by stating:

'$\theta_{n,\mu}(x, y)$ is the sub-family of $\theta(x, y)$ where:

if $a_y \in P(\theta_{n,\mu})(C)$ and if $a_z \in D$ witnesses the uniform parameter bi-interpretation between C and D, then $\theta(x, a_y)$ is interpreted by $\theta^*(w, a_z\beta(a_y))$, and $a_z\beta(a_y) \in P(\theta^*_{n,\mu})(D)$.'

The problems are that we need to state this all in $\mathcal{L}_1$, and we need to be able to identify the parameters a_z which actually witness the bi-interpretation. The reader can see this as the purpose of $\Gamma(y, t)$.

PROPOSITION 4.2.10 *1. Suppose $\mathcal{D}$ is an n-dimensional asymptotic class in a language $\mathcal{L}_2$. Suppose $\mathcal{C}$ is a class of $\mathcal{L}_1$-structures and suppose $\mathcal{C}$ is strongly uniformly parameter bi-interpretable with $\mathcal{D}$ on the $\mathcal{C}$-side. Then $\mathcal{C}$ is an asymptotic class.*

2. In the situation in part 1, suppose that $\mathcal{D}$ is a 1-dimensional asymptotic class. In the notation of 4.2.3, suppose that the perfect matching of the bi-interpretation is m. Suppose that $\varphi(w, z)$ is a family of $\mathcal{L}_2$-sets such that for any $C \in \mathcal{C}$ there is $a_z \in m(C)$, and in the strong uniform parameter bi-interpretation, the underlying set of C is interpreted in $m(C)$ by $\varphi(w, a_z)$. Suppose that in $\mathcal{D}$, the family of sets $\varphi(w, z)$ is uniformly of a fixed dimension d. Then $\mathcal{C}$ is a d-dimensional asymptotic class, and d is the minimal possible asymptotic dimension for $\mathcal{C}$.

PROOF 1. Let $\psi(u, v) \in \mathcal{L}_1$ be an arbitrary family of sets. Suppose $C \in \mathcal{C}$ and $D \in \mathcal{D}$ and $D = m(C)$, where m is the matching of the strong uniform bi-interpretation. Let $\Gamma(y, t)$ be an $\mathcal{L}_1$-formula defining the strong uniform parameter bi-interpretation. as in Definition 4.2.7. Consider the $\emptyset$-definable family $\psi_1(u_1, zv_1) = I_1(\psi(u, v))$ in $\mathcal{L}_2$, where

I_1 is as in 4.2.4. Our notation is intended to convey that the map I_1 includes the uniform interpretation parameter tuple z as a family parameter; if $a_z \in D$ is a witness to the interpretation of C in D inside the uniform parameter bi-interpretation, then $\psi_1(u_1, a_z v_1)$ becomes a family of sets in this interpreted version of C. Since $\mathcal{D}$ is an asymptotic class, the parameter set zv_1 is partitionable by formulae $\psi_{1,n_i,\mu_i}(zv_1)$ for $1 \leq i \leq i_0$ that give uniform, asymptotic estimates across the class $\mathcal{D}$ for the cardinalities of the sub-families that they define. The reader should note that if length$(u_1) = l$, then for each $1 \leq i \leq i_0$ we have $0 \leq n_i \leq n \cdot l$. Now consider the family $\psi_2(u_2, ytv_2) = I_2(\psi_1(u_1, zv_1))$, and the definable-without-parameters formula $\psi_{2,n_i,\mu_i}(ytv_2) = I_2(\psi_{1,n_i,\mu_i}(zv_1))$. As above, our notation is intended to convey that the map I_2 includes the uniform interpretation parameter tuple y as a family parameter.

We may suppose that the family of sets that define the underlying set of C in D is given by the formula $\varphi(w, z)$. Let us suppose that $I_2(\varphi(w, z)) = \varphi_2(w_2, yt)$, and that the parameter set z of $\varphi(w, z)$ is partitionable by formulae $\varphi_{n_j,\nu_j}(z)$ for $1 \leq j \leq j_0$ that give uniform, asymptotic estimates across the class $\mathcal{D}$ for the cardinalities of the sub-families that they define. We also have that $\varphi_{2,n_j,\nu_j}(yt) = I_2(\varphi_{n_j,\nu_j}(z))$.

Then for any $C \in \mathcal{C}$ and $a_y a_t \in C$, if $C \models \Gamma(a_y, a_t)$, then by chasing the definitions we see that the following happen:

1. D may be interpreted inside C as D^*, and C may be interpreted inside D as C^*. There are isomorphisms $\alpha : D \cong D^*$ and $\beta : C \cong C^*$. These isomorphisms have specific properties described in the next items.

2. For $a_v \in C$, then as a set $\beta(\psi(u, a_v)) = \psi_1(u_1, \alpha^{-1}(a_t)\beta(a_v))$, and $\alpha\beta(\psi(u, a_v)) = \psi_2(u_2, a_y a_t \alpha\beta(a_v))$, and the maps β and $\alpha\beta$ are of course bijections. Also, $C \models \psi_{2,n_i,\mu_i}(a_y a_t \alpha\beta(a_v))$ if and only if $D \models \psi_{1,n_i,\mu_i}(\alpha^{-1}(a_t)\beta(a_v))$.

   Next, $\alpha\beta(C) = \alpha(\varphi(w, \alpha^{-1}(a_t))) = \varphi_2(w_2, a_y a_t)$, and this is of course a bijection. Also, $C \models \varphi_{2,n_j,\nu_j}(a_y a_t)$ if and only if $D \models \varphi_{n_j,\nu_j}(\alpha^{-1}(a_t))$.

3. Let us consider the formula

$$\Phi_{n_j,\nu_j}(yt) =_{\text{def}} \Gamma(y,t) \ \wedge \ \varphi_{2,n_j,\nu_j}(yt) \tag{4.12}$$

If $C \models \Phi_{n_j,\nu_j}(a_y a_t)$, it follows from our analysis in the previous item and the definition of asymptotic classes 1.2.7 that:

$$| \ |C| - \nu_j |m(C)|^{\frac{n_j}{n}} || = o(|m(C)|^{\frac{n_j}{n}}) \tag{4.13}$$

where the little o notation has meaning as we take the limit $|m(C)| \longrightarrow \infty$. We see equation 4.13 as a 'calibration ' equation: it tells us how to rescale measure/dimension units in the $\mathcal{D}$-class, to measure/dimension units in the $\mathcal{C}$-class.

4. Remembering that the composite isomorphism $\alpha\beta$ is definable in the uniform parameter bi-interpretation via the formula $i_1(\cdot, a_y)$, let us next consider the formula:

$$\begin{aligned} \Psi_{1,n_i,\mu_i}(y,t,v) &=_{\text{def}} \quad \Gamma(y,t) \ \wedge \ v_2 = i_1(v,y) \ \wedge \ \psi_{2,n_i,\mu_i}(ytv_2) \\ \Psi_{0,n_i,\mu_i}(v) &=_{\text{def}} \quad \exists yt(\Psi_{1,n_i,\mu_i}(y,t,v)) \end{aligned} \tag{4.14}$$

If $C \models \Psi_{1,n_i,\mu_i}(a_v)$, then it follows from our analysis in the previous items and the definition of asymptotic classes 1.2.7 that:

$$||\psi(C,a_v)| - \mu_i |m(C)|^{\frac{n_i}{n}} || = o(|m(C)|^{\frac{n_i}{n}}) \tag{4.15}$$

where the little o notation has meaning as we take the limit $|m(C)| \longrightarrow \infty$. We see equation 4.15 as the raw measure/dimension definition for a $\mathcal{C}$-set interpreted in the $\mathcal{D}$-class.

We now combine the raw measure/dimension definition with the calibration equation. Let $n_{ij} = \frac{n_i}{n_j}$ and let $\mu_{ij} = \frac{\mu_i}{\nu_j^{\frac{n_i}{n_j}}}$. Consider the formula:

$$\Psi_{n_{ij},\mu_{ij}}(v) = \exists yt[\Psi_{1,n_i,\mu_i}(y,t,v) \ \wedge \ \Phi_{n_j,\nu_j}(yt)] \tag{4.16}$$

Claim: Suppose $C \models \Psi_{n_{ij},\mu_{ij}}(a_v)$. Then

$$||\psi(C,a_v)| - \mu_{ij} |C|^{n_{ij}}| = o(|C|^{n_{ij}}) \tag{4.17}$$

Proof of Claim: Firstly, let $R = R_C$ be the remainder term such that

$$|C|^{n_{ij}} = \nu_j^{n_{ij}} |m(C)|^{\frac{n_i}{n}} \cdot (1 + \frac{R}{\nu_j |m(C)|^{\frac{n_j}{n}}})^{n_{ij}} \tag{4.18}$$

We know from equation 4.13 that as $|m(C)| \longrightarrow \infty$, $\frac{R}{\nu_j |m(C)|^{\frac{n_j}{n}}} \longrightarrow 0$. The reader can verify the following crude bounds easily:

$$\forall r \in \mathbb{R},\ 0 \leq r \leq 1 :\ (1+r)^{n_{ij}} \leq 1 + n_{ij} \cdot 2^{n_{ij}-1} r \tag{4.19}$$

$$\forall r \in \mathbb{R},\ 0 \leq r \leq 1 :\ (1-r)^{n_{ij}} \geq 1 - n_{ij} \cdot 2^{n_{ij}-1} r \tag{4.20}$$

It follows that there is $c_0 \in \mathbb{R}^+$ such that:

$$\nu_j^{n_{ij}} |m(C)|^{\frac{n_i}{n}} - c_0 R |m(C)|^{\frac{n_i - n_j}{n}} \leq |C|^{n_{ij}} \leq \nu_j^{n_{ij}} |m(C)|^{\frac{n_i}{n}} + c_0 R |m(C)|^{\frac{n_i - n_j}{n}} \tag{4.21}$$

Rearranging, we have:

$$\frac{|C|^{n_{ij}} - c_0 R |m(C)|^{\frac{n_i - n_j}{n}}}{\nu_j^{n_{ij}}} \leq |m(C)|^{\frac{n_i}{n}} \leq \frac{|C|^{n_{ij}} + c_0 R |m(C)|^{\frac{n_i - n_j}{n}}}{\nu_j^{n_{ij}}} \tag{4.22}$$

which we can conveniently substitute into equation 4.15 to obtain:

$$\frac{\mu_i}{\nu_j^{n_{ij}}} |C|^{n_{ij}} - (R_1 + \frac{\mu_i c_0 R |m(C)|^{\frac{n_i - n_j}{n}}}{\nu_j^{n_{ij}}}) \leq |\psi(C, a_v)| \leq \frac{\mu_i}{\nu_j^{n_{ij}}} |C|^{n_{ij}} + (R_1 + \frac{\mu_i c_0 R |m(C)|^{\frac{n_i - n_j}{n}}}{\nu_j^{n_{ij}}}) \tag{4.23}$$

where we know from equation 4.15, that as $|m(C)| \longrightarrow \infty$, $\frac{R_1}{|m(C)|^{\frac{n_i}{n}}} \longrightarrow 0$, and again, we know from equation 4.13 that as $|m(C)| \longrightarrow \infty$, $\frac{R}{\nu_j |m(C)|^{\frac{n_j}{n}}} \longrightarrow 0$.

Define $\varepsilon =_{\text{def}} R_1 + \frac{\mu_i c_0 R |m(C)|^{\frac{n_i - n_j}{n}}}{\nu_j^{n_{ij}}}$. It is clear from equation 4.21 that as $|m(C)| \longrightarrow \infty$ then $\frac{|C|^{n_{ij}}}{|m(C)|^{\frac{n_i}{n}}} \longrightarrow \nu_j^{n_{ij}}$. Combining this with the asymptotic property of the remainder R stated above, we have that as $|C| \longrightarrow \infty$, ε has $o(|C|^{n_{ij}})$. **End of Proof of Claim**

The reader can verify that the sets $\{\Psi_{n_{ij},\mu_{ij}}(v) :\ 1 \leq i \leq i_0,\ 1 \leq j \leq j_0\}$ stratify the family $\psi(u, v)$.

The dimension of the asymptotic class is apparent from our analysis. The dimensions n_{ij} always have as their denominator a number n_j, where n_j is one of

the possible dimensions of the family $\varphi(w,z)$, the family of $\mathcal{L}_2$-sets in which the underlying sets of the members of $\mathcal{C}$ are interpreted in the uniform parameter bi-interpretation. Suppose the possible dimensions of $\varphi(w,z)$ in $\mathcal{D}$ are $\{n_j : 1 \leq j \leq j_0\}$. Let $n_{\mathcal{C}} = \prod_{j=1}^{j_0} n_j$. Then $n_{\mathcal{C}}$ is a possible dimension for the asymptotic class $\mathcal{C}$, and the minimal possible dimension of $\mathcal{C}$ is a divisor of $n_{\mathcal{C}}$.

2. $\mathcal{C}$ is an asymptotic class by Part 1. Furthermore, applying the last paragraph of the proof of Part 1, the minimal possible dimension of $\mathcal{C}$ is a divisor of d. But since $\mathcal{D}$ is uniformly interpretable in $\mathcal{C}$, the underlying sets of the members of $\mathcal{D}$ are uniformly interpreted in $\mathcal{C}$. If, asymptotically, the underlying sets of the members of $\mathcal{C}$ are d-dimensional in $\mathcal{C}$, then conversely, the underlying sets of the members of $\mathcal{D}$ are asymptotically 1-dimensional in $\mathcal{C}$, and the result follows. (For the flavour of the counting that needs to be done for a thorough verification, the reader may look at our very thorough proof of Part 1; this verification is similar.) $\square$

LEMMA 4.2.11 *Suppose $\mathcal{C}$ and $\mathcal{D}$ are uniformly bi-interpretable classes. Inherit the notation of 4.2.3, 4.2.4 and 4.2.7. If in addition:*

1. *There is a formula $\zeta(z)$, where for any $D \in \mathcal{D}$, then $\zeta(D)$ is non-empty, and for $a_z \in D$ with $\zeta(a_z)$, then the $\mathcal{L}_1$-structure determined by $J_2(a_z)$ is isomorphic to $m^{-1}(D)$.*

2. *There is a formula $\eta(y)$, where for any $C \in \mathcal{C}$, then for $a_y \in C$, $\eta(a_y)$ holds if and only if the $\mathcal{L}_2$-structure determined by $J_1(a_y)$ is isomorphic to some member of $\mathcal{D}$.*

Then $\mathcal{C}$ and $\mathcal{D}$ are strongly uniformly bi-interpretable.

Proof Notice that the assumption for η is different to that for ζ; we do not know a priori that for $a_y \in C$ with $\eta(a_y)$, then $J_1(a_y)$ interprets $m(C)$, only that it interprets some member of $\mathcal{D}$; but we do know that if $J_1(a_y)$ interprets a member of $\mathcal{D}$ then $\eta(a_y)$ holds. We make no claim that ζ captures all possible bi-interpretation parameters.

Let us suppose that $I_2(\theta_{2i}(w,z)) = \theta_{2,2i}(w_2,y,t)$ for each $1 \leq i \leq n_2$, and that $I_2(i_2(w,z)) = i_{2,2}(w_2,y,t)$. Then, since $\mathcal{C}$ and $\mathcal{D}$ are uniformly parameter bi-interpretable,

for any $C \in \mathcal{C}$, there are tuples $a_y, a_t \in C$, such that $J_1(a_y)$ interprets $D = m(C)$ as D^*, $I_2(J_2)(a_y a_t)$ re-interprets C inside D^* as C^{**} say, and $i_{2,2}(w_2, a_y, a_t)$ witnesses an isomorphism between $\alpha(D^{**})$ and $\alpha(D)$. Now let $I_2(\zeta(z)) = \zeta_2(y,t)$. Notice that by the assumptions of the lemma we may also assume that $C \models \zeta_2(a_y, a_t)$, and $C \models \eta(a_y)$. By 4.2.3, the languages $\mathcal{L}_1$ and $\mathcal{L}_2$ are finite, so we may define the following inside $\mathcal{L}_1$:

$\Gamma(y,t) = \{yt :$ $J_1(y)$ interprets an $\mathcal{L}_2$-structure; $I_2(J_2)(yt)$ interprets an $\mathcal{L}_1$-structure; $i_1(x,y)$ is an isomorphism of $\mathcal{L}_1$-structures; $i_{2,2}(w_2, y, t)$ is an isomorphism of $\mathcal{L}_2$-structures; $\zeta_2(y,t)$ and $\eta(y)$ hold. $\}$.

Since $\Gamma(a_y, a_t)$ holds, we see that $C \models \exists yt(\Gamma(y,t))$. For any $a_y a_t \in C$ with $C \models \Gamma(a_y, a_t)$, it is clear that we have a parameter bi-interpretation between C and some $\mathcal{L}_2$-structure D'. But $\Gamma(y,t) \Rightarrow \eta(y)$, so $D' \in \mathcal{D}$. Also, $\Gamma(y,t) \Rightarrow \zeta_2(y,t)$, and so D' must be reinterpreting $m^{-1}(D')$. But then $C = m^{-1}(D')$ and so $D' = m(C) = D$. Thus we have a strong uniform parameter bi-interpretation. $\square$

Lemma 4.2.11 will be used extensively in the next chapter. In general, the least obvious requirement in applying the lemma will be its clause 1. This inspires the following definition:

DEFINITION 4.2.12 Suppose the class $\mathcal{C}$ is UPD in class $\mathcal{D}$. Again, inherit the notation of 4.2.3, 4.2.4 and 4.2.7. Then $\mathcal{C}$ is uniformly interpreted in $\mathcal{D}$ via the $\mathcal{L}_2$-formulae $J_2 = \{\theta_{2i}(w,z) : 1 \leq i \leq n_2\}$. Suppose that there is a formula $\zeta(z)$, where for any $D \in \mathcal{D}$ and $a_z \in D$ with $\zeta(a_z)$, then $J_2(a_z)$ interprets $m^{-1}(D)$. Then we say $\mathcal{C}$ *is strongly UPD in $\mathcal{D}$.*

4.3 Results on Generating Asymptotic Classes of Groups

4.3.1 GS_1 Theories

Let us note that the dimension of the dimension/measure pair introduced in 1.2.8 is not necessarily the S_1-rank. Furthermore, a measurable theory is not necessarily an S_1-theory, according to Hrushovski's Definition 4.2 in [15]; we have already described this in 1.2.5, but for convenience we transcribe that definition here:

DEFINITION 4.3.1 We define a rank $S_1(\theta)$ of a first order formula θ in an $\aleph_0$-saturated structure. $S_1(\theta) > 0$ iff θ has infinitely many solutions. $S_1(\theta) > n+1$ iff there exists a sequence b_i of indiscernibles (over a set of definition for θ) and a formula $\varphi(x,y)$, such that:

1. $S_1((\varphi(x,b_1) \wedge \varphi(x,b_2)) \leq n$.
2. $S_1(\theta \wedge \varphi(x,b_i)) > n$ for each i.

If not $S_1(\theta) > n$ and n is the least such, we say that $S_1(\theta) = n$. If q is a partial type, $S_1(q) = \min\{S_1(\theta) : \ q \text{ implies } \theta\}$. $S_1(a/B) = S_1(\mathrm{tp}(a/B))$.

The reader will notice that in a measurable theory dim has very similar properties to the S_1-rank: it increases in the same manner, and it is definable. The reason such a theory is not necessarily an S_1-theory is that the S_1-rank may differ from dim, and the S_1-rank itself may not be definable. This is the case with the theory $ACFA$. We would like to use the useful group generation theorems available for supersimple groups, in our context. This induces us to define GS_1-theories (generalised S_1-theories):

DEFINITION 4.3.2 Let $\mathcal{M}$ be an $\aleph_0$-saturated model and let dim be a function from $\mathrm{Def}(\mathcal{M})$ to $\mathbb{N}$. Let θ be a formula. Then dim is a generalised S_1-rank if

1. $\dim(\theta) > 0$ iff θ has infinitely many solutions.
2. $\dim\ (\theta) > n+1$ if there exists a sequence b_i of indiscernibles (over a set of definition for θ) and a formula $\varphi(x,y)$ such that (i) $\dim(\varphi(x,b_1) \wedge \varphi(x,b_2)) \leq n$; and (ii) $\dim(\theta \wedge \varphi(x,b_i)) > n$ for each i.

If such a dimension dim is understood we may refer to it as a GS_1-rank for $\mathcal{M}$. Conversely, if we refer to the GS_1-rank of a structure $\mathcal{M}$ or one if its definable subsets then implicit is the assumption that $\mathcal{M}$ is equipped with a dimension dim which satisfies the two clauses.

For a partial type P, $\dim(P)$=$\min\{\dim(\theta) : \ P \vdash \theta\}$.

A complete first order theory T is a GS_1-theory with respect to dim if:

1. dim is a generalised S_1-rank.

2. dim is monotonic.

3. For every formula $\varphi(x, y)$ and integer m, $\{b : \dim(\varphi(x, b)) = m\}$ is a $\emptyset$-definable set.

The next lemma shows that finite GS_1-rank implies finite D-rank. The Shelah D-rank is described in [29] 5.1.13.

LEMMA 4.3.3 *(i) Let $\mathcal{M} \models T$ be an $\aleph_0$-saturated model, where T is a GS_1-theory with respect to* dim. *Suppose that $\{b_i : i \in \omega\}$ is an indiscernible sequence of $\mathcal{M}$-elements over the defining parameters a of $\theta(x, a)$, and suppose that $\varphi(\mathcal{M}, b_i) \subseteq \theta(\mathcal{M}, a)$ for all i. Suppose that $\{\varphi(\mathcal{M}, b_i) : i \in \omega\}$ is inconsistent. Then* $\dim(\theta(\mathcal{M}, a)) > \dim(\varphi(x, b_i))$.

(ii) If T is a GS_1-theory, then for any definable set X, $\dim(X) \geq D(X)$.

PROOF Notice that by the definability of rank property for GS_1-theories, dim is preserved under automorphisms.

Say that $\dim(\varphi(x, b_i)) = d$. By indiscernibility and the inconsistency assumption, let us assume that $\{\varphi(\mathcal{M}, b_i) : i \in \omega\}$ is k-inconsistent. It follows that there is $1 \leq c < k$ such that $\dim(\cap_{i=1}^{c} \varphi(x, b_i)) = d$ and $\dim(\cap_{i=1}^{c+1} \varphi(x, b_i)) < d$. Now let $\chi_j = \cap_{i=1}^{c-1} \varphi(x, b_i) \cap \varphi(x, b_j)$. Then by indiscernibility, and the preservation of dim under automorphisms, $\dim(\chi_j) = d$ for all $j \geq c$. By monotonicity of dim we have $\dim(\chi_j \cap \chi_l) < d$ for all $l \neq j \geq c$. It follows that $\dim(\theta(\mathcal{M}, a)) > d$ by the definition of GS_1-rank.

We show that $D(X) \geq r$ implies $\dim(X) \geq r$. This is done by induction on r. The case $r = 0$ is obvious.

Suppose $D(X) \geq r + 1$. Then we may suppose that $\{b_i : i \in \omega\}$ is an indiscernible sequence of $\mathcal{M}$-elements over the defining parameters of X, $\varphi(\mathcal{M}, b_i) \subseteq X$ for all i,

$D(\varphi(\mathcal{M}, b_i)) \geq r$ and $\{\varphi(\mathcal{M}, b_i) : i \in \omega\}$ is k-inconsistent for some $k \in \mathcal{N}$. Then by induction we have $\dim(\varphi(\mathcal{M}, b_i)) \geq r$, and so applying the previous part of the lemma we have $\dim(X) \geq r + 1$. $\square$

THEOREM 4.3.4 *(i) Let T be a measurable theory, with measure dimension function* dim. *Then T is a GS_1-theory with respect to* dim.

(ii) The almost theory of an asymptotic class is a GS_1-theory. In particular, the theory $PSF_{(m,l,p)}$ is a GS_1-theory.

PROOF (i) he reader can recall Definition 1.2.8 for measurable structures and theories.

There are three clauses for T to satisfy to be a GS_1-theory with respect to dim. Condition (3), that the measure dimension is definable, follows from axiom (iib) of Definition 1.2.8. Condition (2), the monotonicity of dim, is a direct application of axiom (iii) for measurable structures. We must now show that dim is a generalised S_1-rank.

Suppose that dim is not a generalised S_1-rank. Thus, there is $M \models T$ where M is $\aleph_0$-saturated, $n \in \mathbb{N}$, $a \in M$, $\theta(x, y)$ and $\psi(x, y)$ formulas, $\theta = \theta(M, a)$ such that $\dim(\theta) = n$, $\{b_i : i \in \mathbb{N}\}$ a sequence of M-elements indiscernible over a, $\psi_i = \psi(M, b_i)$ such that $\dim(\psi_i \cap \psi_j) < n$ for all $i \neq j \in \mathbb{N}$, and $\dim(\theta \cap \psi_i) \geq n$ for all $i \in \mathbb{N}$.

Let us suppose that the measure function for the measurable model M is μ, and let us suppose that $\mu(\theta) = r > 0$. Let $\chi_i = \theta \cap \psi_i$. Since $\chi_i \subseteq \theta$, it is an easy deduction from axiom (iii) for measurable structures that $\dim(\chi_i) = n$. Since the sequence b_i is indiscernable over a, we may assume that for all $i \in \mathbb{N}$, that $\mu(\chi_i) = s > 0$. Now for any $j \in \mathbb{N}$, let $Y_j = \cup_{i=1}^{j} \chi_i$.

Claim: For $j \in \mathbb{N}$, we have $\dim(Y_j) = n$ and $\mu(Y_j) = js$.

Proof of Claim: The dimension claim is clear from axiom (iii) for measurable structures, since we have $\chi_1 \subseteq Y_j \subseteq \theta$, and $\dim(\chi_1) = \dim(\theta) = n$. We prove the second statement by induction on j. For $j = 1$ it is clear. Now $Y_{j+1} = Y_j \cup \chi_{j+1} =$

$Y_j \coprod \chi_{j+1} \backslash (Y_j \cap \chi_{j+1})$. Notice that by axiom (iii) for measurable structures,

$$\begin{aligned} \dim(Y_j \cap \chi_{j+1}) &= \dim(\cup_{i=1}^{j} \chi_i \cap \chi_{j+1}) \\ &= \max(\dim(\chi_i \cap \chi_{j+1}) : \ 1 \leq i \leq j) \\ &< n \end{aligned}$$

Since $\dim(\chi_{j+1}) = n$, axiom (iii) for measurable structures now implies that $\mu(\chi_{j+1} \backslash (Y_j \cap \chi_{j+1})) = \mu(\chi_{j+1}) = s$, and so we now have:

$$\begin{aligned} \mu(Y_{j+1}) &= \mu(Y_j \coprod \chi_{j+1} \backslash (Y_j \cap \chi_{j+1})) \\ &= \mu(Y_j) + \mu(\chi_{j+1} \backslash (Y_j \cap \chi_{j+1}))) \\ &= js + s \\ &= (j+1)s \end{aligned}$$

and our induction proof is complete. **End of proof of claim**

Now pick $j_0 > \frac{r}{s}$. Then $\dim(\theta) = \dim(Y_{j_0}) = n$, $\mu(Y_{j_0}) = j_0 s > r = \mu(\theta)$, but $Y_{j_0} \subseteq \theta$. Clearly this contradicts axiom (iii) for measurable structures.

(ii) The almost theory of an asymptotic class is a measurable theory. So from part (i), it must be a GS_1-theory. We saw in Theorem 3.3.15 that $PSF_{(m,l,p)}$ is the almost theory of the class of difference fields $\mathcal{C}_{m,l,p}$. □

COROLLARY 4.3.5 *(i) Every GS_1-theory is supersimple.*

(ii) Every measurable theory T is supersimple.

PROOF (i) By 4.3.3 (ii) the D-rank is finite. But by [19] Section 6, if D-rank is finite, then S_1-rank, SU-rank and D-rank agree for all formulas. So this means that a GS_1-theory has finite SU-rank and is, by[29] 5.1.5, supersimple.

(ii) This now follows directly from 4.3.4 and part (i). □

4.3.2 Basic lemmas for uniform parameter bi-interpretations between finite simple groups and finite and finite difference fields

This is a technical section detailing group generation lemmas and definable isomorphism extension lemmas of which we shall make use.

FACT 4.3.6 By 4.3.5, the basic facts about group generation in supersimple theories hold in GS_1-theories. In particular, Theorem 5.4.5 and Remark 5.4.7 of [29] hold. They are a version of Zilber's Indecomposability Theorem in the context of groups with simple theories. We report these results in appropriate versions for groups in GS_1-theories, and prove our versions making very great use of Theorem 5.4.5 and Remark 5.4.7 of [29] and their proofs.

THEOREM 4.3.7 *Let G be a definable group in a GS_1-theory. Let X_i be definable subsets of G ($i \in I$). Then there exists a definable subgroup H of G such that:*

(i) $H \subseteq X_{i_1}^{\pm 1} X_{i_2}^{\pm 1} \dots X_{i_m}^{\pm 1}$ for some $i_1, \dots, i_m \in I$ (every element of H is a product of a bounded number of elements of the X_i's and their inverses.)

(ii) X_i/H is finite for each $i \in I$.

PROOF Firstly, Theorem 5.4.5 gives this result except for one important detail: the group H given by that theorem is *hyperdefinable*. However, examining the proof of Theorem 5.4.5, it is clear that the H given there is type-definable. So we have a type-definable group H. By Corollary 4.3.5, we are working in a supersimple theory. Thus, by Theorem 5.5.4 of [29], $H = \cap_{i \in I} H_i$, where the H_i are definable groups. Since $H \subseteq X_{i_1}^{\pm 1} X_{i_2}^{\pm 1} \dots X_{i_m}^{\pm 1}$, we have $H \cap G \backslash X_{i_1}^{\pm 1} X_{i_2}^{\pm 1} \dots X_{i_m}^{\pm 1} = \emptyset$. Thus $\cap_{i \in I} H_i \cap G \backslash X_{i_1}^{\pm 1} X_{i_2}^{\pm 1} \dots X_{i_m}^{\pm 1} = \emptyset$, and so by compactness there is a finite set $I_0 \subseteq I$ such that $\cap_{i \in I_0} H_i \cap G \backslash X_{i_1}^{\pm 1} X_{i_2}^{\pm 1} \dots X_{i_m}^{\pm 1} = \emptyset$. Let $H_0 = \cap_{i \in I_0} H_i$. Then H_0 witnesses our theorem. □

Here is our version of Remark 5.4.7 of [29]:

PROPOSITION 4.3.8 *In the last theorem assume that the collection of sets X_i is invariant under a set of automorphisms $\mathcal{A}$. Then H may be chosen in 4.3.7 such that H is $\mathcal{A}$-invariant.*

PROOF Since we work in a GS_1-theory, we may take an H of some maximum possible GS_1-rank m that witnesses Theorem 4.3.7. Consider the class $\Theta := \{\theta(H) : \theta \in \mathcal{A}\}$. Any member of Θ witnesses Theorem 4.3.7, and they all have GS_1-rank m.

Claim: The members of Θ are uniformly commensurable.

Proof of claim: If not, then by compactness there are two members say $H_1, H_2 \in \Theta$ such that $H_1/(H_1 \cap H_2) = \infty$. We may re-apply Theorem 4.3.7 to the set of groups $\{H_1, H_2\}$. The result is a definable group H such that H satisfies Theorem 4.3.7 with respect to the X_i, and such that $H_1/(H \cap H_1)$ and $H_2/(H \cap H_2)$ are both finite. This means that the GS_1-rank of $H \cap H_1$ is also m.

Now suppose that $H/(H_1 \cap H)$ is finite. Then $H \cap H_2/(H_1 \cap H \cap H_2)$ would be finite. Since $H_2/(H \cap H_2)$ is finite it would follow that $H_2/(H_1 \cap H \cap H_2)$ would be finite, and so also $H_2/(H_1 \cap H_2)$ would be finite. The latter is against our assumption, so we deduce that $H/(H_1 \cap H)$ is infinite. This means that the GS_1-rank of H is strictly greater than the GS_1-rank of $H_1 \cap H$. But the latter is m. We then have a contradiction to the maximality of m as a rank of a group witnessing Theorem 4.3.7 with respect to the X_i. **End of proof of claim**

We may now apply the Bergman-Lenstra Theorem as reported in [29] as Theorem 4.2.4. We apply it to the uniformly commensurable family of subgroups Θ. It yields a definable group $N \subseteq \langle X_i \rangle$, such that N is $\mathcal{A}$-invariant. This is exactly a definable group we are seeking.□.

We refer to the above collectively as Hrushovski's Group Generation Lemma, or $HGGL$. In fact, additional information about the $HGGL$-generated groups can be extracted from Hrushovski's work in [15] and from [29], and we wish to make use of that information. So we present this material:

PROPOSITION 4.3.9 *Let G be a group definable inside a model with GS_1-theory. Let $B = \langle X_i : i \in I \rangle$ be the group generated by the X_i inside G. Then there is a definable group H so that $H \lhd B$, X_i/H is finite for each $i \in I$, and $H \subseteq X_{i_1}^{\pm 1} X_{i_2}^{\pm 1} \dots X_{i_l}^{\pm 1}$ for some $i_j \in I$.*

PROOF Let $J = \{bX_ib^{-1} : b \in B, i \in I\}$. Then we may apply Theorem 4.3.7 and Proposition 4.3.8 to conclude that there is a definable, normal $H \lhd B$, where $H \subseteq Y_{i_1}^{\pm 1} Y_{i_2}^{\pm 1} \dots Y_{i_m}^{\pm 1}$, and each $Y_{i_j} = bX_{i_j}b^{-1}$ for some $i_j \in I$ and $b_j \in B$. Now $b_j \in B$, so $b_j \in X_{i_{b,j,1}}^{\pm} \dots X_{i_{b,j,m_j}}^{\pm 1}$. Thus

$$H \subseteq X_{i_{b,1,1}}^{\pm 1} \dots X_{i_{b,1,m_1}}^{\pm 1} X_{i_1}^{\pm 1} X_{i_{b,1,1}}^{\pm 1} \dots X_{i_{b,1,m_1}}^{\pm 1} \dots X_{i_{b,m,1}}^{\pm 1} \dots X_{i_{b,m,m_m}}^{\pm 1} X_{i_m}^{\pm 1} X_{i_{b,m,1}}^{\pm 1} \dots X_{i_{b,m,m_m}}^{\pm 1}$$

Theorem 4.3.7 and Proposition 4.3.8 also give that X_i/H is finite for each $i \in I$, so this concludes the proof. □

We begin by giving two immediate consequences of the *HGGL*.

LEMMA 4.3.10 *Suppose G is a simple group and is definable in a model with GS_1-theory. Suppose G interprets an isomorphic copy of itself G^* via an $\mathcal{L}_{\text{groups}}(G)$-interpretation. Suppose that we have an isomorphism $i : G \cong G^*$. Suppose $X \subseteq G$ is an $\mathcal{L}_{\text{groups}}(G)$-definable infinite subset of G, and suppose the restriction $i|_X$ is $\mathcal{L}_{\text{groups}}(G)$-definable. Then i is $\mathcal{L}_{\text{groups}}(G)$-definable.*

PROOF Let $J = \{gXg^{-1} : g \in G\}$. Clearly, if $i|_X$ is $\mathcal{L}_{\text{groups}}(G)$-definable, then $i|_{X^{-1}}$ is $\mathcal{L}_{\text{groups}}(G)$-definable. Also, $i|_{gXg^{-1}}$ is $\mathcal{L}_{\text{groups}}(G)$-definable for any $g \in G$. So $i|_Y$ is $\mathcal{L}_{\text{groups}}(G)$-definable, where $Y = X_1^{\pm 1} \dots X_l^{\pm 1}$ is some product of sets $X_i \in J$. By 4.3.9, there is such a Y and a definable subgroup H, such that $H \subseteq Y$, X/H is finite, and $H \lhd G$. Since X/H is finite and X is infinite, it follows that $H \neq 1$. So $H = G$. So $Y = G$, and $i = i|_G = i|_Y$. Thus, i is $\mathcal{L}_{\text{groups}}(G)$-definable. □

Using the above lemmas, we may simplify the criteria for existence of a bi-interpretation between a simple group G, and an infinite structure S such that S has a GS_1-theory .

LEMMA 4.3.11 *Suppose G is a simple group. Let S be an infinite structure with GS_1-theory, and suppose S interprets G. Also, suppose that G interprets the structure*

S. Suppose that the underlying set of the interpretation of S in G is a subset of G, and that there is a $\mathcal{L}_S$-definable isomorphism between S and its re-interpretation in G. Then S and G are bi-interpretable.

PROOF Let us draw a diagram and explain what we are given:

$$\begin{array}{ccccc} G_U & \supseteq & S_U & \longrightarrow & G_2 \\ & \searrow\ i_G & & \searrow\ i_G & \\ & & & & \\ & \nearrow\ i_S & & \nearrow\ i_S & \\ S_D & \longrightarrow & G_D & \supseteq & S_2 \end{array}$$

[1] The diagram has several copies of G and several copies of the structure S. The top row shows G (copy G_U) containing a definable copy of S (copy S_U). We witness the isomorphism between S and S_U by isomorphism $i_S : S_D \cong S_U$. The bottom row shows S (copy S_D) interpreting a definable copy of G (copy G_D). We witness the isomorphism between G and G_D by isomorphism $i_G : G_U \cong G_D$. The isomorphism i_S induces an interpretation of a copy of G (copy G_2) inside S_U; G_2 may be seen as a re-interpretation of G_U inside itself. Similarly, the isomorphism i_G induces an interpretation of a copy of S (copy S_2) inside G_D; S_2 may thus be seen as a re-interpretation of S_D inside itself. The conditions of the lemma state that the composite isomorphism $i_{GS} = i_G \circ i_S$ may be taken to be definable in the structure S. Suppose that it is defined by the $\mathcal{L}_S$-formula $\theta_{i_{GS}}(x, y, a_S)$ for some $a_S \in S$. Let us suppose that $\theta_{1,i_{GS}}(x_1, y_1, i_S(a_S))$ is the interpretation of $\theta_{i_{GS}}(x, y, a_S)$ inside the interpretation of S_U inside G_U. To prove that S and G are bi-interpretable, we need to show that the composite isomorphism $i_{SG} = i_S \circ i_G$ is definable inside the group G_U.

We begin by showing that the restriction $i_{SG}|_{S_U}$ is definable in G_U. Let $a_w \in S_U$, and let $a_x \in S_D$ be such that $a_w = i_S(a_x)$. Then

$$\begin{aligned} i_G(a_w) &= i_G \circ i_S(a_x) \\ &= \{!x \in S_2 : \theta_{i_{GS}}(x, a_x, a_S)\} \end{aligned}$$

[1] The subscripts $_U$ and $_D$ in the diagram are for up and down, and are merely to separate out different interpretations of S and G.

Thus

$$\begin{aligned} i_S \circ i_G(a_w) &= i_S \circ i_G \circ i_S(a_x) \\ &= i_S(\{!x \in S_2 : \ \theta_{i_{GS}}(x, a_x, a_S)\}) \\ &= \{!x \in G_2 : \ \theta_{1,i_{GS}}(x_1, i_S(a_x), i_S(a_S))\} \\ &= \{!x \in G_2 : \ \theta_{1,i_{GS}}(x_1, a_w, i_S(a_S))\} \end{aligned}$$

This shows that the restriction $i_{SG}|_{S_U}$ is definable in G_U by the formula $\theta_{1,i_{GS}}(x_1, y_1, i_S(a_S))$.

But now the result follows from Lemma 4.3.10. □

We now give a uniform parameter version of Lemma 4.3.10:

LEMMA 4.3.12 *Let $\mathcal{C}$ be a class of finite simple groups. Let $\mathcal{D}$ be a class of finite structures in a finite language, and suppose that the almost theory of $\mathcal{D}$ is a GS_1-theory.*

Suppose that $\mathcal{C}$ and $\mathcal{D}$ are matched via a matching m, and that we have a collection $\Omega := \{\Omega_{C,D} : \ C \in \mathcal{C}, D = m(C)\}$ of parameter bi-interpretations between pairs $(C, m(C))$.

Additionally, suppose that Ω is known to satisfy all the requirements to be a uniform parameter bi-interpretation, except for the clause of 4.2.3 demanding for class $\mathcal{C}$ uniformly definable isomorphisms between groups and their re-interpretations. Suppose that for any pair $C \in \mathcal{C}$, $D \in \mathcal{D}$ with $C = m(D)$, that the underlying set of the interpretation of D in C inside $\Omega_{C,D}$, is a subset of C. Then $\mathcal{C}$ and $\mathcal{D}$ are uniformly parameter bi-interpretable using Ω.

PROOF With respect to m and J, all that is missing is to show the uniformly definable isomorphism for structures and their re-interpretations in $\mathcal{C}$.

We proceed by assuming the lemma is not true, and deriving a contradiction. A contradiction to the lemma involves an infinite set of tuples $\{(C_j, D_j, C_j^*, C_j^{***}, D_j^{**}, i_j) : j \in \omega\}$, where

- $C_j \in \mathcal{C}$ and $D_j = m(C_j)$.

- C_j^* is the interpretation of C_j in D_j, inside Ω_{C_j,D_j}.
- C_j^{***} is the re-interpretation of C_j^* inside itself, inside Ω_{C_j,D_j}.
- $D_j^{**} \subseteq C_j^*$ is the re-interpretation of D_j inside itself, inside Ω_{C_j,D_j}.
- i_j is the isomorphism between C^* and C^{***} inside Ω_{C_j,D_j}.
- The i_j is not $\mathcal{L}_{\text{groups}}$-uniformly parameter definable across $\{C_j^* : j \in \omega\}$.
- However, the restrictions $i_j|_{D_j^{**}}$ are uniformly $\mathcal{L}_{\text{groups}}$-parameter definable across $\{C_j^* : j \in \omega\}$.

To derive a contradiction, it suffices to show that the i_j are $\mathcal{L}_{\text{groups}}$-uniformly parameter definable across $\{C_j^* : j \in \omega\}$. We choose to work with C_j^* and not the C_j because the former come embedded inside the D_j, and so we may apply our results about groups definable inside models with GS_1-theories. The reader can verify that we still obtain results about $\mathcal{L}_{\text{groups}}$- definability.

Now we may take a non-principal ultraproduct of the D_j and work inside this structure. We obtain a tuple $(D, C^*, C^{***}, D^{**}, i)$, where

- $D = \prod_{j\in\omega} D_j/\sim$.
- $D^{**} = \prod_{j\in\omega} D_j^{**}/\sim$.
- $C^* = \prod_{j\in\omega} C_j^*/\sim$.
- $C^{***} = \prod_{j\in\omega} C_j^{***}/\sim$.
- C^* and C^{***} are isomorphic as groups via an isomorphism i, but this isomorphism may not be $\mathcal{L}_{\text{groups}}$-parameter definable. However, $D^{**} \subseteq C^*$ and $i|_{D^{**}}$ is $\mathcal{L}_{\text{groups}}$-parameter definable.

Thus we may apply Lemma 4.3.11 to deduce that i is $\mathcal{L}_{\text{groups}}$-parameter definable via some formula $\theta_i(x, y, a_{C^*})$. Now suppose that the ultraproduct element a_{C^*} has a representative $(a_j : j \in \omega)$. Then it follows that for all but finitely many $j \in \omega$, $\theta_i(x, y, a_j)$ defines i_j. The exceptions may be explicitly handled and we have the necessary contradiction. $\square$

REMARK 4.3.13 Lemma 4.3.12 will be crucial in the following chapter. We will apply the lemma to classes $\mathcal{C}$ of finite simple groups of a fixed Lie Type and Lie Rank, and to classes $\mathcal{D}$, where for a given $\mathcal{C}$, we choose $\mathcal{D}$ to be the class of fields of definition or difference fields of definition of the groups in $\mathcal{C}$. For ease, let us refer to the latter two types of structure as just 'definition fields'. Lemma 4.2.11 will also be critical: we shall work to show uniform parameter bi-interpretations between the classes of group and fields, and then apply 4.2.11 to show that we have strong uniform parameter bi-interpretations.

Chapter 5

Asymptotic Finite Simple Groups

5.1 Chapter Introduction

In this chapter we parse the finite simple groups of Lie type into various classes. For a given class $\mathcal{C}$ of Chevalley groups in our parsing, we exhibit a strong uniform bi-interpretation with a class of pure finite fields. Then, for a given class $\mathcal{C}$ of twisted groups in our parsing, we exhibit a strong uniform bi-interpretation with a class of its 'definition fields'. Definition fields will be expansions of pure fields in which the members $\mathcal{C}$ are naturally interpretable. It transpires that they are either pure fields or difference fields.

As a result of our constructed bi-interpretations, we can apply Proposition 4.2.10 and the theory of finite fields, and the theory of finite fields with a fractional power of the Frobenius, to conclude that our classes of finite simple groups are asymptotic classes.

The chapter is organised as follows: section 5.2 constructs strong uniform parameter bi-interpretations for Chevalley groups. Then section 5.3 presents strong uniform parameter bi-interpretations for twisted simple groups where all roots are of the same length. Finally, in section 5.4, the case of twisted simple groups with roots of differing lengths is presented.

5.2 Chevalley Groups

5.2.1 Background

This is a technical section that we need; it does contain some results and notation around Chevalley groups, but Chapter 16 of [1] would serve much better as an introduction, and [4] contains all the details.

DISCUSSION 5.2.1 We begin by presenting our notation, and some facts about the algebraic objects we use. We follow [4]. We shall work over a family $\mathcal{C}$ of Chevalley groups of a fixed Lie type and Lie rank. We begin by defining the underlying Lie algebra uniformly. The trick is the use of the Chevalley basis. Suppose $\mathbb{L}$ is a simple Lie algebra over $\mathbb{C}$. Suppose Φ is a root system for $\mathbb{L}$ and $\mathbb{L} = \mathbb{H} \oplus \sum_{r\in\Phi} \mathbb{L}_r$ is a Cartan decomposition of $\mathbb{L}$. Let Π be a fundamental system in Φ. Basis elements of

$\mathbb{H}$ $(h_r : r \in \Pi)$ and basis elements for the root spaces $(e_r : r \in \Phi)$ may be picked, so that the brackets of all pairs of these basis elements are integral combinations of basis vectors. The coefficients of multiplication are explicitly stated in [4] Theorem 4.2.1. Such a basis is known as a Chevalley basis. With this presentation, we may extend the basis elements only by coefficients in $\mathbb{Z}$, and view the resulting object as a Lie algebra over $\mathbb{Z}$. Call that object $\mathbb{L}_\mathbb{Z}$. Now let K be an arbitrary field. Clearly there are natural homomorphisms from $\mathbb{L}_\mathbb{Z}$ into Lie algebras $\mathbb{L}_K = K \otimes_\mathbb{Z} \mathbb{L}_\mathbb{Z}$. The bracket $[,]$ on $\mathbb{L}_K$ is uniformly definable as the bilinear extension of the bracket on the Chevalley basis elements. Thus, the Lie algebras $\mathbb{L}_K$ are uniformly definable over all fields. Relative to this UPD of the $\mathbb{L}_K$, the group of linear automorphisms $\mathrm{GL}(\mathbb{L}_K)$ is also UPD over all fields.

Now we review the definition of the root subgroups. For each e_r above, and $\zeta \in K$, the mapping ad ζe_r is a nilpotent derivation of $\mathbb{L}_K$. It is easy to see from the description of the ad action on the basis of a Cartan decomposition that there is an upper bound $n \in \mathbb{N}$ so that for all K, and all $e_r \in \mathbb{L}_K$ we have $(\text{ad } e_r)^n = 0$. This means that the root subgroups

$$X_r(K) = \{\exp(\text{ad } \zeta e_r) = 1 + \zeta \text{ ad } e_r + \frac{\zeta^2(\text{ad } e_r)^2}{2!} + \ldots \frac{\zeta^{n-1}(\text{ad } e_r)^{n-1}}{(n-1)!} : \zeta \in K\}$$

are UPD over all K. We shall frequently work with the root subgroups and we use the following notation:

$$x_r(\zeta) =_{\text{def}} \exp(\text{ad } \zeta e_r)$$

Now for K a finite field, and $\mathbb{L}$ a simple Lie algebra over $\mathbb{C}$, the Chevalley group $\mathbb{L}(K)$ is the group of linear isomorphisms of $\mathbb{L}_K$ generated by the root subgroups $X_r(K)$ above ([4] 4.4).

Since we work over classes of fixed Lie type and Lie rank, we shall at times talk about an ambient $\mathbb{L}$, Φ, Π, and W (the Weyl group of $\mathbb{L}$). In the case of Φ and Π recall that we may fix a Chevalley basis over $\mathbb{Z}$, and then Φ and Π may be given a concrete meaning with respect to this basis.

We now present a further collection of facts and lemmas which we use. The notations used in the following 'fact' will be used in the constructions of the bi-interpretations.

FACT 5.2.2 We assume we have a field K, a Chevalley group $G = \mathbb{L}(K)$ and its adjoint representation on a Lie algebra $\mathbb{L}_K$. We assume $\mathbb{L}_K$ comes equipped with a root system Φ and a root ordering $\prec$. The root ordering $\prec$ is not arbitrary; we assume it is of the specific kind described in [4] Chapter 2, and from Φ and $\prec$, we assume that we have the associated fundamental system of positive roots Π. We also take W to be the Weyl group for Φ.

1. For a fixed root $r \in \Phi$ we denote the group $A_1(K)_r$ to be the group $\langle X_r, X_{-r} \rangle$. In chapter 6 of [4] a homomorphism h_{SL_2} from $SL_2(K)$ onto $\langle X_r, X_{-r} \rangle$ is constructed. We have
$$h_{SL_2} : \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mapsto x_r(t)$$
and
$$h_{SL_2} : \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}) \mapsto x_{-r}(t)$$
In the notation of Carter, for the diagonal elements
$$h_{SL_2} : \begin{pmatrix} t & 0 \\ 0 & \frac{1}{t} \end{pmatrix} \mapsto h_r(t)$$
We denote by H_r the group comprising the elements $h_r(t)$ for $t \in K^\times$. Of course H_r is isomorphic to $K^\times$, and X_r to K^+. There are other important elements that can be defined via the homomorphism h_{SL_2}:
$$n_r(t) =_{\text{def}} h_{SL_2} \begin{pmatrix} 0 & t \\ -t^{-1} & 0 \end{pmatrix}$$
We also define
$$n_r =_{\text{def}} n_r(1)$$
An important group will be N, the subgroup of G generated by H and the elements n_r for all $r \in \Phi$.

2. In [4] 7.1 the group H is defined as the product of all the H_r for $r \in \Phi$. It is a commutative group, commonly known as a maximal torus.

3. By definition, U is the group generated by the roots subgroups X_r for $r \in \Phi^+$. It is a fact that U is a maximal unipotent subgroup of G. Suppose that $r_1, r_2, \ldots, r_l$

are the members of Φ^+ in their $\prec$-order. Theorem 5.3.3 of [4] shows that each element $x \in U$ is expressible uniquely as a product string $x_{r_1}(t_1)x_{r_2}(t_2)\dots x_{r_l}(t_l)$. Call this a Chevalley expression for x, and call $U = X_{r_1}X_{r_2}\dots X_{r_l}$ the Chevalley cell presentation for U.

Let V be the opposite group to U. That is, V is the group generated by the root subgroups X_r for $r \in \Phi^-$. Of course, V is also a maximal unipotent subgroup of G, and has a Chevalley cell presentation.

4. In [4] section 7.1 it is shown that

$$h_r(\lambda)x_s(t)h_r(\lambda)^{-1} = x_s(\lambda^{A_{rs}}t) \quad (\text{for } r,s \in \Phi^+,\ \lambda,t \in K^\times)$$

Recall that $A_{rs} = \frac{2(r,s)}{(r,r)}$ where (r,s) is the Killing form on the roots r,s. The tables of A_{rs} values are on pp. 45 of [4]. In particular, H acts on root subgroups by conjugation. From here on, unless specifically stated, when we refer to the action of H-elements on U or its subgroups, we mean by conjugation. Now let $P = \mathbb{Z}[\Phi]$. Each $h \in H$ induces a character $\chi :\ P \mapsto K^\times$ such that χ may be defined via the action of h on the root subgroups:

$$x_s(\chi(s)\cdot t) = hx_s(t)h^{-1} \ (\text{for}\ \ s \in \Phi,\ x_s(t) \in X_s)$$

and so $\chi(s) = \lambda^{A_{rs}}$ when $h = h_r(\lambda)$.

5. Let $w \in W$. We let $\Psi_1 = \{r \in \Phi^+ :\ w(r) \in \Phi^+\}$, and $\Psi_2 = \{r \in \Phi^+ :\ w(r) \in \Phi^-\}$. We let $U_w^+ = \prod_{r\in\Psi_1} X_r$ and $U_w^- = \prod_{r\in\Psi_2} X_r$. Using the commutator rules for multiplication of root elements (see [4] section 5.2), it is easy to see that U_w^+ and U_w^- are subgroups of U.

Theorem 7.2.2 of [4] shows there is a natural homomorphism $N \twoheadrightarrow W$ with kernel H. For each $w \in W$ we pick a representative preimage $n_w \in N$, with $n_1 = 1$. Then the unique Bruhat decomposition (corollary 8.4.4 of [4]) states that each element of G has a unique expression in the form $g = u_1hn_wu$ where $u_1 \in U$, $h \in H$, $w \in W$ and $u \in U_w^-$.

6. Let $r, s \in \Phi$ and $t, l \in K^\times$. The following formulae all come from [4]:

$$n_r(1) = n_r \quad ([4]\ 6.4.4)$$
$$n_r(-1) = n_r^{-1} \quad ([4]\ 6.4.4)$$
$$n_r(t) = x_r(t)x_{-r}(-t^{-1})x_r(t) \quad ([4]\ 6.4.4)$$
$$h_r(t) = n_r(t)n_r(-1) \quad ([4]\ 6.4.4)$$
$$n_r x_s(t) n_r^{-1} = x_{w_r(s)}(\eta_{r,s}t) \quad ([4]\ 7.2.1)$$

Here $\eta_{r,s} = \pm 1$. Some facts about $\eta_{r,s}$ are presented in [4] 6.4.3 - in particular $\eta_{r,s}\eta_{r,-s} = 1$. So $\eta_{r,s} = \eta_{r,-s} = 1$ or $\eta_{r,s} = \eta_{r,-s} = -1$. We also immediately deduce from these facts that:

$$n_r(1)^2 = n_r(-1)^{-2} = h_r(-1)^{-1} = h_r(-1)$$

and we now use them again to calculate $n_r(t)h_s(l)n_r(t)^{-1}$:

$$\begin{aligned}
& n_r(t)h_s(l)n_r(t)^{-1} \\
= \quad & h_r(t)n_r x_s(l)x_{-s}(-l^{-1})x_s(l)x_s(-1)x_{-s}(1)x_s(-1)n_r^{-1}h_r(t)^{-1} \\
= \quad & h_r(t)((n_r x_s(l)n_r^{-1})(n_r x_{-s}(-l^{-1})n_r^{-1})(n_r x_s(l)n_r^{-1}) \cdot \\
& (n_r x_s(-1)n_r^{-1})(n_r x_{-s}(1)n_r^{-1})(n_r x_s(-1)n_r^{-1}))h_r(t)^{-1} \\
= \quad & h_r(t)(x_{w_r(s)}(\eta_{r,s}l)x_{w_r(-s)}(-\eta_{r,-s}l^{-1})x_{w_r(s)}(\eta_{r,s}l) \cdot \\
& x_{w_r(s)}(-\eta_{r,s})x_{w_r(-s)}(\eta_{r,-s})x_{w_r(s)}(-\eta_{r,s}))h_r(t)^{-1} \\
& = h_r(t)n_{w_r(s)}(\eta_{r,s}l)n_{w_r(s)}(-\eta_{r,s})h_r(t)^{-1} \\
& = h_{w_r(s)}(l)
\end{aligned}$$

Thus we deduce that for any $w \in W$ and $n_w \in N$ we have $n_w h_s(l) n_w^{-1} = h_{w(s)}(l)$. By Section 7.1 of [4] we have that $h_s(l)$ induces the character $r \mapsto l^{2\frac{(s,r)}{(s,s)}}$ where $(,)$ is the Killing form and $r \in \Phi$. Similarly $h_{w(s)}(l)$ induces the character $r \mapsto l^{2\frac{(w(s),r)}{(w(s),w(s))}}$.

REMARK 5.2.3 Exceptions: Suppose we have a uniform parameter bi-interpretation/strong uniform parameter bi-interpretation between classes $\mathcal{C}$ and $\mathcal{D}$, except for a finite number of exceptions. Specifically, suppose $\mathcal{C} = \mathcal{C}_{\text{exceptions}} \coprod \mathcal{C}_{\text{uniform}}$, $\mathcal{D} = \mathcal{D}_{\text{exceptions}} \coprod \mathcal{D}_{\text{uniform}}$, $|\mathcal{C}_{\text{exceptions}}| = |\mathcal{D}_{\text{exceptions}}| = l$ for some $l \in \mathbb{N}$, we have a matching m between $\mathcal{C}$

and $\mathcal{D}$ such that $m(\mathcal{C}_{\text{exceptions}}) = \mathcal{D}_{\text{exceptions}}$, and we have a uniform parameter bi-interpretation/strong uniform parameter bi-interpretation between classes $\mathcal{C}_{\text{uniform}}$ and $\mathcal{D}_{\text{uniform}}$ via the match m. Then we may extend the uniform parameter bi-interpretation/strong uniform parameter bi-interpretation to one between $\mathcal{C}$ and $\mathcal{D}$ via the match m. This is because the languages are finite by definition, and because asymptotic classes treat finite structures, definition formulae can always be augmented to treat special, exceptional pairs explicitly. On the other hand, if $|\mathcal{C}_{\text{exceptions}}| = \infty$, then, of course, the appropriate $\mathcal{C}_{\text{uniform}}/\mathcal{D}_{\text{uniform}}$ subclasses must be specified.

5.2.2 Statement of theorem

Let us begin by discounting the few non-simple Chevalley groups. In all the following statements, the following groups are excluded: $A_1(2)$ and $A_1(3)$, $C_2(2) = B_2(2)$ and $G_2(2)$, and as demanded in Remark 5.2.3, we also explicitly deem $|K| > 3$.

With these provisos, the theorem we prove is:

THEOREM 5.2.4 *Let $\mathcal{C}_{\mathbb{L},n}$ be the class of all finite Chevalley groups of a fixed Lie type $\mathbb{L}$ and fixed Lie rank n. For $G \in \mathcal{C}_{\mathbb{L},n}$, $G = \mathbb{L}(K)$ and G may be matched uniquely with K. With this matching, $\mathcal{C}_{\mathbb{L},n}$ is strongly uniformly parameter bi-interpretable with the class of finite fields.*

The cardinalities of the Chevalley groups have been explicitly determined. Consequently, the first part of the lemma is clear, since for $q \neq q'$ inspection shows $|\mathbb{L}(\mathbb{F}_q)| \neq |\mathbb{L}(\mathbb{F}_{q'})|$.

We now use Lemma 4.3.12 to show the second part of the theorem. In the following sections we break the task into three parts:

1. In 5.2.3 we give the uniform interpetation of the group $\mathbb{L}(K)$ in the field K.
2. In 5.2.4 we give the uniform interpretation of the field K in the group $\mathbb{L}(K)$.
3. In 5.2.4 we also give the uniform isomorphism between K and its re-interpretation inside itself.
4. In 5.2.5 we apply Lemmas 4.2.11 and 4.3.12 to conclude the theorem.

5.2.3 Chevalley groups: Interpreting $\mathbb{L}(\mathbb{F}_q)$ in $\mathbb{F}_q$ uniformly

In Discussion 5.2.1 we showed that $\mathbb{L}_K$ and thus $\mathrm{GL}(\mathbb{L}_K)$ are UPD over the class of fields. We also demonstrated that the root subgroups were UPD. Now by definition the root subgroups generate the simple group $G = \mathbb{L}(K)$.

If we fix the algebra $\mathbb{L}$, and let the finite field K vary, explicit bounds may be given for the length of product strings of root subgroup elements needed to generate the entire group $\mathbb{L}(K)$. These uniform bounds on generation of $\mathbb{L}(K)$ by root subgroups show that the class $\mathcal{C}_{\mathbb{L},n}$ is uniformly interpretable inside the class of finite fields. We now give a proof of the existence of these bounds:

LEMMA 5.2.5 *There is an $m \in \mathbb{N}$ and a map $\varphi : \{1, 2, \ldots m\} \mapsto \Phi$ such that for every $G = \mathbb{L}(K) \in \mathcal{C}_{\mathbb{L},n}$*

$$G = \prod_{i=1}^{m} X_{\varphi(i)}(K)$$

PROOF By the Bruhat decomposition ([4] 8.4.4) we need to show only an upper bound for generation of H, U, V (the opposite group to U) and N (see 5.2.2 (1) for details about these groups). For U and V the necessary result is 5.2.2 (3).

If we follow [4] section 6.1 [1] , we see that any element $x \in SL_2(K)$ may be written $x = \begin{pmatrix} 1 & \zeta_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \zeta_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & \zeta_3 \\ 0 & 1 \end{pmatrix}$, or $x = \begin{pmatrix} 1 & 0 \\ \zeta_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & \zeta_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \zeta_3 & 1 \end{pmatrix} \begin{pmatrix} 1 & \zeta_4 \\ 0 & 1 \end{pmatrix}$ for $\zeta_1,\ \zeta_2,\ \zeta_3, \zeta_4 \in K$. Thus by 5.2.2 (1) every element $h_r(\zeta)$ is generated in a product of four root subgroups. Since we have assumed that the Lie rank of G is n, it follows that any element of H is the product of at most n elements of type $h_r(\zeta)$ for some $r \in \Phi$ and $\zeta \in K$. So it now follows that every element of H is generated in a product of $4n$ root subgroups. From our description these $4n$ subgroups are UPD across $\mathcal{C}_{\mathbb{L},n}$. In fact, this is virtually the same proof as for N. We use the natural isomorphism $N/H \cong W$, where W is the Weyl group of $\mathbb{L}$. The element $n_r(t) \in \langle X_r, X_{-r} \rangle$ (see [4] pp.96 for

[1] In fact, there is a typo in [4] 6.1.1: its final matrix equation should read $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha^{-1} - 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha - 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\alpha^{-1} \\ 0 & 1 \end{pmatrix}$

a precise definition), and so it is lies in the product of at most four root subgroups. However, the image of $n_r(t)$ in W is a reflection in the hyperplane perpendicular to r. These reflections generate W; W is finite and so its generation by reflections certainly has an absolute upper bound! Since H is boundedly generated, and every element of W has a representative generated by a product of boundedly many root subgroups, it follows that N is also generated by a product of boundedly many root subgroups. Again the definition of these root subgroups is UPD over $\mathcal{C}_{\mathbb{L},n}$ and this follows from our description. $\square$

REMARK 5.2.6 In terms of Definition 4.2.12, 5.2.5 means that the Chevalley groups are strongly UPD in finite fields.

5.2.4 Chevalley groups: Interpreting $\mathbb{F}_q$ in $\mathbb{L}(\mathbb{F}_q)$ uniformly and the uniform isomorphism from a field of definition to its re-interpetation

In this section all we are given is $\mathcal{C}_{\mathbb{L},n}$, the family of Chevalley groups of type $\mathbb{L}$. We will produce a uniform parameter interpretation of the class of finite fields inside $\mathcal{C}_{\mathbb{L},n}$. We work with a typical $G \in \mathcal{C}_{\mathbb{L},n}$, and for some adjoint representation of G let us fix a root system Φ, a root ordering $\prec$, a positive system Φ^+ and a fundamental basis Π. We denote the underlying field of G as K. I make no claim here of uniform definability. All we are doing is fixing an adjoint representation of G as in the previous subsection.

Our first aim in this subsection is to interpret K uniformly over $\mathcal{C}_{\mathbb{L},n}$. Here is the key lemma:

LEMMA 5.2.7 *There is $m \in \mathbb{N}$ such that if $|K| > 7$, H is uniformly parameter definable over $\mathcal{C}_{\mathbb{L},n}$, as the intersection $\cap_{i=1}^{m} C_G(h_i)$ of centralisers of some m of its non-trivial elements.*

PROOF Since we have assumed at the beginning of this section that $|K| > 3$, there is $\zeta \in K^\times$ such that $\zeta^2 \neq 1$. Let $r \in \Phi$. Then by 5.2.2 (4), $h_r(\zeta) \in H$ is an element with non-trivial conjugation action on the root subgroup X_r. Now clearly $H \leq C_G(h_r(\zeta))$. Suppose $g \in \cap_{r\in\Phi^+} C_G(h_r(\zeta))$. Fix an arbitrary $r \in \Phi^+$ and for ease denote $h_r(\zeta)$ by h. Then by the unique Bruhat decomposition (5.2.2 (5)) we may

write $g = u_1 h_1 n_w u$ where where $u_1 \in U$, $h_1 \in H$, $w \in W$ and $u \in U_w^-$. Now notice that $hgh^{-1} = hu_1h^{-1} \cdot h_1 \cdot hn_wh^{-1}huh^{-1}$. Since $H \triangleleft N$ (5.2.2 (5)) we may write $hn_wh^{-1} = h_2n_{w'}$ for some $w' \in W$. Further, by 5.2.2 (4), $hu_1h^{-1} \in U$ and $huh^{-1} \in U_w^-$. So by the unique Bruhat decomposition we have the equations $u_1 = hu_1h^{-1}$, $h_1 = h_1h_2$, $n_w = n_{w'}$ and $u = huh^{-1}$. Thus $h_2 = 1$. Also, by the Chevalley expression for elements of U (5.2.2 (3)) and the fact that h acts non-trivially on the root subgroup r, it is immediate that neither u nor u_1 have an r-component in their Chevalley expression. Since r was chosen arbitrarily, we conclude that $u = u_1 = 1$ and $g \in N$.

Claim: For each $n \in N\backslash H$ there is $h \in H$ such that n does not commute with h.

Proof of Claim: Let $n \in N\backslash H$. Suppose n maps to w under the natural homomorphism from N to W. Let $s, r \in \Phi$. Then by 5.2.2 (6), we have (i) $nh_s(l)n^{-1} = h_{w(s)}(l)$, (ii) $h_s(l)$ induces the character χ where $\chi(r) = l^{2\frac{(s,r)}{(s,s)}}$ and (iii) $h_{w(s)}(l)$ induces the character χ' where $\chi'(r) = l^{2\frac{(w(s),r)}{(w(s),w(s))}}$. Now if n and $h_s(l)$ commute then $h_s(l) = h_{w(s)}(l)$ and $\chi = \chi'$. In Section 3.4 of [4] it is shown that $|2\frac{(r,s)}{(r,r)}| \leq 3$. Thus if $\chi = \chi'$ then l must satisfy an equation $l^{k_1-k_2} = 1$, where $0 \leq k_1 = 2\frac{(s,r)}{(s,s)} \leq 3$ and $0 \leq k_2 = 2\frac{(w(s),r)}{(w(s),w(s))} \leq 3$.

Select l^* to be a generator for the cyclic group $K^\times$. Then we see that for $|K| > 7$, if $\chi = \chi'$, then for $(l^*)^{k_1-k_2} = 1$, we require that $k_1 = k_2$, and so $\frac{(s,r)}{(s,s)} = \frac{(w(s),r)}{(w(s),w(s))}$ for all $r \in \Phi$. Since w is an isometry of $\mathbb{L}$ as a Euclidean space, and since Φ spans $\mathbb{L}$, we have $(s - w(s), v) = 0$ for all $v \in \mathbb{L}$. Setting $v = s - w(s)$ we see that this implies that $s = w(s)$. Now there is some $s^* \in \Phi$ such that $w(s^*) \neq s^*$. We conclude that n does not commute with $h_{s^*}(l^*)$. **End of proof claim**

Since H is a normal commutative subgroup of N, it follows that for each non-identity coset nH of the quotient group N/H, we may pick $h_w \in H$ such that h_w does not commute with any element of nH.

Thus for all finite fields with $|K| > 7$, H is UPD and is defined as $H = \cap_{r\in\Phi^+} C_G(h_r(\zeta)) \cap_{w\in W} C_G(h_w)$. $\square$

COROLLARY 5.2.8 *H is uniformly definable in any family of finite Chevalley groups*

of fixed Lie type and Lie rank. So too are the root subgroups X_r.

PROOF The first statement follows by Lemma 5.2.7.

Referring to 5.2.2 (1) and (4), let us examine the conjugation action of H_r on a root subgroup X_r: $h_r(\zeta)x_r(t)h_r(\zeta^{-1}) = x_r(\zeta^2 t)$. It follows that X_r may be presented as the union of at most two H_r-orbits. Since the whole of H acts on X_r via conjugation, it is clear that X_r may be presented as the union of at most two H-orbits. We have now seen that H is UPD, and so the root subgroups X_r are also UPD. □

We will use dot $\cdot$ notation for the H conjugation action on X_r. So for $h \in H$ and $x \in X_r$ we denote hxh^{-1} by $h \cdot x$.

We shall give a uniform parameter interpretation of K in $\mathbb{L}(K)$ in the case where X_r is the union of two H-orbits. In most cases there is, in fact, only one orbit; we exhibit the harder case. In such a case we must have $[K^\times : (K^\times)^2] = 2$, since for any root r and $\zeta, a \in K^\times$ we have $h_r(\zeta) \cdot x_r(a) = x_r(a\zeta^2)$. So pick $\xi \in \mathcal{K}^\times$ with ξ a non-square. We let $X_r^\times = X_r \backslash \{0\}$ and split $X_r^\times$ into two uniformly parameter definable subsets: $H \cdot x_r(1)$ and $H \cdot x_r(\xi)$. We now give a uniform parameter definition for a multiplication $\otimes$ on $X_r^\times$. The parameters used are $x_r(\xi)$, $x_r(\xi^2)$ and $x_r(1)$.

- If $x_r(a), x_r(b) \in H \cdot x_r(1)$ then let h_a be such that $h_a \cdot x_r(1) = x_r(a)$ and let h_b be such that $h_b \cdot x_r(1) = x_r(b)$. We define $x_r(a) \otimes x_r(b) = h_a h_b \cdot x_r(1)$.
- If $x_r(a) \in H \cdot x_r(1),\ x_r(b) \in H \cdot x_r(\xi)$, then let h_a be such that $h_a \cdot x_r(1) = x_r(a)$ and let h_b be such that $h_b \cdot x_r(\xi) = x_r(b)$. We define $x_r(a) \otimes x_r(b) = h_a h_b \cdot x_r(\xi)$.
- If $x_r(a) \in H \cdot x_r(\xi),\ x_r(b) \in H \cdot x_r(\xi)$, then let h_a be such that $h_a \cdot x_r(\xi) = x_r(a)$, let h_b be such that $h_b \cdot x_r(\xi) = x_r(b)$ and let h_c be such that $h_c \cdot x_r(1) = x_r(\xi^2)$. We define $x_r(a) \otimes x_r(b) = h_a h_b h_c \cdot x_r(1)$.

The reader will verify that this gives a well-defined, commutative multiplication on $X_r^\times$. The UPD field structure on X_r is given by (i) X_r is the underlying set, (ii) field addition is the $\mathbb{L}(K)$ group operation, (iii) field multiplication is $\otimes$ defined above, (iv) the additive identity is the identity of $\mathbb{L}(K)$, and (v) the multiplicative identity is the

parameter $x_r(1)$.

We now give the UPD isomorphism from K to $(X_r, \cdot, \otimes, \mathrm{id}(\mathbb{L}(K)), x_r(1))$. This will show that our interpreted structure is a field. Using 5.2.1 we see that there is a UPD isomorphism i^+ given by

$$i^+ : \ K \mapsto X_r(K); \ \ \zeta \mapsto \exp(\mathrm{ad}\ \zeta e_r) \ \ (\zeta \in K)$$

We claim that the map i^+ is a uniform definable isomorphism of fields. Certainly it is an additive isomorphism. It is a routine check that $i^+|_{K^\times}$ is a multiplicative homomorphism. (To get the flavour, in the harder cases of twisted simple groups we explicitly write the verifications; this is done at the end of subsection 5.3.4.)

5.2.5 Conclusion of proof of Theorem 5.2.4

REMARK 5.2.9 Suppose we have a class $\mathcal{C}$, and a uniform parameter interpretation inside $\mathcal{C}$ of a class $\mathcal{D}$ cofinite in the class of finite fields, all via formulae $J(x, y)$. Then $J(x, y)$ can be augmented to a set of formulae $J^*(x, y)$ whereby for any $C \in \mathcal{C}$ and $a_y \in P(J^*)(C)$, $J^*(x, a_y)$ interprets a member of $\mathcal{D}$: all that is done is to only accept those a_y whereby the resulting $J^*(x, a_y) \models$ 'Theory of Fields', and the resulting $J^*(x, a_y)$ is not isomorphic to any of the exceptions - those finite fields not in $\mathcal{D}$. Note that this is a result depending only on the finite axiomatisation of the Theory of Fields, and the additional assumption that the set of exceptions is finite.

Our first step is to prove that a uniform parameter bi-interpretation exists between $\mathcal{C}_{\mathbb{L},n}$ and the class of finite fields. We aim to apply Lemma 4.3.12. But the results of sections 5.2.4 and 5.2.3 put us exactly in a position to apply that lemma.

Next, we aim to apply Lemma 4.2.11 to show that, in fact, we have a strong uniform parameter bi-interpretation. We work with the notation of that lemma. Then, of the requirements to apply the lemma, we have shown the existence of the uniform parameter bi-interpretation. Remark 5.2.6 shows that clause 1 of the requirements of Lemma 4.2.11 is satisfied, and 5.2.9 demonstrates that clause 2 is satisfied.

5.3 Twisted simple groups with same length roots

In this section we give strong uniform parameter bi-interpretations for twisted simple groups where the underlying Chevalley group is of type A, D or E_6.

5.3.1 Background

Most technical material will come from [4].

The finite twisted simple groups can be obtained as subgroups in the fixed points of certain automorphisms of Chevalley groups. The automorphism may be taken to be the product of a 'graph automorphism' and a 'field automorphism'. Graph automorphisms are extensions of symmetries of the Dynkin diagram. They are described in great detail in sections 12.2 and 12.3 of [4]. Field automorphisms are described on pp. 200 of [4], and the particular field automorphisms used in the construction of the various twisted simple groups are explicitly defined on pp. 225. For a Chevalley group $G = \mathbb{L}(K)$ a 'field automorphism' of G derives from a field automorphism of K.

NOTATION 5.3.1 In the sequel we mention many results that apply generally to the families of groups, fields and difference fields that we define. We refer to a typical family in Theorem 5.3.3 as a class $\mathcal{T}$, and if $\mathbb{L}$ is a Lie algebra, and K a field, we refer to the twist of $\mathbb{L}(K)$ via a graph automorphism of order i as ${}^i\mathbb{L}(K)$. Here $i = 2$ except for the case ${}^3D_4(K)$. We refer to a typical member of $\mathcal{T}$ as G^1 or $G^1(K)$. A typical overlying Chevalley group $\mathbb{L}(K)$ will be referred to as G. We will assume that G is given by its adjoint representation on a Lie algebra $\mathbb{L}$ of Lie rank n, and that we are given a Chevalley basis, a root system Φ, a root ordering $\prec$, a fundamental system Π, a unipotent subgroup U, its opposite V, a maximal torus H, etc. We will refer to the automorphism of G from which G^1 is defined as σ. The field of definition of the overlying Chevalley group is referred to as K and the fixed field of the defining automorphism is referred to as K_0. So K is a degree 2 or 3 extension of K_0. The automorphism σ is constructed using two automorphisms f and g where f is a field automorphism and g is a graph automorphism. As said, the graph automorphism g arises from a symmetry of the Dynkin diagram which extends to a map $\tilde{g}$ from Φ to itself. The notation typically used is $f(t) = \bar{t}$ $(t \in K)$, and $\tilde{g}(r) = \bar{r}$ $(r \in \Phi)$.

We now present some facts about twisted simple groups of Lie type:

DISCUSSION 5.3.2 1. A twisted simple group of Lie type begins with a symmetry ρ of the Dynkin diagram associated to its overlying Chevalley group. Proposition 12.2.3 of [4] illustrates how the symmetry ρ extends to a permutation $^-$: $\Phi \mapsto \Phi$, and how this permutation defines an automorphism of the overlying Chevalley group: to summarise, there exist numbers $\gamma_r = \pm 1$ such that the map $x_r(t) \mapsto x_{\bar{r}}(\gamma_r t)$ can be extended to an automorphism of G. The graph automorphism is described in more detail below.

The second principal ingredient in the construction of the twisted Chevalley group is a group 'field automorphism'. These automorphisms are defined in section 12.2 of [4]. To summarise, if $G = G(K)$ and f is an automorphism of K, then the map $x_r(t) \mapsto x_r(f(t))$, $r \in \Phi$, $t \in K$, extends to an automorphism of G, and such an automorphism is called a field automorphism of G.

The automorphism σ used to define G^1 can be taken to be a product of a field and graph automorphism of G.

2. For twisted groups, there are important counterparts to the subgroups V, U, H and N; we transcribe Definition 13.4.2 of [4]:

   (a) U^1 is the set of elements $x \in U$ such that $\sigma(x) = x$.

   (b) V^1 is the set of elements $x \in V$ such that $\sigma(x) = x$.

   (c) G^1 is the group generated by U^1 and V^1.

   (d) H^1 is the intersection of G^1 and H.

   (e) N^1 is the intersection of G^1 and N.

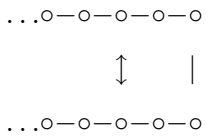
3. An isometry τ of the Lie algebra based upon the Dynkin diagram symmetry may be defined. For any $r \in \Pi$, $\tau(r)$ is a positive multiple of $\bar{r}$, and it transpires that τ acts by conjugation on W. Thus the twisted Weyl subgroup $W^1 \leq W$ may be defined by $W^1 = \{w \in W : \ \tau w = w\tau\}$.

In addition, Proposition 12.2.2 of [4] tells us that in the case that all roots of $\mathbb{L}$ have the same length, then τ coincides with the Dynkin diagram symmetry, $\tau(\Phi) = \Phi$ and τ is an isometry with respect to the Killing form. In this case, the graph automorphism $^-$ described above is τ.

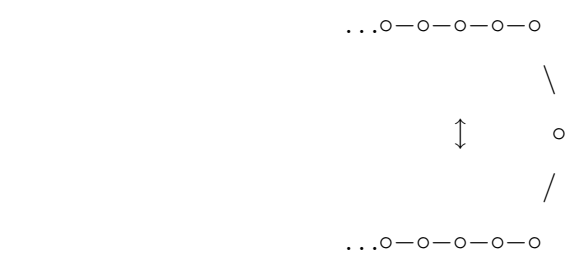
4. In section 2.5 of [4] parabolic subgroups are described: let J be a subset of Π. In brief, define V_J to be the subspace spanned by the roots J, $\Phi_J =_{\text{def}} \Phi \cap V_J$, and W_J to be the subgroup of W generated by the fundamental reflections w_r with $r \in J$. Then it transpires that Φ_J is a system of roots in V_J, J is a fundamental system in Φ_J, and the Weyl group of Φ_J is W_J. The subgroups W_J and their conjugates in W are called parabolic subgroups of W.

   The Dynkin diagram symmetry also induces an equivalence relation on Φ. The equivalence classes are the sets $w(\Phi_J^+)$ as w runs through the twisted Weyl group W^1 and J runs through the orbits of Π under the graph symmetry. For $r \in \Phi$ we refer to the equivalence class of r as $S(r)$. For S an equivalence class, we define $X_S = \prod_{r \in S} X_r$, and X_S^1 to be the σ-fixed points of X_S.

   We will consider groups of type A as an example. Inspection of the Dynkin diagram shows that in type A, S may take three forms. For now, $n = 2m$ or $n = 2m + 1$. Here is the Dynkin diagram of type A_{2m}:



   The Dynkin diagram symmetry is indicated by the arrow. It is clear that in this case all the S are of type $A_1 \times A_1$, except for the swap on the right, where $S = A_2$. Here is the Dynkin diagram of type A_{2m+1}:



Here all equivalence classes S are of type $A_1 \times A_1$, except for the fixed node on the right where S is of type A_1.

The types of equivalence classes just described represent the types of all the equivalence classes found in twisted simple groups of Lie type with all roots of the same length.

Lemmas 13.6.3 and 13.6.4 of [4] give specific information about the form of X_S^1 elements and their multiplication:

If S has type A_1 then X_S^1 consists of elements $x_r(t)$ with $t = \bar{t}$. Elements multiply in an obvious way in this case. We will not concern ourselves with type $A_1 \times A_1$.

If S has type A_2 then X_S^1 consists of elements $x_r(t)x_{\bar{r}}(\bar{t})x_{r+\bar{r}}(u)$ where $u + \bar{u} = -N_{r,\bar{r}}t\bar{t}$. Here $N_{r,\bar{r}}$ is a structure coefficient. We may write an element $x_r(t)x_{\bar{r}}(\bar{t})x_{r+\bar{r}}(u)$ unambiguously as $x_S(t,u)$. The multiplication is then $x_S(t_1,u_1)x_S(t_2,u_2) = x_S(t_1+t_2, u_1+u_2-N_{r,\bar{r}}\bar{t_1}t_2)$.

5. The next important fact is Proposition 13.6.1 of [4]: $U^1 = \prod_{S\subseteq\Phi^+} X_S^1$, where the product may be taken in any order.

6. We investigate $H^1 = H \cap G^1$. Theorem 13.7.2 and Theorem 7.1.1 of [4] give the relevant information: suppose that $P = \mathbb{Z}[\Phi]$ has free basis $\Pi = \{p_1, p_2, \ldots, p_n\}$. We work with the Killing form $(\ ,\ )$ on the root system of $\mathbb{L}$. We have seen in 5.2.2 (4) how H may naturally be considered as a set of K-characters on P. Further information is found in Section 7.1 of [4]; we now outline some important

theory found there:

Because we are working with the Killing form on the Euclidean space generated by the roots Φ, we may consider dual bases in the same space. Let $\{q_1, \ldots, q_l\}$ be the dual basis to the basis $\{h_{p_i} = \frac{2p_i}{(p_i,p_i)} : 1 \leq i \leq n\}$. Specifically, we mean that $q_1, \ldots, q_n$ are defined by:

$$(h_{p_i}, q_j) = \left\{ \begin{array}{ll} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{array} \right\}$$

Let $Q = \mathbb{Z}[\{q_i : 1 \leq i \leq n\}]$. The lattice P is a sublattice of Q. The characters on P induced by H are the restrictions of the free group of K-characters on Q (Theorem 7.1.1 of [4]). We will denote the free basis of Q consisting of the q_i as Ω. The q_j are called the fundamental weights of $\mathbb{L}$. We know that each p_i is a linear combination of the q_j:

$$p_i = \sum_{j=1}^{l} \mu_{ij} q_j$$

The coefficients μ_{ij} are easy to compute, since using the Killing form we see $(h_{p_j}, p_i) = \mu_{ij}$. So $\mu_{ij} = 2\frac{(p_j,p_i)}{(p_j,p_j)} = A_{ji}$, where the quantity A_{ji} is the ji'th entry of the Cartan matrix for $\mathbb{L}$. For the specific cases we will be interested in, the Cartan matrix is known explicitly and can be easily referenced. A good place to start with this material is [4] 7.1.

It transpires that if we define the K-character on Q: $\chi_{r,\lambda}(a) = \lambda^{2(r,a)/(r,r)}$ for some $r \in \Omega, a \in Q, \lambda \in K$, these characters generate H (also 7.1.1). Theorem 13.7.2 gives a characterisation of the elements in H^1: they are the elements of H which induce characters of P that are the restrictions to P of the self-conjugate characters of Q. In short, H^1 is the set of H-elements χ with $\chi(\bar{a}) = \overline{\chi(a)}$ for $a \in Q$.

So let $J(r)$ be the orbit of r under g. Let $\Pi_1 = \{J(r) \subseteq \Pi : g-\text{orbit of } r \text{ is size } 1\}$, $\Pi_2 = \{J(r) \subseteq \Pi : g - \text{orbit of } r \text{ is size } 2\}$, and $\Pi_3 = \{J(r) \subseteq \Pi : g - \text{orbit of } r \text{ is size } 3\}$. We include all sizes of orbit so the result we quote is valid

for all twisted groups with roots all of the same length. For $J(r) \in \Pi_1$ we consider characters $\chi_{1,r,\lambda} = \chi_{r,\lambda}$ where $\lambda = \bar{\lambda}$. For $J(r) \in \Pi_2$ we consider characters of the form $\chi_{2,r,\lambda} = \chi_{r,\lambda} \cdot \chi_{\bar{r},\bar{\lambda}}$. For $J(r) \in \Pi_3$ we consider characters of the form $\chi_{3,r,\lambda} = \chi_{r,\lambda} \cdot \chi_{\bar{r},\bar{\lambda}} \cdot \chi_{\bar{\bar{r}},\bar{\bar{\lambda}}}$. Thus an element $h \in H^1$ is one which induces a character of the form $\prod_{J(r)\in\Pi_1} \chi_{1,r,\lambda_r} \cdot \prod_{J(r)\in\Pi_2} \chi_{2,r,\lambda_r} \cdot \prod_{J(r)\in\Pi_3} \chi_{3,r,\lambda_r}$. Conversely, suppose that $h \in H$, and h induces a character χ on P. By Theorem 7.1.1 of [4] we may assume that χ is a character on Q. We have seen above that in the case of roots all of the same length, τ is an isometry which restricts to a permutation of Ω. So we may define a character χ' on Q such that for all $q \in \Omega$, then $\chi'(q) = \overline{\chi(\bar{q})}$, and if τ has order three we may define a character χ'' on Q such that for all $q \in \Omega$, then $\chi''(q) = \overline{\overline{\chi(\bar{\bar{q}})}}$. Then we may find $h' \in H$ such that h' induces the character which is the restriction of $\chi \cdot \chi'$, or $\chi \cdot \chi' \cdot \chi''$ in the order 3 case. Notice that $h' \in H^1$. Thus every character on P of the form $\prod_{J(r)\in\Pi_1} \chi_{1,r,\lambda_r} \cdot \prod_{J(r)\in\Pi_2} \chi_{2,r,\lambda_r} \cdot \prod_{J(r)\in\Pi_3} \chi_{3,r,\lambda_r}$ is induced by some $h \in H^1$.

7. Proposition 13.5.3 of [4] gives a unique Bruhat decomposition for twisted simple groups of Lie type: we transcribe it. 'Each element of G^1 has a unique expression $g = u'hn_w u$, where $u' = U^1,\ h \in H^1,\ w \in W^1,\ n_w \in N^1$ *and* $u \in (U_w^-)^1$ the set of σ-invariant elements of U_w^-. '

5.3.2 Statement of theorem

The only twisted group with roots all the same length that is not simple is ${}^2A_2(4)$ ([4] 14.4.1). It is excluded from the following discussion. Again, in all the bi-interpretations constructed in the sequel, we exclude groups derived from the exceptional, non-simple Chevalley groups listed at the beginning of the Chevalley groups section. We also assume $|K| > 3$. With these provisos the theorem we prove is

THEOREM 5.3.3 *(a) Fix $n \in \mathbb{N}$ with $n \geq 2$. Let $\mathcal{T}_{A,n} = \{{}^2A_l(q^2) :$ q a prime power$\}$. There is a strong uniform parameter bi-interpretation between $\mathcal{T}_{A,n}$ and the class of finite fields. The strong uniform parameter bi-interpretation matches the group ${}^2A_n(q^2)$ with $\mathbb{F}_q$.*

(b) Fix $n \in \mathbb{N}$ with $n \geq 3$. Let $\mathcal{T}_{D,n} = \{{}^2D_n(q^2) :$ q a prime power$\}$. There is a strong

uniform parameter bi-interpretation between $\mathcal{T}_{D,n}$ and the class of finite fields. The strong uniform parameter bi-interpretation matches the group ${}^2D_n(q^2)$ with $\mathbb{F}_q$.

(c) Let $\mathcal{T}_{E,6} = \{{}^2E_6(q^2) :$ q a prime power$\}$. There is a strong uniform parameter bi-interpretation between $\mathcal{T}_{E,6}$ and the class of finite fields. The strong uniform parameter bi-interpretation matches the group ${}^2E_6(q^2)$ with $\mathbb{F}_q$.

(d) Let $\mathcal{T}_{D,4,3} = \{{}^3D_4(q^3) :$ q a prime power$\}$. There is a strong uniform parameter bi-interpretation between $\mathcal{T}_{D,4}$ and the class of finite fields. The strong uniform parameter bi-interpretation matches the group ${}^3D_4(q^3)$ with $\mathbb{F}_q$.

REMARK 5.3.4 [10] arose in answer to the question 'Is there a formula $\varphi(Y)$ in the language of rings that defines in each finite field of the form $\mathbb{F}_{q^2}$ its subfield $\mathbb{F}_q$?': the answer is no. It follows from this and Theorem 5.3.3 that there is no uniform parameter bi-interpretation matching ${}^2A_n(q^2)$ with the pure field of q^2 elements. If there were, we could compose uniform parameter bi-interpretations: since ${}^2A_n(q^2)$ would be uniformly parameter bi-interpretable with both the pure field of q^2 elements and the pure field of q elements, it would follow that the pure field of q^2 elements would uniformly interpret the pure field of q elements. Similarly, by the results in the section on Chevalley groups, there is no uniform parameter bi-interpretation matching $\mathcal{T}_{A,n}$ and the class $\mathcal{C}_{A,n}$ which matches ${}^2A_n(q^2)$ with $A_n(q^2)$. Similar results apply to the other twisted families in Theorem 5.3.3.

We now use Lemma 4.3.12 to prove the second part of the theorem. In the following sections we break the task into three parts:

1. In 5.3.3 we give the uniform interpetation of the group ${}^i\mathbb{L}(K)$ in the field K_0.
2. In 5.3.4 we give the uniform interpretation of the field K_0 in the group ${}^i\mathbb{L}(K)$.
3. In 5.3.4 we also give the uniform isomorphism between K_0 and its re-interpretation inside itself.
4. In 5.3.5 we apply Lemmas 4.2.11 and 4.3.12 to conclude the theorem.

   Here K_0 refers to the subfield of K specified in Theorem 5.3.3.

5.3.3 Twisted groups with roots of the same length: Uniform interpretation of $G^1 \in \mathcal{T}$ in $\mathbb{F}_q$

We begin by making some general statements using what we already know:

In all the cases of Theorem 5.3.3 except for $\mathcal{T}_{D,4,3}$, the twisted groups are built out of a Chevalley group defined over the field $\mathbb{F}_{q^2}$. In the case of $\mathcal{T}_{D,4,3}$, the twisted group is built out of a Chevalley group defined over $\mathbb{F}_{q^3}$. Thus, we first strongly, uniformly parameter define $\mathbb{F}_{q^2}$ inside $\mathbb{F}_q$ in (a),(b),and (c) of 5.3.3, and we strongly uniformly define $\mathbb{F}_{q^3}$ inside $\mathbb{F}_q$ in case (d). These interpretations come complete with a strongly uniformly parameter definable embedding of $\mathbb{F}_q$ inside $\mathbb{F}_{q^i}$ (i=2 or 3 depending on the case). This is a classical result; one reference is [6] pp. 31.

Second, we give UPD definitions of the overlying Chevalley groups using our UPD field extensions: in 5.3.3 (a) we strongly uniformly parameter define the groups $A_n(q^2)$ using our UPD of $\mathbb{F}_{q^2}$; in (b) we uniformly parameter define the groups $D_n(q^2)$; in (c) we strongly uniformly parameter define the groups $E_6(q^2)$ using our UPD of $\mathbb{F}_{q^2}$; and finally in (d) we strongly uniformly parameter define the groups $D_4(q^3)$ using our UPD of $\mathbb{F}_{q^3}$. This makes use of the work in Section 5.2.

The next step is to interpret the automorphism σ used to define the twisted groups. Proposition 12.2.3 of [4] characterises the graph automorphism for all groups built on Lie algebras where roots all have the same length. From 12.2.3 and the Bruhat decomposition (or even just compactness), these graph automorphisms are UPD inside the class of finite fields. Since the graph symmetry in cases (a), (b) and (c) of 5.3.3 ([4] pp. 200) is of order 2, the field automorphism required to define σ is of order 2 as well (see pp. 225 of [4]); for case (d) the field automorphism is of order 3. Since we have interpreted $\mathbb{F}_{q^i}$ (i= 2 or 3 depending on the case) inside $\mathbb{F}_q$ these field automorphisms are easy to define. Then by the definition of the group field automorphism (pp.200) and the Bruhat decomposition (or again, even just compactness), the field automorphism is clearly uniformly definable. The reader can see additional details about the group field automorphism in 5.3.2 (1).

We have shown in Section 5.2 that the the root subgroups of a Chevalley group are UPD in fields. Thus, by the Chevalley cell presentation of the unipotent group U and its opposite V (see 5.2.2 (3)), U and V are both UPD. Thus, so are the subgroups $U^1 = \{u \in U : \sigma(u) = u\}$ and $V^1 = \{v \in V : \sigma(v) = v\}$. By definition, $G^1 = \langle U^1, V^1 \rangle$. In order to show that G^1 is UPD, what is needed is that for any member G^1 of $\mathcal{T}$, U^1 and V^1 generate G^1 in an absolutely bounded number of steps. We prove this:

LEMMA 5.3.5 *There is $n \in \mathbb{N}$ and a function $\varphi : \{1, 2, \ldots, n\} \mapsto \{U^1, V^1\}$ such that for any $G^1 \in \mathcal{T}$ we have*

$$G^1 = \prod_{i=1}^{n} \varphi(i)(K)$$

PROOF Suppose this were not so. Let $\mathcal{T}$ be a counterexample. Then define $i = 2$ if $\mathcal{T}$ is from case (a,b,c) and define $i = 3$ if $\mathcal{T}$ is from case (d) of 5.3.3. Then there is a sequence of twisted groups indexed by $j \in \mathbb{N}$: $(G^1(\mathbb{F}_{q_j^i}) \in \mathcal{T} : q_j$ a prime power) such that the minimum number of steps for $V^1(\mathbb{F}_{q_j^i})$ and $U^1(\mathbb{F}_{q_j^i})$ to generate $G^1(\mathbb{F}_{q_j^i})$ is greater than j.

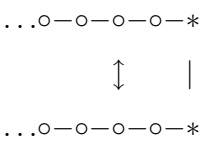
Let K be a non-principal ultraproduct of the $\mathbb{F}_{q_j}$. Then K is a pseudo-finite field. Further, we may apply $\mathcal{L}$os' theorem to all the objects we have shown to be UPD in the $\mathbb{F}_{q_j}$: the ultraproduct of the interpreted $\mathbb{F}_{q_j^i}$ is a degree i extension of K; call it K_i. The ultraproduct of the σ_j is a definable automorphism σ which is a product of a definable graph automorphism and a definable field automorphism of K_i. Thus, the ultraproduct of the $V^1(\mathbb{F}_{q_j^i})$ is $V^1(K_i)$ and the ultraproduct of the $U^1(\mathbb{F}_{q_j^i})$ is $U^1(K_i)$. By [4] Theorem 14.4.1, $G^1(K_i) = \langle U^1(K_i), V^1(K_i) \rangle$ is a simple group. We now work inside $G^1(K_i)$. We denote it G^1, and refer to U^1, V^1, etc.

So, by our construction, U^1 and V^1 do not generate G^1 in finitely many steps. However, at the ultraproduct level, all the objects we have defined have been defined in a pure pseudo-finite field. So we may apply Proposition 4.3.9: it shows that there is a definable group $H \subseteq (U^1V^1)^n$ for some $n \in \mathbb{N}$ such that $H \lhd \langle U^1, V^1 \rangle$ and H/U^1 and H/V^1 are finite. Since $G^1 = \langle U^1, V^1 \rangle$ and since G^1 is simple, it follows that $H = G^1$. So we have a contradiction. $\square$

5.3.4 Twisted groups with roots of the same length: Uniform interpretation of $\mathbb{F}_q$ in $G^1(\mathbb{F}_{q^i})$, ($i = 2$ or 3), and the uniform isomorphism from a field of definition to its re-interpretation)

DISCUSSION 5.3.6 We intend to interpret the field inside twisted root subgroups X_S^1 (see Discussion 5.3.2 (4)). We now run through the cases and declare our intentions specifically. We shall set $n = 2m$ or $n = 2m + 1$.

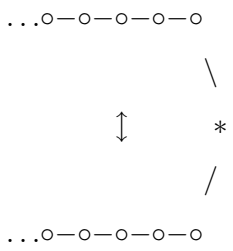
In a class of groups of the form A_{2m} with Dynkin diagram



we intend to interpret the field on X_S^1 where S is the type A_2 equivalence class generated by the starred pair of roots. This is the only time we interpret on an A_2-type equivalence class S. If the class of groups is ${}^2A_{2m}$ with $m \geq 2$ then order the roots in the diagram top left to bottom left, so the starred roots are p_m and p_{m+1}. Inspection of the Cartan matrix shows that $p_m = -q_{m-1} + 2q_m - q_{m+1}$ and $p_{m+1} = -q_m + 2q_{m+1} - q_{m+2}$, where the q_i are in the dual basis as defined in Discussion 5.3.2 (6), as is the use of the Cartan matrix to make these computations . Since, in the case of roots all being of equal length, the graph automorphism is both an isometry with respect to the Killing form and restricts to a permutation of Π, and since we can see that $p_{m+i} = \overline{p_{m-i+1}}$, it follows that $q_{m+i} = \overline{q_{m-i+1}}$; the details about τ being an isometry are found in 5.3.2 (3). In the case where $m = 1$, then $p_1 = 2q_1 - q_2$ and $p_2 = -q_1 + 2q_2$.

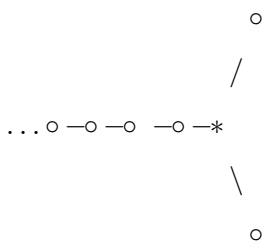
In all other cases we interpret the field on X_S^1 where S is an equivalence clas of type A_1. Here are diagrams indicating our choices.

Here is the Dynkin diagram of A_{2m+1} with $m \geq 1$:



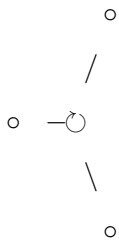
Here we interpret the field on X_S^1, where $S = p_{m+1}$ and $p_{m+1} = -q_m + 2q_{m+1} - q_{m+2}$. Again, $q_{m+1} = \overline{q_{m+1}}$ and $q_{m+2} = \overline{q_m}$. These equations follow from inspection of the Cartan matrix and the fact that the graph automorphism $^-$is an isometry (see 5.3.2 (3) for the isometry facts, and 5.3.2 (6) for the use of the Cartan matrix). The case $m = 0$ is irrelevant, since ${}^2A_1(\mathbb{F}_q) \cong A_1(\mathbb{F}_q)$.

In the case of ${}^2D_m$ with $m \geq 3$, the Dynkin diagram is:



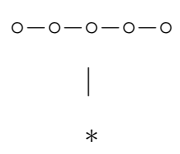
Again we label from left to right, then top, bottom. So we interpret on the A_1 equivalence class generated by the root p_{m-2}. We have $p_{m-2} = -q_{m-3} + 2q_{m-2} - q_{m-1} - q_m$, and $q_{m-3} = \overline{q_{m-3}}$, $q_{m-2} = \overline{q_{m-2}}$, and $q_m = \overline{q_{m-1}}$. The isomorphism ${}^2D_2(q^2) \cong A_1(\mathbb{F}_{q^2})$ means we may omit the case $m = 3$.

In the case of ${}^3D_4$ the diagram is:



Here we shall interpret the field on X_S^1 where S is the class of the node labelled by a clockwise rotation; this is the node fixed by the symmetry (the clockwise rotation is to indicate the symmetry). In this case we have $p_2 = -q_1 + 2q_2 - q_3 - q_4$ where $q_3 = \bar{q_1}$, $q_4 = \bar{q_3}$, and $q_1 = \bar{q_4}$.

The final case is groups of type ${}^2E_6$. The Dynkin diagram is:



So here $p_4 = -q_3 + 2q_4$, $q_3 = \bar{q_3}$ and $q_4 = \bar{q_4}$.

To construct the interpretations we shall need that H^1 is UPD in $\mathcal{T}$. The first step is the following:

LEMMA 5.3.7 *There is $f \in \mathbb{N}$ such that if $|K| \geq f$, for each $r \in \Phi$ there is $h \in H^1$ such that the character χ induced by h satisfies $\chi(r) \neq 1$.*

PROOF Fix $r \in \Phi^+$. From 5.3.2 (6) we may write $r = \sum_{j=1}^{n} a_j q_{i_j}$ with $a_j \in \mathbb{N}$ and $q_{i_j} \in \Omega$. This sum depends only on the Lie type and rank of $\mathbb{L}$, and not on the field K.

If there is a $q = q_{i_j}$ in the sum such that $\bar{q} = q$ then select $\lambda \in K^\times \backslash 1$ such that $\lambda = \bar{\lambda}$. In 5.3.2 (6) we saw that there is an $h \in H^1$ such that h induces the character χ, where $\chi(q) = \lambda$ and $\chi(q') = 1$ for all $q' \in \Omega \backslash \{q\}$. Such an h is sufficient for the lemma.

Otherwise, there is $q = q_{i_j}$ such that $q \neq \bar{q}$. Pick $\lambda \in K^\times$ and notice that by Discussion 5.3.2 (6) there is an $h \in H^1$ such that h induces the character χ where

- if we are in case (a), (b) or (c) of Theorem 5.3.3 then $\chi(q) = \lambda$, $\chi(\bar{q}) = \bar{\lambda}$ and $\chi(q') = 1$ for all $q' \in \Omega \backslash \{q, \bar{q}\}$.

- if we are in case (d) of Theorem 5.3.3 then $\chi(q) = \lambda$, $\chi(\bar{q}) = \bar{\lambda}$, $\chi(\bar{\bar{q}}) = \bar{\bar{\lambda}}$ and $\chi(q') = 1$ for all $q' \in \Omega \backslash \{q, \bar{q}, \bar{\bar{q}}\}$.

In the first case, there are integers fixed integers a and b, independent of K, such that $\chi(r) = \lambda^a \bar{\lambda}^b$. In the second case, there are fixed integers a, b and c, independent of K, such that $\chi(r) = \lambda^a \bar{\lambda}^b \bar{\bar{\lambda}}^c$. Thus, since the field automorphisms for groups with roots all the same size are of order 2 or 3, the automorphism is $\lambda \mapsto \lambda^{|K|^{\frac{1}{i}}}$ with $i = 2$ or 3 depending on which case. But then examine the equations $1 = \lambda^{a+b\cdot|K|^{\frac{1}{2}}}$ and $1 = \lambda^{a+b\cdot|K|^{\frac{1}{3}}+c\cdot|K|^{\frac{2}{3}}}$. For the first , if $|K| > a + b \cdot |K|^{\frac{1}{2}}$, then not all $\lambda \in K^\times$ are roots of this equation. For the second, if $|K| > a + b \cdot |K|^{\frac{1}{3}} + c \cdot |K|^{\frac{2}{3}}$, then not all $\lambda \in K^\times$ are roots of this equation. Pick χ corresponding to a $\lambda \in K^\times$ that is not a root of the relevant equation. Pick $h \in H^1$ that induces χ, and this is the h we sought. $\square$

LEMMA 5.3.8 *There is $m, f \in \mathbb{N}$, such that for $|K| > f$, the subgroup H^1 is uniformly parameter definable in any of the families of Theorem 5.3.3 as the intersection $\cap_{i=1}^{m} C_{G^1}(h_i)$ of some m of its elements.*

PROOF We offer a proof similar to the one in Lemma 5.2.7. Let $g \in G^1$. By the unique Bruhat decomposition for twisted groups (5.3.2 (6)), we may write g uniquely as $g = u' h_0 n_w u$ for some $u' \in U^1$, $h_0 \in H^1$, $n_w \in N^1$, and $u \in (U_w^-)^1$. Then let $h \in H^1$. So $hgh^{-1} = hu'h^{-1} h_0 h n_w h^{-1} huh^{-1}$. It is easily verified using 5.3.2 (2) that $hu'h^{-1} \in U^1$ and $hn_wh^{-1} \in N^1$. Since h preserves all root subgroups X_r under conjugation, it follows that $hU_w^-h^{-1} = U_w^-$, and so $huh^{-1} \in (U_w^-)^1$. Thus, if $g = hgh^{-1}$, then $u' = hu'h^{-1}$, $n_w = hn_wh^{-1}$ and $u = huh^{-1}$. By Lemma 5.3.7, for all sufficiently large $|K|$ we may select parameters $h_r \in H^1$ for each $r \in \Phi^+$, such that, as in Lemma 5.2.7, the character induced by h_r satisfies $\chi(r) \neq 1$. Now suppose $g \in \cap_{r\in\Phi^+} C_{G^1}(h_r)$. Then $u' = h_r u' h_r^{-1}$ so u' cannot have a non-trivial r-component in its Chevalley expression (see 5.2.2 (3)). It follows that $u' = 1$, and by the same logic, $u = 1$. Thus, $\cap_{r\in\Phi^+} C_{G^1}(h_r) \leq N^1$.

Now let $n^1 \in N^1 \backslash H^1$, and suppose n^1 maps to $w^1 \in W^1$ in the natural homomorphism. Let $s \in \Phi$ be such that $w^1(s) \neq s$. There are three cases:

1. Suppose s lies in a τ-orbit of size 1. Then we consider elements of H^1 of the form

$h_s(l)$ such that $l = \bar{l}$. By 5.2.2 (6) we have $nh_s(l)n^{-1} = h_{w^1(s)}(l)$. In this case, as in Lemma 5.2.7, for $|K_0| > 7$ we may find $l^* \in K_0^\times$ such that $h_s(l^*)$ does not commute with n.

2. Suppose s lies in a τ-orbit of size 2. Then we consider elements of H^1 of the form $h_s(l)h_{\bar{s}}(\bar{l})$. By 5.2.2 (6) and the fact that τ commutes with w^1 ([4] pp.217) we have $nh_s(l)h_{\bar{s}}(\bar{l})n^{-1} = h_{w^1(s)}(l)h_{\overline{w^1(s)}}(\bar{l})$. At the level of characters $h_s(l)$ induces the character χ where $\chi(r) = l^{2\frac{(s,r)}{(s,s)}}$, $h_{w^1(s)}(l)$ induces the character χ' where $\chi'(r) = l^{2\frac{(w^1(s),r)}{(w^1(s),w^1(s))}}$, $h_{\bar{s}}(\bar{l})$ induces the character $\bar{\chi}$ where $\bar{\chi}(r) = \bar{l}^{2\frac{(\bar{s},r)}{(\bar{s},\bar{s})}}$ and finally $h_{\overline{w^1(s)}}(\bar{l})$ induces the character $\bar{\chi}'$ where $\bar{\chi}'(r) = \bar{l}^{2\frac{(\overline{w^1(s)},r)}{(w^1(s),\overline{w^1(s)})}}$. Now for n to commute with $h_s(l)h_{\bar{s}}(\bar{l})$ we must have $\chi\bar{\chi} = \chi'\bar{\chi}'$. Now let $\Gamma = |K_0|$, and let l^* be a generator for the cyclic group $K^\times$. Recall that for all $r, s \in \Phi$ we have $|2\frac{(r,s)}{(r,r)}| \leq 3$. Now fix $r \in \Phi$. Let $a = 2\frac{(s,r)}{(s,s)}$, $b = 2\frac{(\bar{s},r)}{(\bar{s},\bar{s})}$, $c = 2\frac{(w^1(s),r)}{(w^1(s),w^1(s))}$ and $d = 2\frac{(\overline{w^1(s)},r)}{(w^1(s),\overline{w^1(s)})}$. Then $-3 \leq a, b, c, d \leq 3$. If $\chi\bar{\chi} = \chi'\bar{\chi}'$, then $(l^*)^{a+\Gamma b} = (l^*)^{c+\Gamma d}$. So we must satisfy

$$(*) \quad (l^*)^{(a-c)+\Gamma(b-d)} = 1$$

Then $|K| \mid ((a-c)+\Gamma(b-d))$. Since $|b-d| < 7$, for $\Gamma > 7$ it is clear that for (*) to be satisfied then $b = d$ and $a = c$. But this was for an arbitrary $r \in \Phi$. So it follows that for all $r \in \Phi$, $2\frac{(s,r)}{(s,s)} = 2\frac{(w^1(s),r)}{(w^1(s),w^1(s))}$. The argument is now similar to 5.2.7: since w^1 is an isometry, it follows that $(s,r) = (w^1(s),r)$ for all $r \in \Phi$. So $s = w^1(s)$, and we have a contradiction.

3. Suppose s lies in a τ-orbit of size 3. We proceed exactly as in the previous case, except this time relative to the H-element $h_s(l)h_{\bar{s}}(\bar{l})h_{\bar{\bar{s}}}(\bar{\bar{l}^*})$. Again, for $|K_0| > 7$ we may equate terms of characters, as in the previous case of this lemma, and the proof is of the same form.

Thus, for each $w^1 \in W^1$, we may find $h_{w^1} \in H^1$ such that h_{w^1} does not commute with any element of the coset n^1H^1 in N^1. It now follows that $H^1 = (\cap_{r\in\Phi^+} C_{G^1}(h_r)) \cap (\cap_{w^1\in W^1} C_{G_1}(h_{w_1}))$. $\square$

REMARK 5.3.9 The cardinalities of the twisted Chevalley groups have been explicitly determined: see Section 14.3 and particularly Theorem 14.3.2 of [4]. Even without this, the fact that the language of groups is finite implies that there are only

finitely many isomorphism classes of Chevalley groups or twisted Chevalley groups of any fixed type and cardinality less than some fixed bound B.

COROLLARY 5.3.10 *H^1 is uniformly definable in any of the families of Theorem 5.3.3.*

PROOF By Lemma 5.3.8, and Remarks 5.2.3 and 5.3.9. □

DEFINITION 5.3.11 *In 5.3.6, we indicated that we would interpret the field on twisted root subgroups X_S^1, for the equivalence class S of a specific choice of root. We call such a root a 'candidate root'.*

LEMMA 5.3.12 *(a) Consider a twisted root subgroup X_S^1 of type A_1 generated by a candidate root r. Then H^1 acts naturally on $X_S^1\backslash\{1\}$ by conjugation, and there are at most two H^1-orbits in X_S^1.*

(b) Consider a twisted root subgroup X_S^1 of type A_2 in a group of type ${}^2A_{2m}$. We assume $S = \{r, \bar{r}, r + \bar{r}\}$ where r is a candidate root. If we write a typical element of X_S^1 as $x_S(t, u)$ (see 5.3.2 (4)) then we may consider the subgroup of X_S^1 of elements where $t = 0$. Call this group Z. Then H^1 acts by conjugation on $Z\backslash\{1\}$ and there is a number $n \in \mathbb{N}$ which bounds the number of H^1-orbits that cover X_S^1, the bound being over all finite simple twisted groups.

PROOF (a) In 5.3.2 (4) we saw that X_S^1 is the collection of σ-fixed points of X_S. Since in this case $X_S = X_r$ and clearly H^1 fixes X_r, it also fixes $X_S^1 = X_r \cap G^1$. To check the number of orbits observe the various expressions in 5.3.6 for r in terms of the dual basis. Each expression included an integral multiple m of an element of the dual basis which is fixed by the graph automorphism, where $1 \leq m \leq 2$. Call that fixed vector q. Now let $\lambda = \bar{\lambda}$ be a fixed element of K. Then the Q-character χ_λ which sends q to λ and all other $q' \in \Omega$ to 1 is a self-conjugate Q-character. So its restriction to P is induced by some $h \in H^1$. But $\chi_\lambda(r) = \lambda^m$. Now recall, from 5.3.2 (4), that $X_S^1 = \{x_r(t) : \ t = \bar{t}\}$, and recall also that $hx_r(t)h^{-1} = x_r(\chi_\lambda(r)t) = x_r(\lambda^m t)$. If $m = 1$, then it is plain then that there is one H^1-orbit in X_S^1. If $m = 2$ then the χ_λ-characters

act as the squares of the fixed field, and there are two H^1-orbits.

(b) Here, we have two cases. If $m = 1$, then by 5.3.2 (6), $r + \bar{r} = q_m + q_{m+1}$, and if $m > 1$ then $r + \bar{r} = -q_{m-1} + q_m + q_{m+1} - q_{m+2}$. The reader can verify that $Z = \{x_{r+\bar{r}}(u) : \ u = -\bar{u}\}$. Now let $h \in H^1$. Then by the character characterisation of elements of H^1 (see 5.3.2 (6)), h induces a character χ on $\mathbb{Z}[\Omega]$ such that, say, $a = \chi(q_{m-1}) = \overline{\chi(q_{m+2})}$ if $m > 1$ and $a = 1$ if $m = 1$, and $b = \chi(q_m) = \overline{\chi(q_{m+1})}$. We have $hx_{r+\bar{r}}(u)h^{-1} = x_{r+\bar{r}}(a\bar{a}b\bar{b}u)$. If $x_{r+\bar{r}}(u) \in Z$ then $u = -\bar{u}$, so $a\bar{a}b\bar{b}u = -\overline{a\bar{a}b\bar{b}u}$. Thus, $hx_{r+\bar{r}}(u)h^{-1} \in Z$, and so H^1 acts on Z by conjugation.

Now suppose we pick $u_0, u_1 \in K^\times$, such that $u_0 = -\bar{u_0}$ and $u_1 = -\bar{u_1}$. Then let $\lambda = \frac{u_1}{u_0}$. We see that $\lambda = \bar{\lambda}$. Let $K_0^- = \{u \in K : \ u = -\bar{u}\}$, and $K_0^{-,\times} = K_0^- \backslash \{0\}$. So any two elements of $K_0^{-,\times}$ have a ratio in the fixed field K_0.

Now let $\lambda \in K_0$. Define χ so that $\chi(q_m) = \lambda$, $\chi(q_{m+1}) = \lambda$, and for all other $q' \in \Omega$, $\chi(q') = 1$. Notice that for all $q \in \Omega$, χ satisfies $\chi(\bar{q}) = \overline{\chi(q)}$. Thus, there is $h \in H^1$ such that $hx_{r+\bar{r}}(t)h^{-1} = x_{r+\bar{r}}(\lambda^2 t)$. Now we can express $K_0^\times$ as at most two cosets of its subgroup $(K_0^\times)^2$. Thus $K_0^{-,\times}$ is at most orbits of $(K_0^\times)^2$ under left multiplication. It follows that Z is covered by at most two orbits of H^1. $\square$

We now give the uniform interpretations of the field. For all cases other than classes $\mathcal{T}_{A,2m}$ we take the underlying set to be X_S^1 as in 5.3.12 (a). For classes $\mathcal{T}_{A,2m}$ we take the underlying set to be Z as in 5.3.12 (b).

We begin by doing all cases other than classes $\mathcal{T}_{A,2m}$. We use the parameter $x_r(1)$. Now pick $u_0, u_1 \in K^\times$ such that $u_0 = \bar{u_0}$ and $u_1 = \bar{u_1}$. By the previous lemma, there are $h_0, h_1 \in H^1$ such that $x_r(u_0) = h_0 x_r(1) h_0^{-1}$, and $x_r(u_1) = h_1 x_r(1) h_1^{-1}$. We define the multiplication:

$$x_r(u_0) \otimes x_r(u_1) = h_1 h_0 x_r(1) h_0^{-1} h_1^{-1}$$

This is well-defined: let h_2 and h_3 be two other H^1 elements playing the role of

h_0 and h_1. Suppose that h_i induces the character χ_i on P. Then $x_r(\chi_0(r)) = h_0 x_r(1) h_0^{-1} = x_r(u_0) = h_2 x_r(1) h_2^{-1} = x_r(\chi_2(r))$ and $x_r(\chi_1(r)) = h_1 x_r(1) h_1^{-1} = x_r(u_1) = h_3 x_r(1) h_3^{-1} = x_r(\chi_3(r))$. Thus $\chi_0(r) = \chi_2(r)$ and $\chi_1(r) = \chi_3(r)$. So $h_3 h_2 x_r(1) h_2^{-1} h_3^{-1} = x_r(\chi_3\chi_2(r)) = x_r(\chi_1\chi_0(r)) = h_1 h_0 x_r(1) h_0^{-1} h_1^{-1}$.

In K_0 we can uniformly define the map $i^+ :\ K \mapsto X_r$ such that $i^+(u) = x_r(u)$. We have remarked that the UPD of K in K_0 comes complete with a UPD embedding of K_0 into K. Call that embedding e. So we may define the UPD composite map

$$i^{tw} :\ K_0 \mapsto X_S^1;\ \ i^{tw} = i^+ \circ e$$

This composite map is the isomorphism between K_0 and its re-interpretation inside G^1.

We now interpret the field for classes $\mathcal{T}_{A,2m}$. Since Z (see Lemma 5.3.12 (b)) is perhaps covered by two copies of H^1, we consider such a case. By considering ratios we again can interpret the field. So let $K_0^- = \{u \in K^\times :\ u = -\bar{u}\}$, let $K_0^{-,\times} = K_0^- \backslash \{1\}$, and fix some $u_0 \in K_0^{-,\times}$. There is an isomorphism of additive groups $B :\ K_0^- \cong K_0$ given by $B(u) = \frac{u}{u_0}$. Notice that $\frac{u_1}{u_0}\frac{u_2}{u_0} = \frac{\frac{u_1 u_2}{u_0}}{u_0}$. We can pull back the multiplication on K_0 using B to define a multiplication $\otimes$ on $K_0^{-,\times}$: $u_1 \otimes u_2 = \frac{u_1 u_2}{u_0}$.

We now turn this multiplication into one on $Z\{1\}$. The two orbits of $Z\{1\}$ under H^1 acting by conjugation are $\vartheta_0 = \{x_{r+\bar{r}}(u) :\ u \in K^\times,\ u = -\bar{u},\ \frac{u}{u_0}$ a square in $K^\times\}$ and $\vartheta_1 = \{x_{r+\bar{r}}(u) :\ u \in K^\times,\ u = -\bar{u},\ \frac{u}{u_0}$ not a square in $K^\times\}$. We select u_1 such that $u_1 = -\bar{u_1}$ and u_1 is not in the H^1-orbit of u_0. Let $u_2 = \frac{u_1^2}{u_0}$. Notice that $u_2 = -\bar{u_2}$. In the multiplication definition we will use three parameters: $x_{r+\bar{r}}(u_0)$, $x_{r+\bar{r}}(u_1)$ and $x_{r+\bar{r}}(u_2)$. We need to break the multiplication definition into three parts:

1. To multiply two elements a, b of ϑ_0: notice there are h_0 and h_1 such that $a = h_0 x_{r+\bar{r}}(u_0) h_0^{-1}$ and $b = h_1 x_{r+\bar{r}}(u_0) h_1^{-1}$. Then define $a \otimes b = h_1 h_0 x_{r+\bar{r}}(u_0) h_0^{-1} h_1^{-1}$.

2. To multiply two elements $a \in \vartheta_0$ and $b \in \vartheta_1$: notice there are h_0 and h_1 such that $a = h_0 x_{r+\bar{r}}(u_0) h_0^{-1}$ and $b = h_1 x_{r+\bar{r}}(u_1) h_1^{-1}$. Then define $a \otimes b = h_1 h_0 x_{r+\bar{r}}(u_1) h_0^{-1} h_1^{-1}$.

3. To multiply two elements a, b of ϑ_1: notice there are h_0 and h_1 such that $a = h_0 x_{r+\bar{r}}(u_1) h_0^{-1}$ and $b = h_1 x_{r+\bar{r}}(u_1) h_1^{-1}$. Then define $a \otimes b = h_1 h_0 x_{r+\bar{r}}(u_2) h_0^{-1} h_1^{-1}$.

The reader can check these maps are well-defined, by elementary character properties. We now show that the uniformly parameter definable map

$$i^{Atw} : \ K_0 \mapsto Z; \quad i^{Atw}(\lambda) = x_{r+\bar{r}}(\lambda u_0) \quad (\lambda \in K_0)$$

is an isomorphism. Additively, this is clearly an isomorphism. Let us check multiplication:

- Let $\lambda^2, \nu^2 \in (K_0^\times)^2$. There are $h_\lambda, h_\nu \in H^1$ such that $x_{r+\bar{r}}(\lambda^2 u_0) = h_\lambda x_{r+\bar{r}}(u_0) h_\lambda^{-1}$ and $x_{r+\bar{r}}(\nu^2 u_0) = h_\nu x_{r+\bar{r}}(u_0) h_\nu^{-1}$. So by clause 1 of the multiplication definition, $i^{Atw}(\lambda^2 \nu^2) = x_{r+\bar{r}}(\lambda^2 \nu^2 u_0) = h_\lambda h_\nu x_{r+\bar{r}}(u_0) h_\nu^{-1} h_\lambda^{-1} = x_{r+\bar{r}}(\lambda^2 u_0) \otimes x_{r+\bar{r}}(\nu^2 u_0) = i^{Atw}(\lambda^2) i^{Atw}(\nu^2)$.

- Let $\lambda \in K_0^\times \backslash (K_0^\times)^2$ and $\nu^2 \in (K_0^\times)^2$. Then we may write $\lambda u_0 = \eta^2 u_1$. Thus there are $h_\eta, h_\nu \in H^1$ such that $x_{r+\bar{r}}(\eta^2 u_1) = h_\eta x_{r+\bar{r}}(u_1) h_\eta^{-1}$ and $x_{r+\bar{r}}(\nu^2 u_0) = h_\nu x_{r+\bar{r}}(u_0) h_\nu^{-1}$. So by clause 2 of the multiplication definition, $i^{Atw}(\lambda \nu^2) = x_{r+\bar{r}}(\lambda \nu^2 u_0) = x_{r+\bar{r}}(\eta^2 \nu^2 u_1) = h_\eta h_\nu x_{r+\bar{r}}(u_1) h_\nu^{-1} h_\eta^{-1} = x_{r+\bar{r}}(\nu^2 u_0) \otimes x_{r+\bar{r}}(\eta^2 u_1) = x_{r+\bar{r}}(\nu^2 u_0) \otimes x_{r+\bar{r}}(\lambda u_0) = i^{Atw}(\nu^2) i^{Atw}(\lambda)$.

- Let $\lambda, \nu \in (K_0^\times) \backslash (K_0^\times)^2$. Then we may write $\lambda u_0 = \eta^2 u_1$ and $\nu u_0 = \zeta^2 u_1$. Thus there are $h_\eta, h_\zeta \in H^1$ such that $x_{r+\bar{r}}(\eta^2 u_1) = h_\eta x_{r+\bar{r}}(u_1) h_\eta^{-1}$ and $x_{r+\bar{r}}(\zeta^2 u_1) = h_\zeta x_{r+\bar{r}}(u_1) h_\zeta^{-1}$. So by clause 3 of the multiplication definition, $i^{Atw}(\lambda \nu) = x_{r+\bar{r}}(\lambda \nu u_0) = x_{r+\bar{r}}(\eta^2 \zeta^2 u_2) = h_\eta h_\zeta x_{r+\bar{r}}(u_2) h_\zeta^{-1} h_\eta^{-1} = x_{r+\bar{r}}(\eta^2 u_1) \otimes x_{r+\bar{r}}(\zeta^2 u_1) = x_{r+\bar{r}}(\nu u_0) \otimes x_{r+\bar{r}}(\lambda u_0) = i^{Atw}(\nu) i^{Atw}(\lambda)$.

5.3.5 Conclusion of proof of Theorem 5.3.3

Our first step is to prove 5.3.3 just for uniform parameter bi-interpretations, and not yet for strong uniform parameter bi-interpretations. We aim to apply Lemma 4.3.12. But the results of Sections 5.3.3, and 5.3.4 put us exactly in a position to apply that lemma.

Next, we aim to apply Lemma 4.2.11 to show that, in fact, we have a strong uniform parameter bi-interpretation. We work with the notation of that lemma: $\mathcal{C}$ is the class

of groups, $\mathcal{D}$ is the class of fields. Then, of the requirements to apply the lemma, we have shown the existence of the uniform parameter bi-interpretation. Next we show that a given family of twisted groups is strongly UPD in finite fields: we know that the overlying Chevalley group is strongly UPD. Further, since we have worked with a Chevalley basis, we have seen that the generating root subgroups are strongly UPD. But the maximal unipotent subgroup U and its opposite group V are then clearly strongly UPD by the big cell presentation of the maximal unipotent subgroup: see [4] Theorem 5.3.3.

For finite fields, we have stated that their unique n-degree extensions, with embedding, are also strongly UPD: this is, once more, because the theory of fields is finitely axiomatisable. It follows that U^1 and V^1 are strongly UPD. We may then apply Lemma 5.3.5 to conclude that G^1 is strongly UPD.

Once again, Remark 5.2.9 demonstrates that clause 2 of Lemma 4.2.11 is also satisfied. We may thus apply Lemma 4.2.11 to conclude the theorem.

5.4 The remainder of the twisted groups

The families of finite simple groups of Lie Type that remain are those twisted groups whose underlying Lie algebras do not have root systems all of whose roots have the same length. So in this section we examine the following classes:

Let SUZ be the class of finite simple groups of type ${}^2B_2$, the Suzuki groups.

Let REE_F be the class of finite simple groups of type ${}^2F_4$, the Ree groups of F-type.

Let REE_G be the class of finite simple groups of type ${}^2G_2$, the Ree groups of G-type.

Let $\mathcal{T}_{\text{diff}} = SUZ \cup REE_F \cup REE_G$ be the class of twisted groups built over difference fields.

DISCUSSION 5.4.1

1. All general results about twisted simple groups in 5.3.2 remain valid here. Those that do not are, in particular, those that pertain to simple groups built from Lie algebras whose root systems have all roots of the same length.

2. A finite simple group in $\mathcal{T}_{\text{diff}}$ is constructed using only a finite simple group of type B_2, F_4 or G_2 as appropriate, and an appropriate group automorphism θ. Let us describe this in detail for each of the subclasses SUZ, REE_F and REE_G:

   For any group ${}^2B_2(K)$ we have $|K| = 2^{2i+1}$ for some $i \in \mathbb{N}$. So let us consider the class of finite difference fields $\mathcal{C}_{(1,2,2)}$, and suppose $(K, \sigma) \in \mathcal{C}_{(1,2,2)}$. Then ${}^2B_2(K)$ is constructed using firstly $B_2(K)$ and a graph automorphism of $B_2(K)$. These are both UPD over $\mathcal{C}_{(1,2,2)}$ - (see Section 5.2). Secondly, a field automorphism of $B_2(K)$ is required. The field automorphism extends the action of σ on K. Suppose that $\{x_r(t) : \ t \in K\}$ is one of the strongly uniformly definable root subgroups; then the action of the field automorphism is the expected one:

   $$\sigma(x_r(t)) = x_r(\sigma(t))$$

   That the action can be extended to $B_2(K)$ strongly uniformly follows from Lemma 5.2.5. It follows that the groups U^1 and V^1 of ${}^2B_2$ are UPD in $\mathcal{C}_{(1,2,2)}$. However, we do not know yet that ${}^2B_2$ itself is UPD in $\mathcal{C}_{(1,2,2)}$, because we lack a theorem like 5.3.5.

   Identically, for any group ${}^2F_4(K)$ we have $|K| = 2^{2i+1}$ for some $i \in \mathbb{N}$, and the same analysis as for groups of type ${}^2B_2$ shows that the groups U^1 and V^1 of ${}^2F_4$ are UPD in $\mathcal{C}_{(1,2,2)}$.

   The groups ${}^2G_2$ are similar. However, for any group ${}^2G_2(K)$ we have $|K| = 3^{2i+1}$ for some $i \in \mathbb{N}$. So this time we work with the class of finite difference fields $\mathcal{C}_{(1,2,3)}$, and suppose $(K, \sigma) \in \mathcal{C}_{(1,2,3)}$. Similar to the groups in SUZ and REE_F, a group ${}^2G_2(K)$ is constructed using firstly $G_2(K)$ and a graph automorphism of $G_2(K)$ which are both UPD over $\mathcal{C}_{(1,2,3)}$, and then a field automorphism of

$G_2(K)$ which extends the action of σ on K. Our conclusion is identical: the groups U^1 and V^1 of ${}^2G_2$ are UPD in $\mathcal{C}_{(1,2,3)}$.

For details about the graph automorphisms used to build the groups in $\mathcal{T}_{\text{diff}}$, see [4] Sections 12.3 and 12.4, which are devoted to this. That they are UPD is clear. The relevant field automorphisms are described on page 225 of [4], at the beginning of Section 13.4.

3. We shall be required to introduce more notation and to recapitulate a few more notions from [4]. We work specifically with the notation of 5.3.2 (6). Additionally, for now let $G = G(K)$ be a Chevalley group over the field K, with maximal torus H. We have already mentioned in 5.3.2 (6) that the elements $h \in H$ correspond to characters on the free group $Q = \mathbb{Z}[\{q_i : 1 \leq i \leq n\}]$. We denote by χ_{p_i,t_i} the character with $\chi_{p_i,t_i}(q_i) = t_i$ and $\chi_{p_i,t_i}(q_j) = 1$ for $j \neq i$. In terms of the free subgroup of Q, $P = \mathbb{Z}[\Phi]$, let $a, r \in P$, then $\chi_{r,t}(a) = t^{2\frac{(r,a)}{(r,r)}}$ - the reader will recall from 5.3.2 (6) and 5.2.2 (4) that $(\cdot,\cdot)$ is the Killing form. Suppose that $h \in H$ and h induces the character $\chi_{r,t}$ on Q. Then in this section we shall write $h = h_r(t)$. More generally, if h induces the character χ on Q, then in this section we shall write $h = h(\chi)$.

4. Let us describe the group H^1 for groups of type ${}^2B_2$, ${}^2F_4$ and ${}^2G_2$. Again, let us assume that $G^1 = G^1((K,\sigma))$, so the field automorphism used for the defining automorphism θ is σ. The theorem we make use of is Theorem 13.7.4 of [4]. It states that the elements $h(\chi) \in H$ which are fixed by θ are the ones for which $\chi(\bar{r}) = \chi(r)^{\lambda(\bar{r})\sigma}$. Here $\lambda(r)$ is 1 if r is a short root, $\lambda(r)$ is 2 if r is a long root and the group is of type ${}^2B_2$ or ${}^2F_4$, and $\lambda(r)$ is 3 if r is a long root and the group is of type ${}^2G_2$.

It also states that for $\mathcal{T}_{\text{diff}}$-groups defined over finite fields, then $h \in H^1$ if and only if h is fixed by the defining automorphism θ. Since our work also relates to twisted simple groups over pseudo-finite difference fields, it is worthwhile remarking that Theorem 13.7.4 of [4] also holds for ultraproducts of $\mathcal{T}_{\text{diff}}$-groups. This is a direct consequence of 5.4.3 part (ii), and it is the reason we include that result.

Let (K, σ) be an appropriate finite or pseudo-finite difference field, and σ satisfying Frob$\sigma^2 = \mathrm{id}$. 'Appropriateness' will be clear from the context of the next three paragraphs:

So now, let us consider a group ${}^2B_2((K, \sigma))$. The overlying Chevalley group is $B_2(K)$. Suppose that $\Pi = \{a, b\}$ with a the short root and b the long root (see [4] 12.3 for details). Then we have $H = \{h_a(s)h_b(t) : \ s, t \in K^\times\}$. Let $h = h_a(s)h_b(t) \in H$. By Lemma 13.7.1 of [4] and Proposition 12.3.3 of [4], we have $\theta(h_a(s)h_b(t)) = h_b(s^{2\sigma})h_a(t^\sigma)$. If $h \in H^1$, then we have $h_a(s)h_b(t) = h_b(s^{2\sigma})h_a(t^\sigma)$. In terms of characters, we must have the equality $\chi_a(s)\chi_b(t) = \chi_a(t^\sigma)\chi_b(s^{2\sigma})$. It follows that $\chi_a(s) = \chi_a(t^\sigma)$, and $\chi_b(t) = \chi_b(s^{2\sigma})$. Then these equations are satisfied if and only if $s = t^\sigma$. So

$$H^1 = \{h_a(t^\sigma)h_b(t) : \ t \in K^\times\}$$

Now let us consider a group ${}^2G_2((K, \sigma))$. The analysis is identical with the following amendment: By Lemma 13.7.1 of [4] and Proposition 12.4.1 of [4], we have $\theta(h_a(s)h_b(t)) = h_b(s^{3\sigma})h_a(t^\sigma)$. However, the result is still the same:

$$H^1 = \{h_a(t^\sigma)h_b(t) : \ t \in K^\times\}$$

Now let us consider ${}^2F_4$. Suppose $\Pi = \{c, a, b, d\}$ with c and a short, and b and d long (see [4] 12.3 for details). A similar analysis shows that

$$H^1 = \{h_c(s^\sigma)h_a(t^\sigma)h_b(t)h_d(s) : \ t, s \in K^\times\}$$

The exceptional non-simple twisted groups excluded from the results in this last section are ${}^2B_2(2)$, ${}^2G_2(3)$ and ${}^2F_4(2)$ ([4] 14.4.1).

We make use of difference fields of the form $(\mathbb{F}_{p^{2k+1}}, \mathrm{Frob}^k)$ so in terms of Chapter 2 and the theories $PSF_{(m,n,p)}$: $n = 2, \ m = 1$.

To begin, we must prove an analogue to Theorem 5.3.5, but for the groups in $\mathcal{T}_{\mathrm{diff}}$. Our theorem and proof will be virtually identical to 5.3.5, but we shall make very strong

use of our results in Chapters 2 on the theory $PSF_{(m,l,p)}$, and of our results in Chapter 3 on GS_1-theories:

LEMMA 5.4.2 *There is $n \in \mathbb{N}$ and a function $\varphi : \{1, 2, \ldots, n\} \mapsto \{U^1, V^1\}$ such that for any $G^1 \in \mathcal{T}_{\text{diff}}$ we have*

$$G^1 = \prod_{i=1}^{n} \varphi(i)(K)$$

PROOF Suppose this were not so. We may assume that all the exceptions come from one of the classes SUZ, REE_F or REE_G. Call this class $\mathcal{T}$; define $q = 3$ if $\mathcal{T} = REE_G$ and define $q = 2$ otherwise. Then we may assume that there is a sequence of groups in $\mathcal{T}$ indexed by $i \in \mathbb{N}$: $G^1(\mathbb{F}_{q^{2k_i+1}}) \in \mathcal{T}_{\text{diff}}$ such that the minimum number of steps for $V^1(\mathbb{F}_{q^{2k_i+1}})$ and $U^1(\mathbb{F}_{q^{2k_i+1}})$ to generate $G^1(\mathbb{F}_{q^{2k_i+1}})$ is greater than j.

Since $\mathcal{T}$ corresponds to an overlying class of Chevalley groups, we denote by $L(F)$ a member of the latter over the field F. Now, consider the difference fields $E = \{(\mathbb{F}_{q^{2k_i+1}}, \text{Frob}^{k_i}) : i \in \mathbb{N}\}$. Let (K, σ) be a non-principal ultraproduct of the members of E. Then $(K, \sigma) \models PSF_{(1,2,q)}$. Further, we may apply $\mathcal{L}$os's theorem to all the objects we have shown to be UPD in the $(\mathbb{F}_{q^{2k_i+1}}, \text{Frob}^{k_i})$: the ultraproduct of the Frob^{k_i} is σ, the ultraproduct of the $L(\mathbb{F}_{q^{2k_i+1}})$ is $L(K)$, the ultraproduct of the UPD group automorphisms of $L(\mathbb{F}_{q^{2k_i+1}})$ described in 5.4.1 (2) is a definable automorphism γ which is a product of a definable graph automorphism and a definable field automorphism of $L(K)$. Thus, the ultraproduct of the $V^1(\mathbb{F}_{q^{2k_i+1}})$ is $V^1(K)$ and the ultraproduct of the $U^1(\mathbb{F}_{q^{2k_i+1}})$ is $U^1(K)$. By [4] Theorem 14.4.1, $G^1(K) = \langle U^1(K), V^1(K) \rangle$ is a simple group. We now work inside $G^1(K)$. We denote it G^1, and refer to U^1, V^1, etc.

So, by our construction, U^1 and V^1 do not generate G^1 in finitely many steps. However, at the ultraproduct level, all the objects we have defined have been defined in (K, σ). Since $(K, \sigma) \models PSF_{(1,2,q)}$ we may apply Theorem 4.3.4 to deduce that (K, σ) is a group of finite GS_1-rank. So we may apply Proposition 4.3.9: it shows that there is a definable group $H \subseteq (U^1 V^1)^n$ for some $n \in \mathbb{N}$ such that $H \lhd \langle U^1, V^1 \rangle$ and H/U^1 and H/V^1 are finite. Since $G^1 = \langle U^1, V^1 \rangle$ and since G^1 is simple, it follows that $H = G^1$. So we have a contradiction. $\square$

COROLLARY 5.4.3 *(i) Let $\mathcal{T} \in \{SUZ, REE_G, REE_F\}$, and let $q = 3$ if $\mathcal{T} = REE_G$, and $q = 2$ otherwise. Then the class $\mathcal{T}$ is UPD in the class of finite difference fields $\mathcal{C}_{(1,2,q)}$.*

(ii) (The ultraproduct of finite $\mathcal{T}_{\text{diff}}$-groups is the $\mathcal{T}$-group built over the ultraproduct of the defining difference fields): Let $\mathcal{T} \in \{SUZ, REE_F, REE_G\}$; define $q = 3$ if $\mathcal{T} = REE_G$ and define $q = 2$ otherwise. Let $\{G^1((K_i, \sigma_i)) : i \in \mathbb{N}\}$ be a sequence of $\mathcal{T}$-groups where for an appropriate difference field (K, σ), $G^1((K, \sigma))$ is the $\mathcal{T}$-group built over the difference field (K, σ). Suppose that all the K_i are finite fields. Let $\mathcal{U}$ be an ultrafilter on $\mathbb{N}$. Let $G^1_{\text{ult}} = \prod_{i\in\mathbb{N}} G^1((K_i, \sigma_i))/\sim_{\mathcal{U}}$. Let $(K, \sigma) = \prod_{i\in\mathbb{N}}(K_i, \sigma_i)/\sim_{\mathcal{U}}$. Then $G^1((K, \sigma)) \cong G^1_{\text{ult}}$.

PROOF (i) Let $\mathcal{T} \in \{SUZ, REE_G, REE_F\}$, and let $q = 3$ if $\mathcal{T} = REE_G$, and $q = 2$ otherwise. Firstly, in Discussion 5.4.1 (2) we explained that for $\mathcal{T}$, the subgroups U^1 and V^1 are UPD in $\mathcal{C}_{(1,2,q)}$. Then it follows by 5.4.2 that for $\mathcal{T}$, G^1 is also UPD in $\mathcal{C}_{(1,2,q)}$.

(ii) This now follows simply from part (i). □

We must also work, similarly as we have done in previous sections, to show that H^1 is UPD.

LEMMA 5.4.4 *Let $G^1 = G^1(K) \in \mathcal{T}_{\text{diff}}$. There is $f \in \mathbb{N}$ such that if $|K| \geq f$, for each $r \in \Phi$ there is $h \in H^1$ such that the character χ induced by h satisfies $\chi(r) \neq 1$.*

PROOF Let Π be the fundamental system for the root system of the Lie algebra of the Chevalley group above G^1. So Π is a free basis for $\mathbb{Z}[\Phi]$. Let σ be the automorphism of K which is the underlying field automorphism in the construction of G^1. Also, suppose that $q = \text{char}(K)$, and $|K| = q^{2n+1}$ for some $n \in \mathbb{N}$. Now let $\Pi^* = \{c, a, b, d\}$, where $\Pi^* \supseteq \Pi$ and $c = d = 0$, if the type of G^1 is not ${}^2F_4$, and $\Pi^* = \Pi$ otherwise. We let a, c be short roots and we let b, d be long roots. Let $r \in \Phi$. Then $r = ea + fb + gc + hd$ for some integers e, f, g, h independent of $|K|$. There are two cases to consider:

Suppose that either of $e, f \neq 0$. Then using 5.4.1 (4) again, we may find $h \in H^1$ which induces a character χ such that $\chi(a) = t$, $\chi(b) = t^{q\sigma}$, $\chi(c) = \chi(d) = 1$, for any $t \in K^\times$. So $\chi(r) = t^e(t^{q\sigma})^f$. Thus, by 5.4.1 (2), $\chi(r) = t^{e+fq^{n+1}}$. But for all large enough K, there must be $t \in K^\times$ such that $t^{e+fq^{n+1}} \neq 1$. We pick $h \in H^1$ that induces a corresponding χ.

If $e = f = 0$ then either of $c, d \neq 0$. The exact analysis of the previous paragraph holds, replacing a with c, b with d, e with g, and f with h. □

This allows us to prove the $\mathcal{T}_{\text{diff}}$-analogue to Lemma 5.3.8:

LEMMA 5.4.5 *There is $f \in \mathbb{N}$, such that for $|K| > f$, the subgroup H^1 is uniformly parameter definable in any of the families SUZ, REE_F or REE_G.*

PROOF We begin by applying 5.4.4 and the unique Bruhat decomposition for twisted groups (5.3.2 (6)). By Bruhat, we may write any $g \in G^1$ uniquely as $g = u'h_0n_wu$ for some $u' \in U^1$, $h_0 \in H^1$, $n_w \in N^1$, and $u \in (U_w^-)^1$. Then let $h \in H^1$. Identically to the first paragraph of the proof of 5.3.8, if $g = hgh^{-1}$, then $u' = hu'h^{-1}$, $n_w = hn_wh^{-1}$ and $u = huh^{-1}$. Now consider u: by 5.2.2 (3) u has a unique Chevalley cell presentation: $u = x_{r_1}(t_1)x_{r_2}(t_2)\dots x_{r_n}(t_n)$. If h does not commute with any of the $x_{r_i}(t_i)$, then h does not commute with u. But then, for large enough $|K|$, for each $r \in \Phi^+$ we may select $h_r \in H^1$ such that h_r does not commute with any element of $X_r\backslash\{0\}$. So $H^1 \subseteq \cap_{r\in\Phi^+}C_{G^1}(h_r) \subseteq N^1$.

Let $J^1 = \cap_{r\in\Phi^+}C_{G^1}(h_r)$. By [4] Section 13.3, we have $|W^1({}^2B_2)| = 2$, $|W^1({}^2G_2)| = 2$ and $|W^1({}^2F_4)| = 16$. Consider the uniformly parameter definable set:

$$(J^1)^{16} = \{g^{16} : \ g \in J^1\}$$

Then $(H^1)^{16} \subseteq (J^1)^{16} \subseteq H^1$. But inspecting our characterisations of H^1 for the $\mathcal{T}_{\text{diff}}$-families in 5.4.1 (4), we see that $|H^1/(H^1)^{16}| \leq 256$. It follows that H^1 is uniformly parameter definable. □

PROPOSITION 5.4.6 *(i) There is a uniform parameter bi-interpretation between $\mathcal{C}_{(1,2,2)}$ and SUZ.*

(ii) There is a uniform bi-interpretation between $\mathcal{C}_{(1,2,2)}$ and REE_F.

(iii) There is a uniform parameter bi-interpretation between $\mathcal{C}_{(1,2,3)}$ and REE_G.

PROOF In the following, we use the notation K^* for the interpretation of a field K in a group G. The reader should not confuse K^* with the multiplicative subgroup of the field K, which is referred to as $K^\times$. Again, we inherit the general notation of the previous sections.

For each part of the theorem we break the uniform bi-interpretation into parts:

(a) We describe the perfect matching m between a class of difference fields and a class of groups.
(b) We exhibit a UPD of the group $m((K,\sigma))$ in the difference field (K,σ). We denote the interpretation $m((K,\sigma))^*$.
(c) We exhibit a UPD of (K,σ) in $m((K,\sigma))$. We denote the interpretation $(K,\sigma)^*$.
(d) We conclude the theorem by applying Lemmas 4.2.11 and 4.3.12.

With this in hand we begin with (i):

(a) The matching is straightforward, and arises from Discussion 5.4.1 (2). Every group in SUZ is a group ${}^2B_2(K)$ where K is a field of cardinality 2^{2k_i+1} for some $k_i \in \mathbb{N}$. So we match $m:\ \mathcal{C}_{(1,2,2)} \leftrightarrow SUZ$ by $m((\mathbb{F}_{2^{2k_i+1}}, \mathrm{Frob}^{k_i})) = {}^2B_2(\mathbb{F}_{2^{2k_i+1}})$.

(b) This is 5.4.3 part (i).
(c) Let (K,σ) be an arbitrary member of $\mathcal{C}_{(1,2,2)}$. We work with ${}^2B_2(K)$. In [4] (pp. 234-236) the following two facts are established about ${}^2B_2(K)$:

(1) With respect to a system of fundamental roots $\{a,b\}$ in the Dynkin diagram of type B_2 there is a twisted root subgroup X_S^1 consisting of elements:

$$x_a(t^\sigma)x_b(t)x_{a+b}(t^{\sigma+1}+u)x_{2a+b}(u^{2\sigma})$$

for all $t, u \in K$.

(2) Expressing an element of X_S^1(uniquely) as $x_s(t,u) = \alpha(t)\beta(u)$ where

$$\alpha(t) = x_a(t^\sigma)x_b(t)x_{a+b}(t^{\sigma+1}) \tag{5.1}$$
$$\beta(u) = x_{a+b}(u)x_{2a+b}(u^{2\sigma})$$

then

$$x_s(t_1,u_1)x_s(t_2,u_2) = x_s(t_1+t_2, u_1+u_2+t_1^\sigma t_2) \tag{5.2}$$

Then as in 5.4.1 (4) we have:

$$H^1 = \{h_a(t^\sigma)h_b(t) : t \in K^\times\}$$

- H^1 is UPD in SUZ By adjusting the resulting UPD formula (Lemma 5.2.3) we see H^1 is UPD.

- Consider the subgroup $Z(X_S^1) = \{\beta(u) : u \in K\}$. Now using the Cartan marix we see that $h(t)\beta(u)h(\frac{1}{t}) = \beta(t \cdot u)$. So H^1 acts on $Z(X_S^1)$ via conjugation with one orbit. Thus $Z(X_S^1)$ is UPD. Exactly as in previous sections we may use the conjugation action of H^1 on $Z(X_S^1)$ to define a multiplication on $Z(X_S^1)\backslash\{0\}$. A full field structure on $Z(X_S^1)$ is obtained by interpreting field addition as G^1 multiplication restricted to $Z(X_S^1)$. This is done explicitly in [27] pp.72.

  With this interpreted field structure on $Z(X_S^1)$ there is a UPD isomorphism of fields $i : K \mapsto Z(X_S^1)$ sending $u \in K$ to $\beta(u)$.

So with the field structure of K being UPD in G^1, we focus on interpreting the automorphism σ.

We begin by verifying that $\{\alpha(s) : s \in K\}$ is a uniformly parameter-definable set. Let $h \in H^1$. So $h = h_a(t^\sigma)h_b(t)$ for some $t \in K^\times$. Then we have

$$\begin{aligned} &h_a(s^\sigma)h_b(s)x_r(t)h_b(\frac{1}{s})h_a(\frac{1}{s^\sigma}) \\ &= h_a(s^\sigma)(x_r(s^{A_{br}} \cdot t))h_a(\frac{1}{s^\sigma}) \\ &= x_r(s^{\sigma \cdot A_{ar}} \cdot s^{A_{br}} \cdot t) \end{aligned}$$

So using this we compute the action of H^1 on an element $\alpha(t)$ where by $\alpha(t)$ we mean an element $\alpha(t)\beta(0)$.

$$\begin{aligned} & h_a(s^\sigma)h_b(s)(x_a(t^\sigma)x_b(t)x_{a+b}(t^{\sigma+1})h_b(\frac{1}{s})h_a(\frac{1}{s^\sigma}) \\ & = x_a(s^{2\sigma}\cdot\frac{1}{s}\cdot t^\sigma)x_b(\frac{1}{s^{2\sigma}}\cdot s^2\cdot t)x_{a+b}(s\cdot t^{\sigma+1}) \end{aligned} \tag{5.3}$$

Letting $\varepsilon = \frac{1}{s^{2\sigma}}\cdot s^2\cdot t$ we see expression 5.3 is $x_a(\varepsilon^\sigma)x_b(\varepsilon)x_{a+b}(\varepsilon^{\sigma+1})$ and this shows that $\{\alpha(t) : t \in K\}$ is closed under the action of H^1. Look at the orbit of $\alpha(1)$. It suffices to show that for all $t \in K^\times$ there exists $s \in K^\times$ with $t = s^{2-2\sigma}$. Since $s \mapsto s^{2-2\sigma}$ is a multiplicative homomorphism of $K^\times$ and we are considering K a finite field of characteristic 2, it suffices to show the kernel of the homomorphism is trivial. But then

$$\begin{aligned} & s^{2-2\sigma} = 1 \\ & \Rightarrow s^{1-\sigma} = 1 \\ & \Rightarrow s = s^\sigma \Rightarrow s = s^\sigma = s^{\sigma^2} = \sqrt{s} \\ & \Rightarrow s = 1 \end{aligned} \tag{5.4}$$

The conclusion is that the set $\{\alpha(t) : t \in K\}$ is a UPD set, since it is the orbit of any of its elements under the conjugation action of the UPD group H^1. So let $A = \{\alpha(t) : t \in K\}$ and let $B = Z(X_S^1) = \{\beta(u) : u \in K\}$. Since $Z(X_S^1)$ was also UPD, we conclude that X_S^1 itself is UPD. We also conclude that there are UPD coordinate functions $f_\alpha : X_S^1 \mapsto A$ and $f_\beta : X_S^1 \mapsto B$ well-defined by the equation $x \in X_S^1 \Rightarrow x = f_\alpha(x)\cdot f_\beta(x)$.

Now consider the following two UPD maps $m_i : A \mapsto B$:

$$\begin{aligned} & m_1(\alpha(t)) = f_\beta(\alpha(1)\cdot\alpha(t)) \\ & m_2(\alpha(t)) = f_\beta(\alpha(t)\cdot\alpha(1)) \end{aligned} \tag{5.5}$$

Computing, we see that $m_1(\alpha(t)) = \beta(t)$ and $m_2(\alpha(t)) = \beta(t^\sigma)$. So consider the map $m_2 m_1^{-1} : \ B \mapsto B$. With respect to the UPD interpretation of the field K, the automorphism $m_2 m_1^{-1}$ is seen to be a UPD interpretation of σ. So we let $K^* = B$ and $\sigma^* = m_2 m_1^{-1}$, and this is the UPD interpretation of (K, σ) in ${}^2B_2(K)$.

(d) The choice of UPD isomorphism is now clear from the interpretation:
We define

$$i : \qquad K \mapsto K^*; \qquad u \mapsto \beta(u)$$
$$\sigma \mapsto \sigma^*$$

The reader can verify that i is an isomorphism of difference fields.

As usual, we now apply Lemma 4.3.12 to show that we have a uniform parameter bi-interpretation, and Lemma 4.2.11 to show that we have a strong uniform parameter bi-interpretation. That clause 1 of the requirements to apply 4.2.11 is satisfied was emphasized in part (b) of the proof. Clause 2 is satisfied simply because difference fields of characteristic 2 whose automorphism σ satisfies:

$$\forall x : \ \sigma^2(x^2) = x$$

are finitely axiomatisable (proof: I just did it).

(ii) Since ${}^2F_4$ has a twisted root group X_S^1 with S of type B_2, the proof is identical to that for the Suzuki groups ${}^2B_2$.

(ii) The proof is identical to the proof of (i), with everything relativised to the Ree groups. There is one non-trivial verification- that the finite simple groups of type ${}^2G_2$ interpret the necessary difference field automorphism. As above, we outline the necessary facts from [4] (13.6.3) and (13.6.4): here $S = \{a, b, a+b, 2a+b, 3a+b, 3a+2b\}$. Again, X_S^1 is UPD. The elements of X_S^1 in this case are of the (unique) form

$$x_a(t^\sigma)x_b(t)x_{a+b}(t^{\sigma+1}+u^\sigma)x_{2a+b}(t^{2\sigma+1}+v^\sigma)x_{3a+b}(u)x_{3a+2b}(v)$$

Expressing this $x \in X_S^1$ as $x = x_s(t,u,v) = \alpha(t)\beta(u)\gamma(v)$ where

$$\begin{aligned}\alpha(t) &= x_a(t^\sigma)x_b(t)x_{a+b}(t^{\sigma+1})x_{2a+b}(t^{2\sigma+1})\\ \beta(t) &= x_{a+b}(u^\sigma)x_{3a+b}(u)\\ \gamma(v) &= x_{2a+b}(v^\sigma)x_{3a+2b}(v)\end{aligned} \tag{5.6}$$

we have the product formula

$$x_s(t_1,u_1,v_1)x_s(t_2,v_2,u_2) = x_s(t_1{+}t_2, u_1{+}u_2{-}t_1t_2^{3\sigma}, v_1{+}v_2{-}t_2u_1{+}t_1t_2^{3\sigma+1}{-}t_1^2t_2^{3\sigma}) \tag{5.7}$$

Now in ([27] chap.5 Lemma 5) the following interpretation of K inside ${}^2G_2(K)$ is given: The underlying set is $Z(X_S^1) = \{\gamma(v) : v \in K\}$, the addition is group G^1 multiplication, and the multiplication is from the conjugation action of H^1 on $Z(X_S^1)$, where H^1 is as in 5.4.1 (4).

Let $A = \{\alpha(t) : t \in K\}$, $B = \{\beta(u) : u \in K\}$ and $C = \{\gamma(v) : v \in K\}$. We begin by showing that A and B are UPD. To that end consider the action of H^1 on A. Letting $h = h_a(y^\sigma)h_b(y)$, we have

$$h\alpha(t)h^{-1} = x_a(y^{2\sigma}\cdot\frac{1}{y}\cdot t^\sigma)x_b(y^{-3\sigma}\cdot y^2\cdot t)x_{a+b}(y^{-\sigma}\cdot y\cdot t^{\sigma+1})x_{2a+b}(y^\sigma\cdot t^{2\sigma+1})$$

and letting $\varepsilon = y^{-3\sigma}\cdot y^2\cdot t$ we see the RHS is just $\alpha(\varepsilon)$. Again, to show A is definable, it is enough to show that the H^1 action has one non-trivial orbit. This reduces to showing that for any $t \in K^\times$ there exists $y \in K^\times$ such that $t = y^{2-3\sigma}$. Since we are working in finite fields, and $y \mapsto y^{2-3\sigma}$ is a homomorphism $K^\times \mapsto K^\times$ we need only show the kernel is trivial. But then

$$y^{2-3\sigma} = 1 \Rightarrow y^2 = y^{3\sigma} \Rightarrow y^{2\sigma} = y \Rightarrow y^\sigma = y^{2\sigma^2} \Rightarrow y^{2\sigma} = y^{4\sigma^2}$$

Thus $y^3 = y^{12\sigma^2} = y^4$

Thus $y = 1$

In the case of B, again say $h \in H^1 = h_a(y^\sigma)h_b(y)$. Then

$$h\beta(u)h^{-1} = x_{a+b}(y^{-\sigma} \cdot y \cdot u^\sigma)x_{3a+b}(y^{3\sigma} \cdot y^{-1} \cdot u)$$

and letting $\varepsilon = y^{3\sigma} \cdot y^{-1} \cdot u$ this is indeed $\beta(\varepsilon)$. The UPD of B reduces in this case to showing that the action of H^1 on B has exactly two non-trivial orbits. This comes from the fact that the multiplicative homomorphism $y \mapsto y^{3\sigma-1}$ has kernel $\{\pm 1\}$. Here it is easy: $y^{3\sigma-1} = 1 \Rightarrow y^{3\sigma} = y \Rightarrow y = y^\sigma \Rightarrow y = y^{\sigma^2} = y^{\frac{1}{3}} \Rightarrow y^3 = y \Rightarrow y = \pm 1$.

So as with the Suzuki group we have UPD coordinate functions $f_\alpha : X_S^1 \mapsto A$, $f_\beta : X_S^1 \mapsto B$ and $f_\gamma : X_S^1 \mapsto C$, well-defined by the equation $\forall x \in X_S^1\ x = f_\alpha(x)f_\beta(x)f_\gamma(x)$. Now we must give a uniform parameter definition for the automorphism. So consider the following two UPD maps $m_i : A \mapsto B$:

$$\begin{aligned} m_1 &: A \mapsto B \quad \alpha(t) \mapsto f_\beta(\alpha(t) \cdot x_s(-1,0,0)) \\ m_2 &: A \mapsto B \quad \alpha(t) \mapsto f_\beta(x_s(-1,0,0) \cdot \alpha(t)) \end{aligned} \tag{5.8}$$

Inspection of expression 5.8 shows that $m_1(\alpha(t)) = \beta(t)$ and $m_2(\alpha(t)) = \beta(t^{3\sigma})$. So letting $f = m_2 \circ m_1^{-1}$ we have $f(\beta(t)) = \beta(t^{3\sigma})$ Now we transfer this morphism to C. Consider the map

$$T : B \mapsto C \quad \beta(t) \mapsto f_\gamma \circ (\beta(t) \cdot x_s(-1,0,0))$$

Computing, we see that $i = T \circ f \circ\ T^{-1}$ is an isomorphism from C onto itself such that $i'(\gamma(v)) = \gamma(v^{3\sigma})$. We have a UPD automorphism of the interpreted field. The inverse of the frobenius is of course definable, so the automorphism of fields $\gamma(v) \mapsto \gamma(v^\sigma)$ is UPD. $\square$

Bibliography

[1] M. Aschbacher. *Finite groups*, volume 10 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 2000.

[2] M.F Atiyah and I.G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley series in mathematics. Addison-Wesley, 1969.

[3] J. Ax. The elementary theory of finite fields. *Annals of Mathematics*, 88:239–271, 1968.

[4] R. Carter. *Simple groups of Lie type*, volume XXVIII of *Pure and Applied Mathematics*. John Wiley and Sons, 1972.

[5] C.C. Chang and H.J. Keisler. *Model theory*. Number 73 in Studies in logic and foundations of mathematics. North Holland, 1998.

[6] Z. Chatzidakis. Theorie des corps finis et pseudo-finis. Technical report, CNRS/Paris 7, 1996.

[7] Z. Chatzidakis. Model theory of finite fields and pseudo-finite fields. *Annals of Pure and Applied Logic*, 88(2-3):95–108, 1997.

[8] Z. Chatzidakis and E. Hrushovski. The model theory of difference fields. *Transactions of the American Mathematical Society*, (351):2997–3071, 1999.

[9] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil. Model theory of difference fields, ii: Periodic ideals and the trichotomy in all characteristics. *Proceedings of the London Mathematical Society*, 85(2):257–311, 2002.

[10] Z. Chatzidakis, L. van den Dries, and A. Macintyre. Definable sets over finite fields. *Journal fur die reine und angewandte Mathematik*, (427):107–135, 1992.

[11] R.M. Cohn. *Difference Algebra*, volume 17 of *Interscience tracts in pure and applied mathematics*. Interscience publishers, Inc., 1965.

[12] R. Elwes. Personal communication, 2003.

[13] E. Hrushovski. The Elementary Theory of the Frobenius Automorphisms.

[14] E. Hrushovski. Strongly minimal expansions of algebraically closed fields. *Israel Journal of Mathematics*, 79:129–151, 1992.

[15] E. Hrushovski. Pseudofinite fields and related structures. In *Model Theory And Applications*, pages 151–212. 2003. Editors: L. Belair, Z. Chatzidakis, P. D'Aquino, D. Marker, M. Otero, F. Point, A. Wilkie.

[16] E. Hrushovski and A. Pillay. Groups definable in local fields and pseudo-finite fields. *Israel Journal of Mathematics*, (85):203–262, 1994.

[17] E. Hrushovski and A. Pillay. Definable subgroups of algebraic groups over finite fields. *Journal fur die reine und angewandte Mathematik*, (462):69–91, 1995.

[18] P.T. Johnstone. *Notes on logic and set theory*. Cambridge University Press, 1987.

[19] B. Kim and A. Pillay. Simple theories. *Annals of Pure and Applied Logic*, 88:149–164, 1997.

[20] L. Kramer, G. Rohrle, and K. Tent. Defining k in g(k). *Journal of Algebra*, 216:77–85, 1999.

[21] S. Lang. *Introduction to Algebraic Geometry*, volume 5 of *Interscience tracts in pure and applied mathematics*. Interscience publishers, Inc., 1958.

[22] S. Lang. *Algebra*. Addison-Wesley, third edition, 1993.

[23] D. Macpherson and C. Steinhorn. Asymptotic classes and measurable structures. 2003.

[24] Francoise Point. Ultraproducts and Chevalley Groups. *Archive for Mathematica Logic*, 38:355–372, 1999.

[25] M. Ryten and I. Tomasic. ACFA and measurability. *Selecta Mathematica, New Series*, 11:523–537, 2005.

[26] G.E. Sacks. *Saturated model theory*. W.A. Benjamin, 1972.

[27] S. Thomas. *Classification theory of simple locally finite groups*. PhD thesis, Bedford College, University of London, 1983.

[28] L. van den Dries and K. Schmidt. Bounds in the theory of polynomial rings over fields. *Inventiones mathematicae*, (76):77–91, 1984.

[29] F.O. Wagner. *Simple theories*. Kluwer, 2000.

[30] John S. Wilson. On Simple Pseusofinite Groups. *Journal of the London Mathematical Society*, 51:471–490, 1993.