F-STRUCTURES AND INTEGRAL POINTS ON SEMIABELIAN VARIETIES OVER FINITE FIELDS

RAHIM MOOSA AND THOMAS SCANLON

ABSTRACT. Motivated by the problem of determining the structure of integral points on subvarieties of semiabelian varieties defined over finite fields, we prove a quantifier elimination and stability result for finitely generated modules over certain finite simple extensions of the integers given together with predicates for cycles of the distinguished generator of the ring.

1. INTRODUCTION

The Mordell-Lang conjecture asserts that for G a semiabelian variety over the complex numbers, $X \subset G$ a subvariety, and $\Gamma \leq G(\mathbb{C})$ a finitely generated subgroup of the complex points, the set of points $X(\mathbb{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ. This fails when $\mathbb{C}$ is replaced by a field of positive characteristic. For example, suppose that X and G are defined over a finite field $\mathbb{F}_q$ and that $F : G \to G$ is the corresponding Frobenius morphism. Let $K := \mathbb{F}_q(X)$ and let $\Gamma \leq G(K)$ be the $\mathbb{Z}[F]$-submodule generated by $\gamma := \mathrm{id}_X : X \to X$ thought of as an element of $X(K)$. Then $X(K) \cap \Gamma$ contains the infinite set $\{F^n\gamma : n \in \mathbb{N}\}$. If X contains no translates of algebraic subgroups of G, then this fact already contradicts the naïve translation of the Mordell-Lang conjecture to positive characteristic.

Hrushovski salvages the Mordell-Lang conjecture in positive characteristic by proving a function field version in which varieties defined over finite fields are treated as exceptions to the general rule [2]. In this paper we generalize the rule so that these varieties are no longer exceptional.

In the case that X is a curve, the presence of these Frobenius orbits is the only obstruction to a clean statement of Mordell's conjecture. Samuel showed that if C is a curve of geometric genus at least two defined over a finite field, then for any finitely generated field K extending the field of definition of C, the set of K-rational points on C is a finite set of Frobenius orbits [8]. Continuing with the example at the end of the first paragraph, suppose that $Y = \overline{X + X}$ also contains no translates of infinite algebraic subgroups of G. This is the case, for example, when X is a curve of genus at least three embedded into its Jacobian $G = J_X$. Then $Y(K) \cap \Gamma$ contains the set $\{F^m\gamma + F^n\gamma : n, m \in \mathbb{N}\}$. We show in Section 7 of this paper that to handle the general case of the Mordell-Lang problem for G defined over a finite field we need only permit such sums of finitely many Frobenius orbits (together with groups) into the description of $X(K) \cap \Gamma$. It seems that the main step in proving this result was to recognize the correct form of these intersections.

Date: 29 June 2003.
Rahim Moosa was partially supported by an NSERC postdoctoral fellowship.
Thomas Scanlon was partially supported by NSF Grant DMS-0071890.

The Mordell-Lang conjecture and related statements have model theoretic interpretations. On the face of it, the Mordell-Lang conjecture in its original form may be rephrased as *The structure induced on a finitely generated subgroup of a semiabelian variety of the complex numbers from the field structure is weakly normal.* Moreover, as Pillay showed, the finitely generated group is actually stably embedded. More precisely, if K is an algebraically closed field of characteristic zero and Γ is a finitely generated subgroup of the K-points of some semiabelian variety over K, then the theory of the structure $(K, +, \times, \Gamma)$ is stable and the formula "$x \in \Gamma$" is weakly normal [6]. As observed by the second author in [10] this result implies a version of uniformity for the Mordell-Lang conjecture.

The present paper addresses the question of determining the model theoretic properties of the structure induced on Γ by $(K, +, \times, \Gamma)$, when K is an algebraically closed field of positive characteristic and Γ is a finitely generated Frobenius submodule of a semiabelian variety defined over a finite field. As certain infinite Frobenius orbits may be definable in Γ, the induced structure cannot be weakly normal. However, we show that it is stable, and hence, as in Pillay [6], $(K, +, \times, \Gamma)$ is stable. As a consequence of this analysis we obtain a uniform version of the Mordell-Lang conjecture for semiabelian varieties over a finite field.

While the structure of integral points on semiabelian varieties defined over finite fields serves as motivation, we perform our technical work in the abstract setting of "F-structures". We work with cetain fixed finite simple extension R of $\mathbb{Z}$, which we denote by $\mathbb{Z}[F]$, and the class of finitely generated R-modules. For a finitely generated R-module M, an *F-set* will be a finite union of finite sums of points, submodules, and "F-cycles" (see Section 2 for the formal definitions). We prove quantifier elimination and stability for finitely generated R-modules with predicates for these F-sets. The key is a translation between properties of F-sets and of sets definable in the structure $(\mathbb{N}, 0, \sigma)$ where σ is the successor operation.

In the present paper we have restricted our attention to semiabelian varieties defined over finite fields. However, as might be expected, these results extend, via Hrushovski's theorem concerning the relative Mordell-Lang conjecture in positive characteristic, to semiabelian varieties defined over an arbitrary field of positive characteristic. In a sequel to this paper [5], the present authors describe the structure of the set of K-rational points on subvarieties of abelian varieties where K is a finitely generated field of positive characteristic.

Our collaboration on this paper began during the MSRI Model Theory of Fields program during the Spring of 1998. Both authors thank MSRI for providing excellent working conditions. We are also grateful to the referee for pointing out a mistake in an earlier version, and for many useful suggestions.

2. Preliminaries and Statement of Results

Throughout this paper R will denote a commutative ring, and $F \in R$ a distinguished element of R, satisfying the following conditions:

- $R = \mathbb{Z}[F]$ and F is integral over $\mathbb{Z}$;
- F is not a zero-divisor in R; and
- $\displaystyle\bigcap_{n=0}^{\infty} F^n R = \{0\}$.

The main consequence of our standing assumptions on R is contained in the following proposition:

Proposition 2.1. *If M is a finitely generated R-module, then $F^\infty M := \bigcap_{n=0}^{\infty} F^n M$ is a finite set.*

Proof. Let (F) be the ideal in R generated by F, let $\pi\colon R \to R/(F)$ be the quotient map, and let $N = F^\infty M$. As N is finitely generated, and $FN = N$, Nakayama's Lemma says that there is an $r \in R$ with $rN = 0$ and $\pi(r) = 1$.

We claim that r is not a zero-divisor. Indeed, suppose $sr = 0$ for some $s \neq 0$ in R. Then $0 = \pi(sr) = \pi(s)\pi(r) = \pi(s)$. Hence, $s \in (F)$. On the other hand, as $F^\infty R = 0$, $s = F^n t$ for some $n \geq 0$ and $t \in R \setminus (F)$. Hence, $F^n tr = 0$, and as F is not a zero divisor, $tr = 0$. But then, as before, $\pi(t) = 0$, implying that $t \in (F)$ – which is a contradiction.

It follows that $I = (r) \cap \mathbb{Z}$ is a nonzero ideal of $\mathbb{Z}$. Indeed, as R is a finite extension of $\mathbb{Z}$, r is integral over $\mathbb{Z}$. The minimal polynomial of r over $\mathbb{Z}$ must have a nonzero constant term, since r is not a zero-divisor. This constant term is visibly in $(r) \cap \mathbb{Z}$. Hence $\mathbb{Z}/I$ is a finite ring, and $R/(r)$, being a finitely generated $\mathbb{Z}/I$-module, is also a finite ring. Finally, as r kills N, N is a finitely generated $R/(r)$-module – and hence is itself a finite set. $\square$

Example 2.2. We describe our intended example.

Fix G a semiabelian variety over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. The group variety G admits an algebraic endomorphism $F : G \to G$ induced from the q-power Frobenius $x \mapsto x^q$. Let $R = \mathbb{Z}[F]$ be the (commutative) subring of the endomorphism ring of G, $\mathrm{End}(G)$, generated by F.

We check that F is integral over $\mathbb{Z}$. Over $\mathbb{F}_q^{\mathrm{alg}}$, G is an extension of an abelian variety by a cartesian power of the multiplicative group:

$$0 \longrightarrow \mathbb{G}_m^\mu \longrightarrow G \longrightarrow A \longrightarrow 0$$

Using the fact that there are no non-trivial algebraic homomorphisms from $\mathbb{G}_m^\mu$ to A, nor from A to $\mathbb{G}_m^\mu$, it is not hard to see that $\mathrm{End}(G)$ embeds into $\mathrm{End}(\mathbb{G}_m^\mu)\times\mathrm{End}(A)$. As both $\mathrm{End}(\mathbb{G}_m^\mu)$ and $\mathrm{End}(A)$ are finite extensions of $\mathbb{Z}$ (see VII.1 of [3] for the latter), it follows that $\mathrm{End}(G)$ is also. Hence F is integral over $\mathbb{Z}$.

Since F is injective on $G(\mathbb{F}_q^{\mathrm{alg}})$, it is not a zero-divisor. Finally, the only infinitely F-divisible element of R is the zero map. To see this, choose a finitely generated field extending $\mathbb{F}_q$, L, such that $G(L)$ is Zariski-dense in G (for example, take L to be the function field of G over $\mathbb{F}_q$). Every endomorphism in R is defined over L (in fact over $\mathbb{F}_q$). If $\alpha \in F^\infty R$, then $\alpha G(L) \subset \bigcap_{n>0} F^n G(L) = G(k)$, where $k := \bigcap_{n>0} L^{q^n}$ is a finite field. Hence α takes a Zariski-dense subgroup of G to a finite group. It follows that the kernel of α is of finite index in G, and as G is connected, α must be the zero map.

The finitely generated R-modules that we are interested in will appear as submodules $\Gamma \leq G(K)$, where K is a finitely generated regular field extension of $\mathbb{F}_q$. A particularly relevant case is when Γ is the set of rational or integral points on G. For example, if G is an abelian variety, then $G(K)$ is a finitely generated group by the Lang-Néron theorem (see 6.1 of [4]), and as it is closed under the Frobenius endomorphism, it is a finitely generated R-module. We can consider $\Gamma := G(K)$

itself. For semiabelian varieties, we can consider $\Gamma := G(\mathcal{R})$, where $\mathcal{R} \subset K$ is a finitely generated ring extension of $\mathbb{F}_q$. To see that $G(\mathcal{R})$ is a finitely generated group, it suffices to consider consider abelian varieties and the multiplicative group separately. The former is by Lang-Néron and for the latter see Corollary 2.7.3 of [4]. Notice that in all these cases $F^\infty\Gamma \leq G(\mathbb{F}_q)$, since finite generatedness and regularity imply that $\bigcap_{n>0} K^{q^n} = K \cap \mathbb{F}_q^{\mathrm{alg}} = \mathbb{F}_q$.

Definition 2.3. Fix a finitely generated R-module M.

An *F-cycle in M* is a set of the form

$$C(a;\delta) := \{a + F^\delta a + F^{2\delta}a + \cdots + F^{n\delta}a \colon n \in \mathbb{N}\},$$

where $a \in M$ and $0 < \delta \in \mathbb{N}$. For sums of F-cycles, we use the notation

$$C(a_1, \ldots, a_r; \delta_1, \ldots, \delta_r) := \sum_{i=1}^{r} C(a_i; \delta_i),$$

where $a_1, \ldots, a_r \in M$, and $\delta_1, \ldots, \delta_r \in \mathbb{N}$ with each $\delta_i > 0$. If it is the case that $\delta_1 = \cdots = \delta_r =: \delta$, then we abbreviate $C(a_1, \ldots, a_r; \delta_1, \ldots, \delta_r)$ by $C(a_1, \ldots, a_r; \delta)$.

An *F-set in M* is a finite union of sets of the form

$$b + C(a_1, \ldots, a_r; \delta_1, \ldots, \delta_r) + H,$$

where $b, a_1, \ldots, a_r \in M$, $\delta_1, \ldots, \delta_r \in \mathbb{N}$ with $\delta_i > 0$, and H is a submodule of M. We denote by $\mathcal{F}(M)$ the collection of all F-sets in M.

A *groupless F-set* is a finite union of sets of the form $b + C(a_1, \ldots, a_r; \delta_1, \ldots, \delta_r)$. We denote by $\mathrm{Groupless}(M)$ the collection of all groupless F-sets in M.

Finally, an *F-structure* is a pair $(M, \mathcal{F})$ where M is a finitely generated R-module and $\mathcal{F} := \bigcup_{n \geq 0} \mathcal{F}(M^n)$. We view $(M, \mathcal{F})$ as a first-order structure in the language where there is a predicate for each member of $\mathcal{F}$.

Here are the main results of this paper:

Theorem A. *The theory of an F-structure admits quantifier elimination and is stable* (Theorems 5.13 and 6.11, respectively).

We also obtain the following version of Mordell-Lang for semiabelian varieties over finite fields (this is Theorem 7.8). As in Example 2.2 we fix the following data: *G is a semiabelian variety over a finite field $\mathbb{F}_q$, $F \colon G \to G$ is the algebraic endomorphism induced by the q-power Frobenius map, $R = \mathbb{Z}[F]$ is the subring of the endomorphism ring of G generated by F, K is a finitely generated regular extension of $\mathbb{F}_q$, and $\Gamma \leq G(K)$ is a finitely generated R-submodule.*

Theorem B. *If $X \subseteq G$ is a closed subvariety, then $X(K) \cap \Gamma \in \mathcal{F}(\Gamma)$. Moreover, the submodules of Γ that appear are of the form $H(K) \cap \Gamma$ where $H \leq G$ is an algebraic subgroup over $\mathbb{F}_q$.*

Combining these, we conclude (this is Corollary 7.10):

Theorem C. *If $\mathcal{U}$ is an algebraically closed field extending K, then* $\mathrm{Th}(\mathcal{U}, +, \times, \Gamma)$ *is stable.*

As an application of our analysis, we also obtain the following uniform version of Theorem B (this is Corollary 7.15):

Theorem D. *Suppose $\{X_b\}_{b\in B}$ is an algebraic family of closed subvarieties of G. There are $A_1,\ldots,A_\ell \in \mathcal{F}(\Gamma)$ such that for any $b \in B$ there exist $I \subset \{1,\ldots,\ell\}$ and points $(\gamma_i)_{i\in I}$ from Γ, such that $X_b(K)\cap\Gamma = \bigcup_{i\in I}\gamma_i + A_i$.*

Remark 2.4. The assumption of regularity is not very restrictive. If $\Gamma \le G(\mathcal{U})$ is any finitely generated R-module, then there exists a finitely generated field extension $K'/\mathbb{F}_q$, such that $\Gamma \le G(K')$. Taking $r > 0$ such that $K' \cap \mathbb{F}_q^{\mathrm{alg}} = \mathbb{F}_{q^r}$, we have that K' is a regular extension of $\mathbb{F}_{q^r}$. Note that Γ can also be viewed as a $\mathbb{Z}[F^r]$-module. Replacing q with q^r, the above theorems apply.

In the remainder of this section we give an alternate description of groupless F-sets in terms of F-orbits rather than F-cycles. This will be useful to us in latter sections, and may also shed more light on the nature of F-sets.

Definition 2.5. Fix a finitely generated R-module M. An *F-orbit in M* is a set of the form $S(a;\delta) := \{F^{n\delta}a : n \in \mathbb{N}\}$, where $a \in M$ and $0 < \delta \in \mathbb{N}$. A *cycle-free groupless F-set* in M is a finite union of sets of the form

$$b + S(a_1,\ldots,a_r;\delta_1,\ldots,\delta_r),$$

where $b, a_1,\ldots,a_r \in M$, $\delta_1,\ldots,\delta_r \in \mathbb{N}$ with each $\delta_i > 0$, and where

$$S(a_1,\ldots,a_r;\delta_1,\ldots,\delta_r) := \sum_{i=1}^{r} S(a_i;\delta_i)$$

is used to denote sums of F-orbits. Again, if it is the case that $\delta_1 = \cdots = \delta_r =: \delta$, then we abbreviate $S(a_1,\ldots,a_r;\delta_1,\ldots,\delta_r)$ by $S(a_1,\ldots,a_r;\delta)$. We denote by Orb_M the collection of all cycle-free groupless F-sets in M.

Remark 2.6. As the terminology suggests, $\mathrm{Orb}_M \subset \mathrm{Groupless}(M)$. Indeed, one need only observe that for $a \in M$ and $\delta > 0$,

$$S(a;\delta) = \{a\} \cup a + C(F^\delta a - a;\delta).$$

Note that $\{a\} \in \mathrm{Groupless}(M)$, as, for example, $\{a\} = a + C(0;1)$.

Lemma 2.7. *Suppose M is a finitely generated R-module and $U \in \mathrm{Groupless}(M)$. There exists a finitely generated R-module M' extending M, such that $U \in \mathrm{Orb}_{M'}$.*

Proof. It is sufficient to do this for U an F-cycle. Suppose $U = C(b;\delta)$, where $b \in M$ and $\delta > 0$. We construct M' as follows. Let x be an indeterminate, and consider the free R-module generated by x over M, $N := M \oplus R\cdot x$. Let I be the R-submodule of N generated by the element $F^\delta x - x - b \in N$. Then $M' := N/I$, the quotient of N by I, is again a finitely generated R-module.

We claim that the natural embedding of M in N induces an embedding of M in M'. For this it is sufficient to show that $M \cap I = \{0\}$. Let $c \in M \cap I \subset N$. Then $c = r(F^\delta x - x - b)$, for some $r \in R$. This implies that $c + rb = (F^\delta r - r)x$, and hence $(F^\delta r - r)x \in M \cap (R\cdot x) = \{0\}$. It follows that $F^\delta r = r$, and so multiplication by F^δ in R fixes r. Hence $r \in F^\infty R$, which by our standing assumptions is $\{0\}$. In particular, $c = 0$, as desired.

Let $a \in M'$ be the image of x under the quotient map $N \to M'$. Then in M', $F^\delta a - a = b$. Hence, $C(b;\delta) = -a + S(F^\delta a;\delta)$. We have described an F-cycle as a cycle-free groupless F-set in the sense of M', as desired. $\square$

Remark 2.8. The construction of the finitely generated R-module M' in the above proof will appear again, and warrants a name. We say that M' is a *δ-splitting extension of M at b*. More generally, we say that *M' is obtained from M by a finite sequence of splitting extensions* if there are

$$M = M_0 \leq M_1 \leq \cdots \leq M_r = M',$$

where for $i \leq r-1$, M_{i+1} is a δ_i-splitting extension of M_i at b_i, for some $\delta_i > 0$ and $b_i \in M_i$.

That we do not pick up any additional structure in passing to these extensions is expressed by the following strengthening of Remark 2.6:

Lemma 2.9. *Suppose M is a finitely generated R-module and $N \leq M$ is a submodule. If $S \in \mathrm{Orb}_M$ and $S \subset N$, then $S \in \mathrm{Groupless}(N)$.*

Proof. Taking finite unions, we may assume that $S = b + S(\overline{a}; \overline{\delta})$ where $b \in M$, $\overline{a} = (a_1, \ldots, a_n) \in M^n$, and $\overline{\delta} = (\delta_1, \ldots, \delta_n) \in \mathbb{N}^n$. As in Remark 2.6, for each $i \leq n$, we may write $S(a_i; \delta_i) = \{a_i\} \cup a_i + C(F^{\delta_i} a_i - a_i; \delta_i)$. Hence

$$\begin{aligned} S &= b + \sum_{i=1}^{n} [\{a_i\} \cup a_i + C(F^{\delta_i} a_i - a_i; \delta_i)] \\ &= \bigcup_{I \subset \{1, \ldots, n\}} (b + a_1 + \cdots + a_n) + \sum_{i \in I} C(F^{\delta_i} a_i - a_i; \delta_i) \end{aligned}$$

Note, first of all, that $b + a_1 + \cdots + a_n \in S \subset N$. Moreover, for each $i \leq n$, $F^{\delta_i} a_i - a_i \in N$. Indeed,

$$b + a_1 + \cdots + a_{i-1} + F^{\delta_i} a_i + a_{i+1} + \cdots + a_n$$

and

$$b + a_1 + \cdots + a_{i-1} + a_i + a_{i+1} + \cdots + a_n$$

are visibly in $S \subset N$. Taking the difference of these two elements, we get that $F^{\delta_i} a_i - a_i \in N$. Hence $S \in \mathrm{Groupless}(N)$. □

Definition 2.10. Suppose M is a finitely generated R-module and $N \leq M$ is a submodule. Then Orb_M^N denotes the class of all cycle-free groupless F-sets in M that are contained in N.

As a consequence of Lemmas 2.7 and 2.9, we obtain that for any finitely generated R-module M,

$$\mathrm{Groupless}(M) = \bigcup_{M \leq M'} \mathrm{Orb}_{M'}^M,$$

where the union is taken over all finitely generated R-modules extending M. In this way, the study of groupless F-sets is to a large extent reduced to the study of cycle-free groupless F-sets.

Remark 2.11. In the above equality, we could have restricted this union to any collection, $\mathcal{M}$, of finitely generated R-modules extending M with the following property: For any $a_1, \ldots, a_r \in M$ and $\delta_1, \ldots, \delta_r > 0$, there is an $M' \in \mathcal{M}$ and $b_1, \ldots, b_r \in M'$ such that $F^{\delta_i} b_i - b_i = a_i$ for all $i \leq r$. For example, the class of all R-modules obtained from M by a finite sequence of splitting extensions.

3. Groupless F-sets and $(\mathbb{N}, 0, \sigma, P_\delta)$.

Our main tool for understanding cycle-free groupless F-sets will be a correspondence between them and a certain well-understood structure on the natural numbers, $\mathbb{N}$. For each $\delta > 0$, we can view $\mathbb{N}$ as a structure in the language $\mathcal{L}_\delta$ where there is a constant symbol for 0, a function symbol σ for the successor function, and a unary predicate $P_\delta(x)$ that signifies "$x \equiv 0 \operatorname{mod} \delta$". We say that a subset of $\mathbb{N}^n$ is *δ-definable* to mean that it is $\mathcal{L}_\delta$-definable.

While the model theory of $\mathrm{Th}(\mathbb{N}, 0, \sigma, P_\delta)$ is both straightforward and well-known, we were unable to find an appropriate reference in the literature. We have therefore included an appendix in which we discuss various properties of this theory. We will refer the reader to this appendix whenever some aspect of the model theory of $\mathrm{Th}(\mathbb{N}, 0, \sigma, P_\delta)$ is invoked.

We also consider the full structure on $\mathbb{N}$ given by all these predicates. To this end we set $\mathcal{L} = \bigcup_{\delta>0} \mathcal{L}_\delta$, and say that a subset of $\mathbb{N}^n$ is *definable* to mean that it is $\mathcal{L}$-definable. We will be interested mainly in sets definable by equations in $\mathcal{L}$.

Definition 3.1. By a *δ-equation* we mean a formula of the form
- $x \equiv q \operatorname{mod} \delta$, for some $0 \leq q < \delta$; or,
- $x = \sigma^r(y)$, for some $r \in \mathbb{N}$; or,
- $x = p$, for some $p \in \mathbb{N}$,

where x and y are (singleton) variables. By an *equation* we mean a δ-equation for some $\delta > 0$. A (δ-)*variety* in $\mathbb{N}^n$, is then the solution set to finitely many (δ-)equations in the variables $x_1, \ldots, x_n$. A translate of a (δ-)variety is called a (δ-)*basic set.* A (δ-)*closed* set is a finite union of (δ-)basic sets.

Remark 3.2. Suppose $\delta, \gamma, r > 0$ and $\delta = r\gamma$. Then every γ-definable (respectively γ-closed) set is a δ-definable (respectively δ-closed) set. Indeed, if $0 \leq q < \gamma$ then

$$x \equiv q \operatorname{mod} \gamma \iff \bigvee_{\ell=0}^{r-1} x \equiv (\ell\gamma + q) \operatorname{mod} \delta.$$

In particular, this shows that every definable (respectively closed) set is δ'-definable (respectively δ'-closed) for some $\delta' > 0$.

Remark 3.3. *The δ-closed sets are exactly the projections of the positive quantifier-free definable sets in $(\mathbb{N}, 0, \sigma, P_\delta)$. In particular, they are closed under unions, intersections, and projections.*

Proof. Suppose $B = \overline{r} + V$, where $\overline{r} = (r_1, \ldots, r_n) \in \mathbb{N}^n$ and $V \subset \mathbb{N}^n$ is a δ-variety. Note that V is a positive quantifier-free definable set. Now,

$$B = \overline{r} + V = \pi[\Gamma(\sigma^{\overline{r}}) \cap (V \times \mathbb{N}^n)],$$

where $\sigma^{\overline{r}} : \mathbb{N}^n \to \mathbb{N}^n$ is the map $(\sigma^{r_1}, \ldots, \sigma^{r_n})$, $\Gamma(\sigma^{\overline{r}}) \subset \mathbb{N}^n \times \mathbb{N}^n$ is the graph of $\sigma^{\overline{r}}$, and π is the projection $\pi(x_1, \ldots, x_n, y_1, \ldots, y_n) = (y_1, \ldots, y_n)$. We have expressed B as the projection of a positive quantifier-free definable set. It follows that every δ-closed set is the projection of a positive quantifier-free definable set. On the other hand, every positive quantifier-free definable set is δ-closed. Hence it remains to show that *δ-closed sets are preserved under projections.*

Without loss of generality, we may assume that $\delta = 1$ and work in $(\mathbb{N}, 0, \sigma)$. That is, we may ignore congruence conditions. Indeed, in the appendix we describe a definable bi-interpretation of $(\mathbb{N}, 0, \sigma, P_\delta)$ and $(\mathbb{N}, 0, \sigma)$ that takes δ-closed sets to 1-closed sets and vice-versa.[1] Moroever, if X is a definable set in $(\mathbb{N}, 0, \sigma, P_\delta)$, such that the set obtained by interpreting X in $(\mathbb{N}, 0, \sigma)$ and then re-interpreting it back in $(\mathbb{N}, 0, \sigma, P_\delta)$ is δ-closed, then X itself must have been δ-closed.[2] Since interpretations commute with projections, it does suffice to show that that 1-closed sets are preserved under projections.

We will show that for $V \subset \mathbb{N}^{n+1}$ and $\pi \colon \mathbb{N}^{n+1} \to \mathbb{N}^n$ the projection, if V is a variety then πV is basic. This will suffice. Fix co-ordinate variables $x_1, \ldots, x_n, y$ for $\mathbb{N}^{n+1}$ and assume $\pi V \neq \emptyset$. Choose a finite set of equations, Λ, defining V, such that the number, m, of equations in Λ that involve y is minimal. Clearly, if $m = 0$ then πV is a variety. We assume that $m > 0$.

Suppose Λ includes an equation of the form $y = p$ for some $p \in \mathbb{N}$. If Λ contains any other equation involving y, then that equation can either be removed or replaced by an equation not involving y, without changing V. By the minimality of m, this is the only equation in Λ that refers to y. But then, πV is clearly a variety. We may assume that no such equation appears in Λ. A similar argument allows us to assume that Λ also does not contain any equation of the form $y = \sigma^a(x_i)$ for some $a \in \mathbb{N}$ and $i \leq n$.

We are left to consider the case when Λ contains an equation $\sigma^a(y) = x_i$ for some $a \in \mathbb{N}$ and $i \leq n$. As before, the minimality of m ensures that this is the only equation in Λ that involves y. Let $\Theta = \Lambda \setminus \{\sigma^a(y) = x_i\}$, and let $W \subset \mathbb{N}^n$ be the variety defined by Θ. Then $\pi V = \{(r_1, \ldots, r_n) \in W \colon r_i \geq a\}$. We wish to show that such a set is basic. Let $J \subset \{1, \ldots, n\}$ be those indices $j \leq n$ such that Θ implies an equation of the form $\sigma^{b_j}(x_j) = x_i$ or $x_j = \sigma^{c_j}(x_i)$. As $i \in J$, J is non-empty. Note that if $k \notin J$, then Θ will not imply any equation relating x_k with some x_j for $j \in J$. We also observe that if for some $j \in J$, Θ implies that $x_j = p$ for some $p \in \mathbb{N}$, then Θ determines x_i also, and as πV is nonempty, every element of W must have ith coordinate $\geq a$. But then, $\pi V = W$ and we are done. Hence we may assume that no such equation is implied by Θ.

Let b be greatest with the property that for some $j \in J$, Θ implies $\sigma^b(x_j) = x_i$. Taking $j = i$ we see that $b \geq 0$. If $b \geq a$, then Θ must force $x_i \geq a$. Again, this means that $\pi V = W$ and we are done. Hence, we may assume that $0 \leq b < a$. Finally, for each $j \in J$, let $a_j = a - b$; and for each $k \notin J$, let $a_k = 0$. Then πV is the basic set $(a_1, \ldots, a_n) + W$. $\square$

We describe the relevance of these structures on $\mathbb{N}$ to groupless F-sets. Fix a finitely generated R-module M and a tuple $\overline{a} = (a_1, \ldots, a_n) \in M^n$. We set the following notation:

- For $B \subset \mathbb{N}^n$, $F^B\overline{a} := \{\sum_{i=1}^{n} F^{b_i} a_i \colon (b_1, \ldots, b_n) \in B\} \subset M$.
- For $\overline{r} = (r_1, \ldots, r_n) \in \mathbb{N}^n$, $F^{\overline{r}}\overline{a} := \sum_{i=1}^{n} F^{r_i} a_i \in M$.
- For $\overline{r}, \overline{s} \in \mathbb{N}^n$, $\overline{r}$ is *$\overline{a}$-equivalent* to $\overline{s}$, written $\overline{r} \sim_{\overline{a}} \overline{s}$, if $F^{\overline{r}}\overline{a} = F^{\overline{s}}\overline{a}$.
- For $b \in M$, $\log_{\overline{a}} b := \{\overline{r} \colon b = F^{\overline{r}}\overline{a}\} \subset \mathbb{N}^n$.

[1] See Proposition A.2.
[2] See Lemma A.5.

The set $\log_{\overline{a}} b$ describes the ways in which b can be written as sums of iterates of F applied to $a_1, \dots, a_n$. Note that $\sim_{\overline{a}}$ is an equivalence relation and that $\overline{r} \sim_{\overline{a}} \overline{s}$ if and only if $(\overline{r}, \overline{s}) \in \log_{(\overline{a}, -\overline{a})} 0$.

Suppose B is a variety defined by a single equation. Then it is of one of the following forms:

I $\{(m_1, \dots, m_n) \in \mathbb{N}^n \colon m_t \equiv q \bmod \delta\}$, for some $0 \le q < \delta$ and $t \le n$.
II $\{(m_1, \dots, m_n) \in \mathbb{N}^n \colon m_s = \sigma^r(m_t)\}$, for some $r \in \mathbb{N}$ and $s, t \le n$.
III $\mathbb{N}^t \times \{p\} \times \mathbb{N}^{n-t-1}$, for some $p \in \mathbb{N}$ and $t < n$.

Clearly, $F^B \overline{a}$ is then of the form (respectively):

I $S(a_1, \dots, a_{t-1}, F^q a_t, a_{t+1}, \dots, a_n; 1, \dots, 1, \delta, 1, \dots, 1)$.
II $S(a_1, \dots, a_{s-1}, F^r a_s + a_t, a_{s+1}, \dots, a_{t-1}, a_{t+1}, \dots, a_n; 1)$.
III $F^p a_t + S(a_1, \dots, a_{t-1}, a_{t+1}, \dots, a_n; 1)$.

Iterating this procedure, it is not hard to see that for any variety $B \subset \mathbb{N}^n$, $F^B \overline{a}$ is a cycle-free groupless F-set. Conversely, if $S = c + S(\overline{a}; \overline{\delta})$, for some $c \in M$, $\overline{a} \in M^n$, and $\overline{\delta} = (\delta_1, \dots, \delta_n)$, then $S = F^B(c, \overline{a})$, where $B \subset \mathbb{N}^{n+1}$ is the variety $\{(0, r_1, \dots, r_n) \colon r_i \equiv 0 \bmod \delta_i\}$. We have:

Lemma 3.4. *Suppose $S \subset M$. Then $S \in \mathrm{Orb}_M$ if and only if $S = \bigcup_{i=1}^{\ell} F^{B_i} \overline{a}_i$ for some sequence of tuples $\overline{a}_1, \dots, \overline{a}_\ell$ and closed sets $B_1, \dots, B_\ell$.*

Proof. This follows from the preceding discussion once we have observed that for translates $B_2 = \overline{r} + B_1$, $F^{B_2}(x_1, \dots, x_m) = F^{B_1}(F^{r_1} x_1, \dots, F^{r_n} x_m)$, and for unions $B = \bigcup_{i=1}^{l} B_i$, $F^B \overline{x} = \bigcup_{i=1}^{l} F^{B_i} \overline{x}$. □

Proposition 3.5. *Suppose M is a finitely generated R-module. Then for all $\overline{a} \in M^n$ and $b \in M$, $\log_{\overline{a}} b$ is closed. In particular, $\overline{a}$-equivalence is a definable equivalence relation on $\mathbb{N}^n$.*

The proof of Proposition 3.5 is somewhat technical and we delay it for the time being. In Theorem 4.3 below, we will not only prove that $\log_{\overline{a}} b$ is closed, but we will also describe how the set varies with b.

For the remainder of this section, we describe a number of consequences of this proposition, concentrating mainly on the behaviour of the class of groupless F-sets. The following remark is an immediate consequence of the definitions.

Remark 3.6. Suppose M and N are finitely generated R-modules and $f \colon M \to N$ is a surjective R-module homomorphism.

- If $A \in \mathrm{Orb}_M$ (respectively Groupless(M) or $\mathcal{F}(M)$), then $f(A) \in \mathrm{Orb}_N$ (respectively Groupless(N) or $\mathcal{F}(N)$).
- If $A \in \mathcal{F}(N)$, then $f^{-1}(A) \in \mathcal{F}(M)$.
- If $A \in \mathrm{Orb}_N$ (respectively Groupless(N)) then there exists $B \in \mathrm{Orb}_M$ (respectively Groupless(M)) with $f(B) = A$.

Lemma 3.7. *Suppose M is a finitely generated R-module.*

(a) Orb_M *is preserved under intersections.*
(b) *If $S \in \mathrm{Orb}_M$ and $N \le M$ is a submodule, then $S \cap N \in \mathrm{Orb}_M$.*

Proof. For part (a), suppose $S, T \in \mathrm{Orb}_M$. By Lemma 3.4, and taking finite unions, we may assume that $S = F^B \overline{a}$ and $T = F^C \overline{b}$, for some $\overline{a} \in M^n$, $\overline{b} \in M^m$, $B \subset \mathbb{N}^n$ closed, and $C \subset \mathbb{N}^m$ closed. But then $S \cap T = F^D \overline{a}$, where

$$D := \{\overline{r} \in B : \text{for some } \overline{s} \in C, (\overline{r}, \overline{s}) \in \log_{(\overline{a}, -\overline{b})} 0\}.$$

By Proposition 3.5, $\log_{(\overline{a},-\overline{b})} 0$ is closed. As closed sets are preserved under intersections and projections, D is a closed set. Hence $F^D\overline{a} \in \mathrm{Orb}_M$.

For part (b), we may again assume $S = F^B\overline{a}$ for some $\overline{a} \in M^n$ and closed $B \subset \mathbb{N}^n$. Let $\pi\colon M \to M/N$ be the quotient map. Then $c \in S \cap N$ if and only if $\pi(c) = 0$ and $c = F^{\overline{r}}\overline{a}$ for some $\overline{r} \in B$. But then $0 = F^{\overline{r}}\pi(\overline{a})$. Hence $S \cap N = F^{(B\cap Z)}\overline{a}$, where $Z := \log_{\pi(\overline{a})} 0$. By Proposition 3.5 applied to M/N, we have that $Z \subset \mathbb{N}^n$ is closed. Hence $S \cap N \in \mathrm{Orb}_M$. □

Corollary 3.8. *Suppose M is a finitely generated R-module.*

(a) $\mathrm{Groupless}(M)$ *is preserved under intersections.*
(b) *If $U \in \mathrm{Groupless}(M)$ and N is a submodule, then $U \cap N \in \mathrm{Groupless}(N)$.*

Proof. We first go up and then come back down. Suppose $U, V \in \mathrm{Groupless}(M)$. Using Lemma 2.7, let M' be a finitely generated R-module that extends M, and such that $U, V \in \mathrm{Orb}_{M'}$. Then by part (a) of Lemma 3.7, $U \cap V \in \mathrm{Orb}_{M'}$. As $U \cap V \subset M$, we have by Lemma 2.9, that $U \cap V \in \mathrm{Groupless}(M)$.

For part (b), let M' be a finitely generated R-module that extends M, and such that $U \in \mathrm{Orb}_{M'}$. Now N is also a submodule of M', and so by part (b) of Lemma 3.7, $U \cap N \in \mathrm{Orb}_{M'}$, and hence in $\mathrm{Groupless}(N)$ by Lemma 2.9. □

Proposition 3.9. *Suppose M is a finitely generated R-module.*

(a) $\mathcal{F}(M)$ *is preserved under intersections.*
(b) *If $X \in \mathcal{F}(M)$ and $N \leq M$ is a submodule, then $X \cap N \in \mathcal{F}(N)$.*

Proof. For part (a), it suffices to show that if $U, V \in \mathrm{Groupless}(M)$ and $G, H \leq M$ are submodules, then $(U + G) \cap (V + H) \in \mathcal{F}(M)$. We proceed by a series of increasingly more general cases. Note that Case 2, below, implies part (b).

Case 1*:* $\underline{V = 0 \text{ and } G \cap H = 0}$. Notice that

$$(U + G) \cap H = [(U \cap (G + H)) + G] \cap H.$$

As $G + H \cong G \oplus H$, we have a projection map $\eta\colon G + H \to H$. Moreover,

$$[(U \cap (G + H)) + G] \cap H = \eta(U \cap (G + H)).$$

By part (b) of Corollary 3.8, $U \cap (G + H) \in \mathrm{Groupless}(G + H)$. Hence

$$(U + G) \cap H = \eta(U \cap (G + H)) \in \mathrm{Groupless}(H) \subset \mathcal{F}(M).$$

Case 2*:* $\underline{V = 0}$. Let $\pi\colon M \to M/(G \cap H)$ be the quotient map. Then

$$(U + G) \cap H = \pi^{-1}\pi[(U + G) \cap H] = \pi^{-1}[(\pi U + \pi G) \cap \pi H].$$

Now $\pi U \in \mathrm{Groupless}(M/(G \cap H))$. By case 1, $(\pi U + \pi G) \cap \pi H \in \mathrm{Groupless}(\pi H)$. It follows that $(U + G) \cap H \in \mathcal{F}(H)$. This proves part (b) of the proposition, as well as part (a) for this case.

Case 3*:* *The general case*. Note that $(U + G) \cap (V + H)$ is the projection onto the first coordinate of $[(U + G) \times (V + H)] \cap \Delta \subset M^2$ where Δ is the diagonal. On the other hand, it is not hard to see that $(U + G) \times (V + H) = (U \times V) + (G \times H)$, and that $U \times V \in \mathrm{Groupless}(M^2)$. By case 2, $[(U \times V) + (G \times H)] \cap \Delta$ is in $\mathcal{F}(M^2)$. Hence $(U + G) \cap (V + H) \in \mathcal{F}(M)$. □

We describe a class of quantifier-free definable sets, more general than F-sets, to which these methods apply.

Definition 3.10. A *generalised groupless F-set* is a finite union of sets of the form $U \setminus V$ where $U, V \in \text{Groupless}(M)$. We denote by $\text{Groupless}^*(M)$ the collection of all generalised groupless F-sets. A *generalised F-set* is a finite union of sets of the form $A + H$, where $A \in \text{Groupless}^*(M)$ and $H \leq M$ is a submodule. The class of generalised F-sets is denoted by $\mathcal{F}^*(M)$.

Remark 3.11. Corollary 3.8 implies:

- $\text{Groupless}^*(M)$ is preserved under unions and intersections.
- If $A, B \in \text{Groupless}^*(M)$ then so is $A \setminus B$.
- If $N \leq M$ and $A \in \text{Groupless}^*(M)$, then $A \cap N \in \text{Groupless}^*(N)$.

Proposition 3.12. *Suppose M is a finitely generated R-module and $A \subset M$. Then $A \in \text{Groupless}^*(M)$ if and only if there is a finitely generated R-module M' extending M, tuples $\overline{a}_1, \dots, \overline{a}_\ell$ from M', and $\mathcal{L}$-definable sets $Y_1, \dots, Y_\ell$, such that $A = \bigcup_{i=1}^{\ell} F^{Y_i}\overline{a}_i$.*

Proof. We begin with the right-to-left direction. Taking finite unions, we may assume that $A = F^Y\overline{a}$ where $Y \subset \mathbb{N}^n$ is definable and $\overline{a} \in (M')^n$, where M' is a fixed finitely generated R-module extending M. As $A \subset M$, it is sufficient to prove that $A \in \text{Groupless}^*(M')$. Let $\delta > 0$ be such that both Y and $\overline{a}$-equivalence are δ-definable (we are applying Proposition 3.5 to M' here). We work in the structure $(\mathbb{N}, 0, \sigma, P_\delta)$. As pointed out in the appendix, this structure is of finite Morley rank (in fact of rank 1).[3] We proceed by induction on $(\text{RM}, \text{dM})(Y)$, the case of $\text{RM}\, Y = 0$ being trivial. We can write Y as $B \setminus Z$ where $B \subset \mathbb{N}^n$ is δ-closed, $Z \subset B$ is δ-definable, and $(\text{RM}, \text{dM})(B) = (\text{RM}, \text{dM})(Y)$.[4] It follows that $(\text{RM}, \text{dM})(Z) < (\text{RM}, \text{dM})(Y)$.

Let $X \subset Z$ be the set

$$X := \{\overline{r} \in Z : \text{if } \overline{s} \in B \text{ and } \overline{s} \sim_{\overline{a}} \overline{r} \text{ then } \overline{s} \in Z\}.$$

Then $A = F^B\overline{a} \setminus F^X\overline{a}$. Indeed, $F^Y\overline{a} \subset F^B\overline{a} \setminus F^X\overline{a}$ is clear from the definition of X. For the other direction suppose $b \in F^B\overline{a} \setminus F^X\overline{a}$. In particular, $b = F^{\overline{r}}\overline{a}$ for some $\overline{r} \in B \setminus X$. If $\overline{r} \in B \setminus Z = Y$ then $b \in A$ as desired. If not, then $\overline{r} \in Z \setminus X$. By the definition of X, there is $\overline{s} \in B$ with $\overline{s} \sim_{\overline{a}} \overline{r}$, and $\overline{s} \notin Z$. It follows that $b = F^{\overline{r}}\overline{a} = F^{\overline{s}}\overline{a} \in F^Y\overline{a} = A$.

Now, X is δ-definable and $(\text{RM}, \text{dM})(X) < (\text{RM}, \text{dM})(Y)$. By induction, we have $F^X\overline{a} \in \text{Groupless}^*(M')$. As B is closed, $F^B\overline{a} \in \text{Orb}_{M'} \subset \text{Groupless}^*(M')$. Hence $A = F^B\overline{a} \setminus F^X\overline{a} \in \text{Groupless}^*(M')$.

For the converse, taking finite unions, we may assume that $A = U \setminus V$, where $U, V \in \text{Groupless}(M)$. Let M' be a finitely generated R-module extending M, such that $U, V \in \text{Orb}_{M'}$. Taking finite unions again, and applying Lemma 3.4, we may assume that $U = F^B\overline{a}$ and $V = \bigcup_{i=1}^{m} F^{C_i}\overline{b}_i$ where $\overline{a}, \overline{b}_1, \dots, \overline{b}_m$ are tuples from M' and $B, C_1, \dots, C_m$ are closed sets. But then $A = F^Y\overline{a}$, where

$$Y := \{\overline{r} \in B : \bigwedge_{i=1}^{m} \forall \overline{s} \in C_i, (\overline{r}, \overline{s}) \notin \log_{(\overline{a}, -\overline{b}_i)} 0\}.$$

[3] See Propositions A.1 and A.2.

[4] See Proposition A.6, which is a uniform version of this.

Y is visibly definable, and this completes the proof of the proposition. □

Remark 3.13. In the above proposition, we could have taken M' to be obtained from M by a finite sequence of splitting extensions.

We wish to use Proposition 3.12 to prove that, like F-sets, the class of generalised F-sets is preserved under images and preimages of surjective R-module homomorphisms. We begin with a lemma.

Lemma 3.14. *Let $f\colon M_1 \to M_2$ be a surjective R-module homomorphism between finitely generated R-modules, $a \in M_1$, $f(a) = b$, and $\delta > 0$. Suppose M_1' is the δ-splitting extension of M_1 at a and M_2' is the δ-splitting extension of M_2 at b. Then there is a natural surjective R-module homomorphism $f'\colon M_1' \to M_2'$ that extends f, and such that* $\ker f' = \ker f$.

Proof. Recall that $M_1' := (M_1 \oplus R\cdot x)/R\cdot(F^\delta x - x - a)$, where x is an indeterminate. This was defined in Remark 2.8 and appears in the proof of Lemma 2.7. It was shown in that lemma that the natural inclusion of $M_1 \subset M_1 \oplus R \cdot x$ induces an inclusion of $M_1 \subset M_1'$. Similarly, $M_2' := (M_2 \oplus R \cdot y)/R \cdot (F^\delta y - y - b)$. Clearly, we can lift f to $\hat{f}\colon M_1 \oplus R \cdot x \to M_2 \oplus R \cdot y$, by $x \mapsto y$, with $\ker \hat{f} = \ker f$. As $\hat{f}$ maps $R \cdot (F^\delta x - x - a)$ onto $R \cdot (F^\delta y - y - b)$, it descends to a map $f'\colon M_1' \to M_2'$ that is surjective and extends f. On the other hand,

$$(\hat{f})^{-1}[R \cdot (F^\delta y - y - b)] = R \cdot (F^\delta x - x - a) + \ker \hat{f} = R \cdot (F^\delta x - x - a) + \ker f$$

Hence, $\ker f' = \ker f$. □

Proposition 3.15. *Suppose $f\colon M_1 \to M_2$ is a surjective R-module homomorphism of finitely generated R-modules. The class of generalised F-sets is preserved under images and preimages of f.*

Proof. Suppose $A \in \mathrm{Groupless}^*(M_1)$ and $H \leq M_1$. We want to show that $f(A+H)$ is a generalised F-set in M_2. As $f(A + H) = f(A) + f(H)$, it suffices to show that $f(A) \in \mathrm{Groupless}^*(M_2)$. By Proposition 3.12, and taking finite unions, we may assume that $A = F^Y\overline{a}$, where $Y \subset \mathbb{N}^n$ is definable and $\overline{a} \in (M_1')^n$, for some M_1' that is obtained from M_1 by a finite sequence of splitting extensions. Iterating Lemma 3.14 we obtain M_2' extending M_2, and a lifting of f to a surjective R-module homomorphism $f'\colon M_1' \to M_2'$. Then $f'(A) = F^Y f'(\overline{a})$. But as f' lifts f, we have that $f'(A) = f(A)$. So by Proposition 3.12 again, $f(A) \in \mathrm{Groupless}^*(M_2)$.

We now check preimages. Suppose $A \in \mathrm{Groupless}^*(M_2)$ and $H \leq M_2$. We may again assume that $A = F^Y\overline{b}$, where Y is definable and $\overline{b}$ is a tuple from a finitely generated R-module obtained from M_2 by a finite sequence of splitting extensions, M_2'. Let M_1' extend M_1, and let $f'\colon M_1' \to M_2'$ be a surjective lifting of f such that $\ker f' = \ker f$ (using Lemma 3.14). Let $\overline{a}$ from M_1' be such that $f'(\overline{a}) = \overline{b}$. We claim that

$$f^{-1}(A + H) = (F^Y\overline{a} \cap M_1) + f^{-1}(H).$$

Right-to-left containment is clear from the fact that f' extends f. For the converse note that $f'^{-1}(H) = f^{-1}(H) + \ker f' = f^{-1}(H) + \ker f = f^{-1}(H)$. Hence

$$f'^{-1}(F^Y\overline{b} + H) = F^Y\overline{a} + f'^{-1}(H) = F^Y\overline{a} + f^{-1}(H).$$

As $f^{-1}(A + H) \subset M_1$, it follows that

$$f^{-1}(A + H) \subset [F^Y\overline{a} + f^{-1}(H)] \cap M_1 = (F^Y\overline{a} \cap M_1) + f^{-1}(H).$$

So $f^{-1}(A+H) = (F^Y\overline{a} \cap M_1) + f^{-1}(H)$. As $F^Y\overline{a} \in \mathrm{Groupless}^*(M_1')$, Corollary 3.8 implies that $F^Y\overline{a} \cap M_1 \in \mathrm{Groupless}^*(M_1)$, and so $f^{-1}(A+H) \in \mathcal{F}^*(M_1)$. $\square$

It is visible from the definitions that a generalised *groupless* F-set is a boolean combination of groupless F-sets, and hence quantifier-free definable. This is not immediately obvious for generalised F-sets that are not groupless. Nevertheless,

Corollary 3.16. *Every generalised F-set in a cartesian power of M is quantifier-free definable in $(M, \mathcal{F})$.*

Proof. Suppose $A \in \mathrm{Groupless}^*(M^n)$ and $H \leq M^n$ is a submodule. It suffices to show that $A + H$ is a boolean combination of sets from $\mathcal{F}(M^n)$. Consider the quotient map $\pi\colon M^n \to M^n/H$. By (the proof of) Proposition 3.15, πA is in $\mathrm{Groupless}^*(M^n/H)$. Hence, πA is a boolean combination of groupless F-sets in M^n/H. But $A+H = \pi^{-1}\pi A$. The corollary now follows from Remark 3.6 together with the fact that π^{-1} commutes with boolean operations. $\square$

Proposition 3.17. *Suppose M is a finitely generated R-module.*

(a) *$\mathcal{F}^*(M)$ is preserved under intersections.*
(b) *If $X \in \mathcal{F}^*(M)$ and $N \leq M$ is a submodule, then $X \cap N \in \mathcal{F}^*(N)$.*

Proof. This follows exactly as in the analogous statement for $\mathcal{F}(M)$ (Proposition 3.9). One uses Remark 3.11 instead of Corollary 3.8, and the fact that the class of generalised F-sets is also preserved under images and preimages of surjective R-module homomorphisms (Proposition 3.15). $\square$

4. Uniform Definability of Logarithmic Equivalence

Fix a finitely generated R-module M. In this section, we aim to give a uniform description of $\log_{\overline{a}} b$, which will in particular prove Proposition 3.5. In order to do so, it is convenient to distinguish certain kinds of translates of sets in $\mathbb{N}$:

Definition 4.1. A tuple $\overline{r} \in \mathbb{N}^n$ is called *disjoint from a set* $B \subset \mathbb{N}^n$ if for all $i \leq n$, if the ith coordinate of $\overline{r}$ is nonzero then every element of B has zero as its ith coordinate. In this case, we write $\overline{r} \oplus B$ to mean the translate $\overline{r} + B$. We call $\overline{r} \oplus B$ a *disjoint-translate* of B.

Let $\overline{a} \in M^n$, $\overline{r} \in \mathbb{N}^n$, and $B \subset \mathbb{N}^n$ closed. The purpose of introducing disjoint-translates is that if $\overline{r} \oplus B$ is a disjoint-translate of B, then we have a particularly simple description of $F^{(\overline{r}\oplus B)}\overline{a}$ in terms of $F^B\overline{a}$. Let $I_B \subset \{1, \dots, n\}$ be the *support of B* – that is, those indices $i \leq n$ such that some element of B has a nonzero ith coordinate. We employ the following notation.

$B^\circ \subset \mathbb{N}^{|I_B|}$ is the projection of B onto the I_B-coordinates;
$\overline{a}^\circ \in M^{|I_B|}$ is the projection of $\overline{a}$ onto the I_B-coordinates;
$\overline{a}_\circ \in M^{(n-|I_B|)}$ is the projection of $\overline{a}$ onto the $(\{1, \dots, n\} \setminus I_B)$-coordinates;
$\overline{r}_\circ \in \mathbb{N}^{(n-|I_B|)}$, is the projection of $\overline{r}$ onto the $(\{1, \dots, n\} \setminus I_B)$-coordinates;

After permuting the indices, $\overline{r} \oplus B$ is just $\overline{r}_\circ \times B^\circ$. In fact, we have:

$$F^{(\overline{r}\oplus B)}\overline{a} = F^{\overline{r}_\circ}\overline{a}_\circ + F^{B^\circ}\overline{a}^\circ.$$

Notice that $F^{B^\circ}\overline{a}^\circ$ depends on B and $\overline{a}$, but not on $\overline{r}$. Only the point by which $F^{B^\circ}\overline{a}^\circ$ is being translated depends on $\overline{r}$. That is, as you disjoint-translate a closed set, the groupless F-sets that you obtain only vary by translation. We often refer to $B^\circ, \overline{a}^\circ$ as the *canonical contraction* of $B, \overline{a}$ and the expression $F^{\overline{r}_\circ}\overline{a}_\circ + F^{B^\circ}\overline{a}^\circ$ as the *canonical form* of $F^{(\overline{r}\oplus B)}\overline{a}$.

Another advantage of disjoint-translates is that they form a uniformly definable family of sets. Since we do not have "+" in our language $\mathcal{L}$, arbitrary translations of a definable set do *not* form a uniformly definable family. The following lemma says that every uniformly definable family of varieties is essentially of this form.

Lemma 4.2. *Suppose $\delta > 0$ and $V \subset \mathbb{N}^{m+n}$ is a δ-variety. There is a δ-variety $W \subset \mathbb{N}^n$ such that for all $\overline{r} \in \mathbb{N}^m$, $V_{\overline{r}}$ is either empty or a disjoint-translate of W.*

Proof. Let us use $x_1, \ldots, x_m, y_1, \ldots, y_n$ as coordinate variables for $\mathbb{N}^{m+n}$. Rearrange the coordinates so that for some $0 \leq \ell \leq n$ the equations defining V imply a condition of the form $y_i = \sigma^t(x_j)$ or $x_j = \sigma^t(y_i)$ for some $j \leq m$, if and only if $i \leq \ell$. We have that either $V_{\overline{r}} = \emptyset$ or $V_{\overline{r}} = \overline{s} \times W'$, where $\overline{s} \in \mathbb{N}^\ell$ varies with $\overline{r}$ and $W' \subset \mathbb{N}^{n-\ell}$ is a fixed δ-variety. Then $W = \{0\}^\ell \times W'$ satisfies the conclusion of the lemma. □

In any case, we aim to prove the following:

Theorem 4.3. *Suppose M is a finitely generated R-module. There exists a positive integer $\delta_M > 0$ such that the following holds: Suppose $\overline{a} = (a_1, \ldots a_n) \in M^n$. There are δ_M-basic sets $B_1, \ldots, B_\ell$ in $\mathbb{N}^n$, such that for all $b \in M$, there is some $J \subset \{1, \ldots, \ell\}$, and for each $j \in J$ there is some $\overline{r}_j \in \mathbb{N}^n$ disjoint from B_j, such that*

$$\log_{\overline{a}} b = \bigcup_{j \in J} (\overline{r}_j \oplus B_j).$$

We first explain what δ_M will be. Let $K = \bigcup_n \ker F^n$. Note that $FK \subset K$, and hence K is a submodule of M. Moreover, if $F(c) \in K$ then $c \in K$. As M is finiteley generated and R is Noetherian, K is finitely generated. Hence $K = \ker F^{N_1}$ for some $N_1 \geq 0$. It follows that F is injective on $F^\infty M$. Indeed, if $c \in F^\infty M$, then we can write $c = F^{N_1}b$ for some $b \in M$. Now, if $Fc = 0$ then $b \in \ker F^{N_1+1} \subset \ker F^{N_1}$, and hence $c = 0$. As $F^\infty M$ is a finite set, it follows that some positive power of F must fix $F^\infty M$ pointwise. From now on, given a finitely generated R-module M, δ_M will be the least positive integer such that F^{δ_M} fixes $F^\infty M$ pointwise.

Our proof of the theorem will proceed via a series of lemmas. For each $i \geq 0$, let $M_i = K + F^i M$. These are the points that are F^i divisible modulo K. We obtain a filtration of M, and define M_ω to be the intersection of this descending chain of R-submodules:

$$M_0 = M \supset M_1 \supset M_2 \supset \cdots \supset M_\omega = \bigcap_{n=0}^{\infty} M_n$$

This in turn induces a valuation on M, $v \colon M \to \omega + 1$, given by $v(x) \geq n$ if and only if $x \in M_n$.

Lemma 4.4. *For all $x \in M$, $v(Fx) = 1 + v(x)$.*

Proof. This is clear if $v(x) = \omega$ (i.e., if $x \in M_\omega$). Assume $v(x) = m < \omega$. Let $y \in M$ and $\alpha \in K$ be such that $x = F^m y + \alpha$. Then $Fx = F^{m+1}y + F\alpha$, and hence $v(Fx) \geq m + 1$. Now suppose that $v(Fx) > m + 1$. That is, there exists $z \in M$ and $\beta \in K$, such that $Fx = F^{m+2}z + \beta$. Hence $F^{m+1}y + F\alpha = F^{m+2}z + \beta$, and so

$F^{m+1}(y - Fz) \in K$. Hence $y - Fz \in K$. That is, $y = Fz + \theta$ for some $\theta \in K$. It follows that $x = F^{m+1}z + F^m\theta + \alpha \in M_{m+1}$, contradicting $v(x) = m$. □

Lemma 4.5. *Suppose $a_1, \ldots, a_t \in M \setminus M_\omega$. If $k_1, \ldots, k_t \in \mathbb{N}$ satisfy $k_j - k_1 > v(a_1)$ for all $j > 1$, then $v(\sum_{i=1}^t F^{k_i} a_i) = k_1 + v(a_1)$.*

Proof. Notice that for each $j > 1$,

$$v(F^{k_j} a_j) = k_j + v(a_j) > k_1 + v(a_1) + v(a_j) \geq k_1 + v(a_1) = v(F^{k_1} a_1).$$

The lemma now follows from the fact that the valuation of a sum is the unique minimum valuation of the summands (if such a unique minimum exists). □

Lemma 4.6. *Suppose $a_1, \ldots, a_t \in M \setminus M_\omega$. There exists $N > 0$ such that for all $k_1 < \cdots < k_t$, and $\ell_1, \ldots, \ell_t$ from $\mathbb{N}$ satisfying*

(a) *$k_1 > N$ and $k_i - k_{i-1} > N$ for all $1 < i \leq t$; and,*
(b) *$\ell_i > N$, and $|\ell_i - \ell_j| > N$ for all $i \neq j$ from $\{1, \ldots, t\}$;*

if

$$\sum_{i=1}^{t} F^{k_i} a_i = (\sum_{i=1}^{t} F^{\ell_i} a_i) \operatorname{mod} M_\omega,$$

then for some permutation σ of $\{1, \ldots, t\}$, and for each $i \leq t$,

$$F^{\ell_{\sigma(i)}} a_{\sigma(i)} - F^{k_i} a_i \in M_\omega.$$

In particular, $k_i + v(a_i) = \ell_{\sigma(i)} + v(a_{\sigma(i)})$ for all $i \leq t$.

Proof. For the "in particular" clause notice that $F^{\ell_{\sigma(i)}} a_{\sigma(i)} - F^{k_i} a_i \in M_\omega$ implies that the two summands must have the same value, and so by Lemma 4.4 we must have that $k_i + v(a_i) = \ell_{\sigma(i)} + v(a_{\sigma(i)})$.

Now let $m := \max\{v(a_i) \colon i \leq t\}$ and let

$$N := \max\{m, v(F^{m-v(a_i)} a_i - F^{m-v(a_j)} a_j) \colon \\ i, j \text{ such that } F^{m-v(a_i)} a_i - F^{m-v(a_j)} a_j \notin M_\omega\}$$

Suppose $k_1, \ldots, k_t, \ell_1, \ldots, \ell_t$ satisfy the hypotheses of the Lemma, and let σ be a permutation of $\{1, \ldots, t\}$ so that $\ell_{\sigma(1)} < \cdots < \ell_{\sigma(t)}$.

We will show that this σ and N work. We show it by induction on t: the case of $t = 1$ is obvious and we assume that $t \geq 2$. We claim it is sufficient to show that $F^{\ell_{\sigma(1)}} a_{\sigma(1)} - F^{k_1} a_1 \in M_\omega$. Indeed, this implies that

$$\sum_{i=2}^{t} F^{k_i} a_i = (\sum_{i=2}^{t} F^{\ell_{\sigma(i)}} a_{\sigma(i)}) \operatorname{mod} M_\omega,$$

and so by induction $F^{\ell_{\sigma(i)}} a_{\sigma(i)} - F^{k_i} a_i \in M_\omega$ for $i = 2, \ldots, t$, and we are finished. Assume $F^{\ell_{\sigma(1)}} a_{\sigma(1)} - F^{k_1} a_1 \notin M_\omega$ and seek a contradiction.

Note that by Lemma 4.5, our choice of N, and our choice of σ, we already know that $k_1 + v(a_1) = \ell_{\sigma(1)} + v(a_{\sigma(1)})$. Using this we compute:

$$\begin{aligned} F^{\ell_{\sigma(1)}} a_{\sigma(1)} - F^{k_1} a_1 &= F^{\ell_{\sigma(1)} + v(a_{\sigma(1)}) - m} (F^{m - v(a_{\sigma(1)})} a_{\sigma(1)}) - F^{k_1} a_1 \\ &= F^{k_1 + v(a_1) - m} (F^{m - v(a_{\sigma(1)})} a_{\sigma(1)}) - F^{k_1} a_1 \\ &= F^{k_1 + v(a_1) - m} (F^{m - v(a_{\sigma(1)})} a_{\sigma(1)} - F^{m - v(a_1)} a_1) \end{aligned}$$

Evaluating both sides we get that

$$v(F^{\ell_{\sigma(1)}}a_{\sigma(1)} - F^{k_1}a_1) = k_1 + v(a_1) - m + v(F^{m-v(a_{\sigma(1)})}a_{\sigma(1)} - F^{m-v(a_1)}a_1).$$

Now, since we are assuming that $F^{\ell_{\sigma(1)}}a_{\sigma(1)} - F^{k_1}a_1 \notin M_\omega$ this gives

$$v(F^{\ell_{\sigma(1)}}a_{\sigma(1)} - F^{k_1}a_1) \leq k_1 + v(a_1) - m + N < k_2 + v(a_1) - m \leq k_2$$

We also have that

$$k_1 + v(a_1) - m + N = \ell_{\sigma(1)} + v(a_{\sigma(1)}) - m + N \leq \ell_{\sigma(1)} + N < \ell_{\sigma(2)}.$$

We have shown that $v(F^{\ell_{\sigma(1)}}a_{\sigma(1)} - F^{k_1}a_1) < k_2, \ell_{\sigma(2)}$. Note that

$$\sum_{i=2}^{t} F^{k_i}a_i - \sum_{i=2}^{t} F^{\ell_{\sigma(i)}}a_{\sigma(i)} = (F^{\ell_{\sigma(1)}}a_{\sigma(1)} - F^{k_1}a_1) \bmod M_\omega,$$

and so $v(\sum_{i=2}^{t} F^{k_i}a_i - \sum_{i=2}^{t} F^{\ell_{\sigma(i)}}a_{\sigma(i)}) = v(F^{\ell_{\sigma(1)}}a_{\sigma(1)} - F^{k_1}a_1) < k_2, \ell_{\sigma(2)}$. On the other hand, $v(\sum_{i=2}^{t} F^{k_i}a_i - \sum_{i=2}^{t} F^{\ell_{\sigma(i)}}a_{\sigma(i)})$ is greater than or equal to the minimum value of its summands, each of which $\geq k_2, \ell_{\sigma(2)}$. This contradiction proves the lemma. □

The following lemma is a special case of Theorem 4.3.

Lemma 4.7. *Let $a_1, \ldots, a_n \in M_\omega$. There exist δ_M-basic sets $B_1, \ldots, B_\ell \subset \mathbb{N}^n$, such that for all $b \in M$, there is some $J \subset \{1, \ldots, \ell\}$ and for each $j \in J$ there is some $\overline{r}_j \in \mathbb{N}^n$ disjoint from B_j, such that $\log_{\overline{a}} b = \bigcup_{j \in J}(\overline{r}_j \oplus B_j)$.*

Proof. Let us first deal with the case when each $a_i \in F^\infty M$. Recall that F^{δ_M} fixes $F^\infty M$ pointwise. So for all $m \in \mathbb{N}$, $F^m a_i = F^{(m'\delta_M + r)}a_i = F^r a_i$ where $r \in \mathbb{N}$ is strictly less than δ_M and $m' \in \mathbb{N}$. Hence, if $\overline{m} \in \log_{\overline{a}} b$, then there exists $\overline{r}_\circ \in \log_{\overline{a}} b$ each of whose coordinates are strictly less than δ_M, and $\overline{m} = \overline{m}'(\delta_M, \ldots, \delta_M) + \overline{r}_\circ$ for some $\overline{m}' \in \mathbb{N}^n$. Moreover, for all $\overline{m}' \in \mathbb{N}^n$, $\overline{m}'(\delta_M, \ldots, \delta_M) + \overline{r}_\circ \in \log_{\overline{a}} b$. That is, $B(\overline{r}_\circ) := \overline{r}_\circ + \{\overline{n} \in \mathbb{N}^n : \overline{n} \equiv 0 \bmod \delta_M\}$ is contained in $\log_{\overline{a}} b$. Note that $B(\overline{r}_\circ)$ is a δ_M-basic set. Now, the collection $\{B(\overline{r})\}$ as $\overline{r}$ varies among all n-tuples each of whose coordinates are strictly less than δ_M, is finite (independently of b) and covers all of $\mathbb{N}^n$. It follows that $\log_{\overline{a}} b$ is equal to the union of some of these $B(\overline{r})$'s, and we have proved the lemma in this case.

Consider the general case (where each a_i is only assumed to be in M_ω). Let $N_1 \in \mathbb{N}$ be such that $K = \ker F^{N_1}$. For all $a \in M_\omega$, $F^{N_1}a \in F^\infty M$. Now those elements of $\overline{m} \in \log_{\overline{a}} b$ where $m_i \geq N_1$ for all $i \leq n$, is just $(N_1, \ldots, N_1) + \log_{\overline{a}''} b$, where $\overline{a}'' = (F^{N_1}a_1, \ldots, F^{N_1}a_n)$. As each $F^{N_1}a_i \in F^\infty M$, we have already proved the desired conclusion for $\log_{\overline{a}''} b$. We are left to consider those elements $\overline{m} \in \log_{\overline{a}} b$ such that for some $i \leq n$, $m_i < N_1$. Since there are only finitely many possible values for i and for $r < N_1$ – independent of b – we need only show that for any fixed $i \leq n$ and $r < N_1$, the set $\{\overline{m} \in \log_{\overline{a}} b : m_i = r\}$ has the desired form. We proceed by induction on n: the case of $n = 1$ being trivial. For $n \geq 2$, the set of elements $\overline{m} \in \log_{\overline{a}} b$ satisfying $m_i = r$ can be described as the set of all

$$(m_1, \ldots, m_{i-1}, r, m_{i+1}, \ldots, m_n) \in \mathbb{N}^n$$

such that

$$(m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n) \in \log_{\overline{a}'}(b - F^r a_i),$$

where $\overline{a}' = (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. By the inductive hypothesis applied to $\overline{a}'$, $\log_{\overline{a}'}(b - F^r a_i) = \bigcup_{j \in J}(\overline{r}'_j \oplus B'_j)$, where the $B'_j \subset \mathbb{N}^{n-1}$ come from a finite collection of δ_M-basic sets that depends only on $\overline{a}'$, and hence only on $\overline{a}$ and i. For each $j \in J$, let $\overline{r}_j \in \mathbb{N}^n$ be the tuple obtained from $\overline{r}'_j$ by plugging in 0 between the $(i-1)$st and ith coordinate, and let $B_j \subset \mathbb{N}^n$ be the δ_M-basic set obtained from B'_j by plugging in r between the $(i-1)$st and ith coordinate of each element. It is then not hard to see that

$$\{\overline{m} \in \log_{\overline{a}} b \colon m_i = r\} = \bigcup_{j\in J} (\overline{r}_j \oplus B_j),$$

This gives us the desired description for $\{\overline{m} \in \log_{\overline{a}} b \colon m_i = r\}$. □

We are in a position to prove Theorem 4.3 itself. Let us restate the Theorem: *Suppose* $\overline{a} = (a_1, \dots, a_n) \in M^n$. *There exist* δ_M*-basic sets* $B_1, \dots, B_\ell \subset \mathbb{N}^n$*, such that for all* $b \in M$*, there is some* $J \subset \{1, \dots, \ell\}$*, and for each* $j \in J$ *there is some* $\overline{r}_j \in \mathbb{N}^n$ *disjoint from* B_j*, such that*

$$\log_{\overline{a}} b = \bigcup_{j\in J} (\overline{r}_j \oplus B_j).$$

Proof. Arrange the indices so that $a_1, \dots, a_t \notin M_\omega$ and $a_{t+1}, \dots, a_n \in M_\omega$. We proceed by induction on t. The case $t = 0$ is taken care of by Lemma 4.7. Now suppose that $0 < t \leq n$, and fix $b \in M$. We will describe $\log_{\overline{a}} b$ making sure that the data that appear in this description are independent of b.

Let N be the bound given by Lemma 4.6 applied to $a_1, \dots, a_t$. We can divide $\log_{\overline{a}} b$ into the following pieces:

1. $\log_{\overline{a}} b^\sharp$: the set of those $\overline{m} \in \log_{\overline{a}} b$ for which both m_i and $|m_i - m_j|$ are greater than N, for all $i, j \leq t$, $i \neq j$.

$2_{i,r}$. $\{\overline{m} \in \log_{\overline{a}} b \colon m_i = r\}$, for fixed $i \leq t$ and $0 \leq r \leq N$.

$3_{i,j,r}$. $\{\overline{m} \in \log_{\overline{a}} b \colon m_j = m_i + r\}$ for fixed $i, j \leq t$, $i \neq j$, and $0 \leq r \leq N$.

We will analyse these pieces of $\log_{\overline{a}} b$ separately, and in the order presented above.

First of all, we claim that for $\overline{m} \in \log_{\overline{a}} b^\sharp$ there are only finitely many possible choices for $(m_1, \dots, m_t)$. Indeed, let $\overline{m}' \in \log_{\overline{a}} b^\sharp$ be another element. Notice that

$$\sum_{i=1}^{t} F^{m'_i} a_i = (\sum_{i=1}^{t} F^{m_i} a_i) \bmod M_\omega.$$

Lemma 4.6 ensures there is only one possible choice of $(m_i + v(a_i) : i \leq t)$, up to permutations of $\{1, \dots, t\}$. Hence there are only $t!$ many possible choices for $(m_1, \dots, m_t)$.

Fixing any such choice of $r_1, \dots, r_t$, call the set of $\overline{m} \in \log_{\overline{a}} b^\sharp$ where $m_i = r_i$ for all $i \leq t$, $\log_{\overline{a}} b^\sharp(\overline{r})$. Then

$$\log_{\overline{a}} b^\sharp(\overline{r}) = (r_1, \dots, r_t, 0, \dots, 0) \oplus (\{0\} \times \cdots \times \{0\} \times \log_{\overline{a}''}(b - \sum_{i=1}^{t} F^{r_i} a_i))$$

where $\overline{a}'' = (a_{t+1}, \dots, a_n)$. Each of the coordinates of $\overline{a}''$ is in M_ω, and so Lemma 4.7 applies. This describes $\log_{\overline{a}} b^\sharp(\overline{r})$ in terms of unions of disjoint-translates of δ_M-basic sets that come from a finite collection that does not depend on b nor on $\overline{r}$. Ranging over the possible choices of $(r_1, \dots, r_t)$ we obtain the desired conclusions for $\log_{\overline{a}} b^\sharp$.

Fix $i \le t$ and $0 \le r < N$, and consider case $2_{i,r}$. The set of elements $\overline{m} \in \log_{\overline{a}} b$ satisfying $m_i = r$ can be described as the set of all

$$(m_1, \ldots, m_{i-1}, r, m_{i+1}, \ldots, m_n) \in \mathbb{N}^n$$

such that

$$(m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n) \in \log_{\overline{a}'}(b - F^r a_i),$$

where $\overline{a}' = (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. By the inductive hypothesis applied to $\overline{a}'$, $\log_{\overline{a}'}(b - F^r a_i) = \bigcup_{j \in J}(\overline{r}'_j \oplus B'_j)$, where the $B'_j \subset \mathbb{N}^{n-1}$ come from a finite collection of δ_M-basic sets that depends only on $\overline{a}'$, and hence only on $\overline{a}$ and i. For each $j \in J$, let $\overline{r}_j \in \mathbb{N}^n$ be the tuple obtained from $\overline{r}'_j$ by plugging in 0 between the $(i-1)$st and ith coordinate, and let $B_j \subset \mathbb{N}^n$ be the basic set obtained from B'_j by plugging in r between the $(i-1)$st and ith coordinate of each element. Then

$$\{\overline{m} \in \log_{\overline{a}} b \colon m_i = r\} = \bigcup_{j \in J}(\overline{r}_j \oplus B_j),$$

This gives us the desired description for $\{\overline{m} \in \log_{\overline{a}} b \colon m_i = r\}$. As there are only finitely many choices for i and r (independently of b), this takes care of case 2.

We are left to consider cases $3_{i,j,r}$ for fixed $i, j \le t$, $i \ne j$, and $0 \le r \le N$. Assume that $i < j$. The set of elements of $\log_{\overline{a}} b$, for which $m_j = m_i + r$ can be described as the set of all

$$(m_1, \ldots, m_{j-1}, m_i + r, m_{j+1}, \ldots, m_n) \in \mathbb{N}^n$$

such that

$$(m_1, \ldots, m_{j-1}, m_{j+1}, \ldots, m_n) \in \log_{\overline{a}'}(b),$$

where now $\overline{a}' = (a_1, \ldots, a_{i-1}, a_i + F^r a_j, a_{i+1}, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n)$. The inductive hypothesis applied to $\overline{a}'$ yields $\log_{\overline{a}'} b = \bigcup_{k \in J}(\overline{r}'_k \oplus B'_k)$, where $B'_k \subset \mathbb{N}^{n-1}$ are δ_M-basic sets that come from a finite collection that depends only on $\overline{a}'$, and hence only on $\overline{a}, i, j$, and r. For each $k \in J$, we consider two cases separately:

(1) If some element of B'_k has nonzero ith coordinate then let
  - $\overline{r}_k \in \mathbb{N}^n$ be the tuple obtained from $\overline{r}'_k$ by plugging in 0 between the $(j-1)$st and jth coordinate;
  - $B_k \subset \mathbb{N}^n$ be obtained from B'_k by plugging in the sum of the ith coordinate and r between the $(j-1)$st and jth coordinate of each element.

(2) If the ith coordinate of every element of B'_k is zero then let
  - $\overline{r}_k \in \mathbb{N}^n$ be obtained from $\overline{r}'_k$ by plugging in the sum of the ith coordinate of $\overline{r}'_k$ and r between the $(j-1)$st and jth coordinate of $\overline{r}'_k$;
  - $B_k \subset \mathbb{N}^n$ be obtained from B'_k by plugging in 0 between the $(j-1)$st and jth coordinate of each element.

In either case, B_k is δ_M-basic, $\overline{r}_k$ is disjoint from B_k, and the B_k's come from a finite collection of δ_M-basic sets that only depend on $\overline{a}, i, j$, and r (this was why the cases were distinguished). We have

$$\{\overline{m} \in \log_{\overline{a}} b \colon m_j = m_i + r\} = \bigcup_{k \in J}(\overline{r}_k \oplus B_k).$$

A similar argument deals with the case when $j < i$. Ranging over the finitely many possibilities for $i, j \le t$, and $r \le N$, we complete the proof of Theorem 4.3 (and hence of Proposition 3.5). $\square$

5. Quantifier Elimination

Fix a finitely generated R-module M. We have already seen in Section 3 that as a consequence of the closedness of the "log" sets, the class Groupless(M) is preserved under intersections. In this section we use the uniformity of the "log" sets, given by Theorem 4.3, to obtain a description of these intersections that is uniform with respect to translation. We then use this uniformity, together with some other ingredients, to obtain quantifier elimination for the theory of an F-structure.

We begin with the following uniform version of Lemma 2.9:

Lemma 5.1. *Suppose $S \in \mathrm{Orb}_M$. There are $T_1, \ldots, T_\ell \in \mathrm{Orb}_M$ and $d_1, \ldots, d_\ell \in S$ such that*

(a) $S = \bigcup_{i=1}^{\ell} d_i + T_i$.

(b) *If $N \leq M$ is a submodule and $c + S \subset N$ for some $c \in M$, then for all $i \leq \ell$, $T_i \in \mathrm{Groupless}(N)$ and $c + d_i \in N$.*

Proof. First note that (b) follows from (a). Indeed, if $c + S \subset N$, then since $d_1, \ldots, d_\ell \in S$, it follows that each $c_i + d_i \in N$. Also, $c + d_i + T_i \subset N$. Hence $T_i \subset N$, and so by Lemma 2.9, $T_i \in \mathrm{Groupless}(N)$.

For part (a), taking finite unions we assume that $S = b + S(\overline{a}; \overline{\delta})$ where $\overline{a} = (a_1, \ldots, a_n)$ and $\overline{\delta} = (\delta_1, \ldots, \delta_n)$ with each $\delta_i > 0$. We can write

$$S = \bigcup_{I \subset \{1,\ldots,n\}} (b + a_1 + \cdots + a_n) + \sum_{i \in I} [-a_i + S(F^{\delta_i} a_i; \delta_i)].$$

Let $d := b + a_1 + \cdots + a_n \in S$, and let

$$T := \bigcup_{I \subset \{1,\ldots,n\}} \sum_{i \in I} [-a_i + S(F^{\delta_i} a_i; \delta_i)]$$

which is in Orb_M. Then $S = d + T$, as desired. □

The next lemma gives us a uniform description of the intersection of a cycle-free groupless F-set with a submodule.

Lemma 5.2. *Suppose $S \in \mathrm{Orb}_M$ and $G \leq M$ is a submodule. Then there exist $U_1, \ldots, U_\ell \in \mathrm{Groupless}(G) \cap \mathrm{Orb}_M$, and for each $J \subset \{1, \ldots, \ell\}$ there exists $X_J \in \mathcal{F}^*(M \times G^{|J|})$ such that the following holds:*

(a) *For all J and $(c, c_j)_{j \in J} \in X_J$, $(c + S) \cap G = \bigcup_{j \in J} (c_j + U_j)$.*

(b) *For every $c \in M$ with $(c + S) \cap G$ non-empty, there is some non-empty $J \subset \{1, \ldots, \ell\}$ and $(c_j)_{j \in J} \in G^{|J|}$ with $(c, c_j)_{j \in J} \in X_J$.*

Proof. First of all, by Lemma 5.1, it suffices to find the U_j's in Orb_M and the X_J's in $\mathcal{F}^*(M \times M^{|J|})$. Also, taking finite unions and translating, we may assume that $S = S(\overline{a}; \overline{\delta})$. We write $S = F^D \overline{a}$, where $D = \delta_1 \mathbb{N} \times \cdots \times \delta_n \mathbb{N}$.

Let $\pi \colon M \to M/G$ be the quotient map. Note that if $(c + S) \cap G \neq \emptyset$, then $\pi c = F^{\overline{r}}(-\pi \overline{a})$ for some $\overline{r} \in D$, and

$$(c + S) \cap G = c + F^{(\log_{(-\pi \overline{a})}(\pi c) \cap D)} \overline{a}.$$

Let $B_1, \ldots B_{\ell'} \subset \mathbb{N}^n$ be the basic sets obtained by Theorem 4.3 applied to M/G and $-\pi \overline{a}$. Reordering if necessary, let $0 \leq \ell \leq \ell'$ be such that for all $1 \leq i \leq \ell$,

$C_i := B_i \cap D$ is nonempty, and for all $j > \ell$, $B_j \cap D$ is empty. For each $1 \leq i \leq \ell$, let $U_i := F^{C_i^\circ}\overline{a}^\circ$, where $C_i^\circ, \overline{a}^\circ$ is the canonical contraction of $C_i, \overline{a}$ (see the discussion following Definition 4.1).

We now define the X_J's. Fix $J \subset \{1, \dots, \ell\}$. Let A_J be the collection of tuples $(\overline{r}, \overline{s}_j)_{j\in J}$ such that

- for each $j \in J$, $\overline{s}_j$ is disjoint from C_j; and,
- $\log_{(-\pi\overline{a})}(F^{\overline{r}}(-\pi\overline{a})) \cap D = \bigcup_{j\in J} \overline{s}_j \oplus C_j$.

Note that A_J is definable since $\log_{(-\pi\overline{a})}(F^{\overline{r}}(-\pi\overline{a}))$ is the $(-\pi\overline{a})$-equivalence class of $\overline{r}$, and hence, as $\overline{r}$ varies, is uniformly definable over $\overline{r}$. If $(\overline{r}, \overline{s}_j)_{j\in J} \in A_J$ and $j \in J$, recall that $F^{\overline{s}_{j\circ}}\overline{a}_\circ + F^{C_j^\circ}\overline{a}^\circ$ is the canonical form of $F^{(\overline{s}_j \oplus C_j)}\overline{a}$. Let A'_J be the collection of tuples $(\overline{r}, \overline{s}_{j\circ})_{j\in J}$ where $(\overline{r}, \overline{s}_j)_{j\in J} \in A_J$. Then A'_J is also definable. Finally, let $X_J \subset M \times M^{|J|}$ be the set of tuples $(x, x_j)_{j\in J}$ such that $\pi x = F^{\overline{r}}(-\pi\overline{a})$ and $x_j - x = F^{\overline{s}_{j\circ}}\overline{a}_\circ$, for some $(\overline{r}, \overline{s}_{j\circ})_{j\in J} \in A'_J$. Now X_J is a generalised F-set by Propositions 3.12 and 3.15. Note that X_J may be empty.

We check (a). Suppose $(c, c_j)_{j\in J} \in X_J$. Then there exists $(\overline{r}, \overline{s}_j)_{j\in J} \in A_J$ such that $c_j - c = F^{\overline{s}_{j\circ}}\overline{a}_\circ$ and $\log_{(-\pi\overline{a})}(\pi c) \cap D = \bigcup_{j\in J} \overline{s}_j \oplus C_j$. Hence

$$F^{(\log_{(-\pi\overline{a})}(\pi c)\cap D)}\overline{a} = \bigcup_{j\in J} F^{(\overline{s}_j\oplus C_j)}\overline{a} = \bigcup_{j\in J} c_j - c + U_j$$

and so

$$(c + S) \cap G = c + F^{(\log_{(-\pi\overline{a})}(\pi c)\cap D)}\overline{a} = \bigcup_{j\in J} c_j + U_j.$$

We check (b). Let $c \in M$ with $(c + S) \cap G$ is non-empty. Then $-\pi c \in \pi S$. Hence, for some $\overline{r} \in D$, $F^{\overline{r}}(-\pi\overline{a}) = \pi c$. Moreover, by Theorem 4.3, for some $J' \subset \{1, \dots, \ell'\}$, and tuples $\overline{s}_j$ for $j \in J'$,

$$\log_{(-\pi\overline{a})} \pi c = \bigcup_{j\in J'} (\overline{s}_j \oplus B_j).$$

As $D = \delta_1\mathbb{N} \times \cdots \times \delta_n\mathbb{N}$, it is not hard to see that for each $j \in J'$, if $j \leq \ell$ and $\overline{s}_j \in D$ then $\overline{s}_j$ is disjoint from $B_j \cap D = C_j$ (which is non-empty) and $(\overline{s}_j \oplus B_j) \cap D = \overline{s}_j \oplus C_j$. On the other hand, if $\overline{s}_j \notin D$ or $j > \ell$, then $(\overline{s}_j \oplus B_j) \cap D$ is empty. Let $J = \{j \in J' : \overline{s}_j \in D \text{ and } j \leq \ell\}$. We have

$$\log_{(-\pi\overline{a})}(F^{\overline{r}}(-\pi\overline{a})) \cap D = \log_{(-\pi\overline{a})} \pi c \cap D = \bigcup_{j\in J} (\overline{s}_j \oplus C_j).$$

Note that $J \neq \emptyset$ since $\overline{r} \in \log_{-\pi\overline{a}}(\pi c) \cap D$. Letting $c_j = c + F^{\overline{s}_{j\circ}}\overline{a}_\circ$ for each $j \in J$, we see that $(c, c_j)_{j\in J} \in X_J$, as desired. □

Proposition 5.3. *Suppose $S \in \mathrm{Orb}_M$ and $G, H \leq M$ are submodules. Then there exist $U_1, \dots, U_\ell \in \mathrm{Groupless}(G)$, and for each $J \subset \{1, \dots, \ell\}$ there exists $X_J \in \mathcal{F}^*(M \times G^{|J|})$, such that the following holds:*

(a) *For all J and $(c, c_j)_{j\in J} \in X_J$, $(c + S + H) \cap G = \bigcup_{j\in J} (c_j + U_j + (H \cap G))$.*
(b) *For every $c \in M$ with $(c + S + H) \cap G$ non-empty, there is some non-empty $J \subset \{1, \dots, \ell\}$ and $(c_j)_{j\in J} \in G^{|J|}$ with $(c, c_j)_{j\in J} \in X_J$.*

Proof. Let $V_1, \dots V_\ell \in \text{Groupless}(G{+}H)$, and $Y_J \in \mathcal{F}^*(M \times (G{+}H)^{|J|})$ for each $J \subset \{1, \dots, \ell\}$, be given by Lemma 5.2 applied to S and $G + H$. Let π be the quotient map $M \to M/(G{\cap}H)$, and $\eta \colon \pi(G{+}H) \to \pi G$ be the projection map corresponding to the isomorphism $\pi(G{+}H) \cong \pi G \oplus \pi H$. For each $i \leq \ell$, let $U_i \in \text{Groupless}(G)$ be such that $\pi U_i = \eta\pi V_i$. For each $J \subset \{1, \dots, \ell\}$, let $X_J \subset M \times G^{|J|}$ be those tuples $(x, x_j)_{j\in J}$ such that for some $(y_j)_{j\in J} \in (G{+}H)^{|J|}$, $(x, y_j)_{j\in J} \in Y_J$ and $\pi x_j = \eta\pi y_j$. As generalised F-sets are preserved under intersections and images/preimages of surjective R-module homomorphisms, the X_J's are generalised F-sets.

These U_i's and X_J's work. For (a), suppose $(c, c_j)_{j\in J} \in X_J$ and $(c, d_j)_{j\in J} \in Y_J$ with $\pi c_j = \eta\pi d_j$ for each $j \in J$. By part (a) of Lemma 5.2,

$$(c + S) \cap (G + H) = \bigcup_{j\in J} d_j + V_j.$$

Fixing $j \in J$, we have

$$\begin{aligned}(d_j + V_j + H) \cap G &= \pi^{-1}[(\pi d_j + \pi V_j + \pi H) \cap \pi G] \\ &= \pi^{-1}[\eta\pi d_j + \eta\pi V_j] \\ &= c_j + U_j + (H \cap G)\end{aligned}$$

Hence

$$\begin{aligned}(c + S + H) \cap G &= [(c + S) \cap (G + H) + H] \cap G \\ &= \bigcup_{j\in J} c_j + U_j + (H \cap G)\end{aligned}$$

as desired. For part (b) suppose $c \in M$ with $(c + S + H) \cap G$ non-empty. Then $(c + S) \cap (H + G)$ is non-empty, and so by part (b) of Lemma 5.2, there is a non-empty $J \subset \{1, \dots, \ell\}$ and $(d_j)_{j\in J} \in (G + H)^{|J|}$ such that $(c, d_j)_{j\in J} \in Y_J$. Now for each $j \in J$, let $c_j \in G$ be such that $\pi c_j = \eta\pi d_j$. Then, $(c, c_j)_{j\in J} \in X_J$. □

Remark 5.4. We actually obtain that $(c + S + H) \cap G$ is non-empty if and only if there is some non-empty $J \subset \{1, \dots, \ell\}$ and $(c_j)_{j\in J} \in G^{|J|}$ with $(c, c_j)_{j\in J} \in X_J$. In particular the set of such c is a generalised F-set by Proposition 3.15.

The following description of intersections of F-sets in general uses only part of what is given by Proposition 5.3.

Corollary 5.5. *Suppose $U, V \in \text{Groupless}(M)$ and $G, H \leq M$ are submodules. Then there exist $W_1, \dots, W_\ell \in \text{Groupless}(M)$ such that for all $c, d \in M$ there is $J \subset \{1, \dots, \ell\}$ and points $(e_j)_{j\in J}$ from M, such that*

$$(c + U + H) \cap (d + V + G) = \bigcup_{j\in J} e_j + W_j + (H \cap G).$$

Proof. We may assume that U and V are cycle-free groupless F-sets. Indeed, let M' be a finitely generated R-module extending M such that $U, V \in \text{Orb}_{M'}$, and let $W_1, \dots, W_\ell \in \text{Groupless}(M')$ witness the truth of the corollary in this case. Then for $c, d \in M$ there is $J \subset \{1, \dots, \ell\}$ and points $(e_j)_{j\in J}$ from M', such that

$$(c + U + H) \cap (d + V + G) = \bigcup_{j\in J} e_j + W_j + (H \cap G).$$

But as $(c + U + H) \cap (d + V + G) \subset M$, each $e_j + W_j \subset M$. Note that there is a further extension M'' of M' such that $W_1, \dots, W_\ell \in \text{Orb}_{M''}$. So Lemma 5.1 applies to $W_j \in \mathrm{Orb}_{M''}$, and we find W_{ij}'s in Groupless(M) (independently of the e_j's) such that $e_j + W_j$ is a finite union of sets of the form $e_{ij} + W_{ij}$ where the e_{ij}'s are now also from M. Hence we may and do assume that $U, V \in \mathrm{Orb}_M$,

Applying Proposition 5.3 to $U \times V \in \mathrm{Orb}_{M^2}$, $H \times G \leq M^2$, and the diagonal $\Delta \leq M^2$, we obtain $\hat{W}_1, \dots, \hat{W}_\ell \in \mathrm{Groupless}(M^2)$ such that for all $c, d \in M$ there is $J \subset \{1, \dots, \ell\}$ and points $(\hat{e}_j)_{j \in J}$ from M^2, such that

$$[(c,d) + (U \times V) + (H \times G)] \cap \Delta = \bigcup_{j \in J} \hat{e}_j + \hat{W}_j + (H \times G) \cap \Delta.$$

For each $i \leq \ell$, let W_i be the projection of $\hat{W}_i$ onto the first coordinate. Then $W_1, \dots, W_\ell$ witness the truth of the corollary. □

Remark 5.6. In Corollary 5.5, if $d = 0$ and $V = 0$, then we can actually find the W_i's in Groupless(G). Indeed, this follows from the above proof: we can replace Δ with $\Delta \cap (G \times G)$ and hence find the $\hat{W}_i$'s in Groupless$(G \times G)$ by Proposition 5.3. Taking projections yields $W_i \in \mathrm{Groupless}(G)$ for all $i = 1, \dots, \ell$.

The next step for quantifier elimination is to understand when a given F-set is covered by translates of other F-sets. We begin with the groupless case.

Lemma 5.7. *Suppose $U, V_1, \dots, V_\ell \in \mathrm{Groupless}(M)$. Then the set*

$$X := \{(c_0, c_1, \dots c_\ell) \in M^{\ell+1} \colon c_0 + U \subset \bigcup_{i=1}^{\ell} (c_i + V_i)\}$$

is a generalised F-set.

Proof. Let $\eta \colon M^{\ell+1} \to M^\ell$ be given by $\eta(a_0, \dots a_\ell) = (a_1 - a_0, \dots, a_\ell - a_0)$. Let $Y := \{(c_1, \dots c_\ell) \in M^\ell \colon U \subset \bigcup_{i=1}^{\ell} (c_i + V_i)\}$. Note that $X = \eta^{-1}(Y)$. It suffices, therefore, to show that $Y \in \mathcal{F}^*(M^\ell)$ (by Proposition 3.15).

We may assume that $U, V_1, \dots, V_\ell \in \mathrm{Orb}_M$. Indeed, if M' is a finitely generated R-module extending M such that $U, V_1, \dots, V_\ell \in \mathrm{Orb}_{M'}$, and if Y' is the set $\{(c_1, \dots c_\ell) \in (M')^\ell \colon U \subset \bigcup_{i=1}^{\ell} (c_i + V_i)\}$, then $Y = Y' \cap M^\ell$. So if $Y \in \mathcal{F}^*((M')^\ell)$, then $Y \in \mathcal{F}^*(M^\ell)$ (by part (b) of Proposition 3.17).

Taking finite unions, we may assume that $U = F^B \overline{x}$, and that for each $i \leq \ell$, $V_i = F^{C_i} \overline{z}_i$; where $B \subset \mathbb{N}^p$, $C_i \subset \mathbb{N}^{r_i}$ are closed, $\overline{x} \in M^p$, and $\overline{z}_i \in M^{r_i}$. We need to deal with the situation when some of the V_i's are extraneous. To this end, for fixed $I \subset \{1, \dots, \ell\}$ let

$$Y_I := \{(c_i)_{i \in I} \in M^{|I|} \colon U \subset \bigcup_{i \in I} c_i + V_i \text{ and for each } i \ (c_i + V_i) \cap U \neq \emptyset\}.$$

Letting $Y_I' := \{(c_1, \dots, c_\ell) \in M^\ell \colon (c_i)_{i \in I} \in Y_I\}$, we have $Y = \bigcup_{I \subset \{1, \dots, \ell\}} Y_I'$. Now, for fixed $(c_i)_{i \in I} \in Y_I$ and $i \in I$, $c_i = F^{\overline{r}} \overline{x} - F^{\overline{s}} \overline{z}_i$ for some $\overline{r} \in B$ and $\overline{s} \in C_i$. So $c_i \in F^{\mathbb{N}^{q_i}} \overline{a}_i$ where $\overline{a}_i = (\overline{x}, -\overline{z}_i)$ and $q_i = p + r_i$. Letting $\overline{y}_i = (\overline{a}_i, \overline{z}_i)$ and

$$Z_I := \{(F^{\overline{t}_i} \overline{a}_i)_{i \in I} \colon F^B \overline{x} \subset \bigcup_{i \in I} F^{(\overline{t}_i \times C_i)} \overline{y}_i\},$$

we obtain $Y_I \subset Z_I$. Moreover, if $Z'_I := \{(c_1, \dots, c_\ell) \in M^\ell \colon (c_i)_{i \in I} \in Z_I\}$, then $Y'_I \subset Z'_I \subset Y$. Hence $Y = \bigcup_{I \subset \{1,\dots,\ell\}} Z'_I$, and we need only show that each Z'_I is a generalised F-set. For this, it suffices to show that each Z_I is a generalised F-set.

Using the definability of logarithmic equivalence, it is not hard to see that for any fixed $I \subset \{1, \dots, \ell\}$, the set of $(\overline{t}_i)_{i \in I}$ such that $F^B\overline{x} \subset \bigcup_{i \in I} F^{(\overline{t}_i \times C_i)}\overline{y}_i$, is definable. It follows, by Proposition 3.12, that $Z_I \in \mathrm{Groupless}^*(M^{|I|})$. □

Lemma 5.8. *If G is an infinite subgroup of M, then $G \notin \mathrm{Groupless}(M)$.*

Proof. Suppose G is a groupless F-set and seek a contradiction. Let M' extend M so that $G \in \mathrm{Orb}_{M'}$. Then there are tuples $\overline{a}_1, \dots \overline{a}_\ell$ from M', and closed sets $B_1, \dots, B_\ell$, such that $G = \bigcup_{i=1}^{\ell} F^{B_i}\overline{a}_i$. Extending the $\overline{a}_i$'s and B_i's in an appropriate manner, we may assume that for some $n > 0$, $\overline{a}_1, \dots, \overline{a}_\ell \in (M')^n$ and that $B_1, \dots, B_\ell \subset \mathbb{N}^n$ are mutually disjoint. Let $B = \bigcup_{i=1}^{\ell} B_i$. Let $\sim$ be the definable equivalence relation on B given by

$$\overline{r} \sim \overline{s} \iff \bigvee_{i,j \leq \ell} (\overline{r} \in B_i \text{ and } \overline{s} \in B_j \text{ and } F^{\overline{r}}\overline{a}_i = F^{\overline{s}}\overline{a}_j).$$

There is a natural bijection between $B/\sim$ and G.

For each $i, j, k \leq \ell$, define $P_{ijk} \subset B_i \times B_j \times B_k$ to be the definable relation $F^{\overline{r}_1}\overline{a}_i + F^{\overline{r}_2}\overline{a}_j = F^{\overline{r}_3}\overline{a}_k$. We obtain a group structure on $B/\sim$ by declaring that $e_1 + e_2 = e_3$ if for some $i, j, k \leq \ell$, there exists $(\overline{r}_1, \overline{r}_2, \overline{r}_3) \in P_{ijk}$ such that the $\sim$-class of $\overline{r}_\ell$ is equal to e_ℓ for $\ell = 1, 2, 3$. For some $\delta > 0$, this infinite group is interpretable in the structure $(\mathbb{N}, 0, \sigma, P_\delta)$, contradicting the triviality of $\mathrm{Th}(\mathbb{N}, 0, \sigma, P_\delta)$.[5] □

Lemma 5.9. *Suppose $H_1, \dots, H_n \leq G$ are submodules of M such that each H_i is of infinite index in G, and $U_1, \dots, U_n \in \mathrm{Groupless}(M)$. Then*

$$G \neq \bigcup_{i=1}^{n} U_i + H_i.$$

Proof. We proceed by induction on n. Consider the case of $n = 1$. Let π be the reduction modulo H_1 map. If $G = U_1 + H_1$, then $\pi G = \pi U_1$. But as πG is infinite, this would contradict Lemma 5.8.

Suppose $n > 1$. We assume the result is false and seek a contradiction. Define a quasiordering on $1, \dots, n$ by $i \sqsubseteq j$ if and only if $H_i \cap H_j$ has finite index in H_i. *We may assume that $\sqsubseteq$ is a partial ordering.* If not, then it must be the case that for some $i \neq j$, $H_i \cap H_j$ is of finite index in both H_i and H_j. But then, by Corollary 5.5, $(U_i + H_i) \cap (U_j + H_j) = U' + (H_i \cap H_j)$ for some groupless F-set U'. But by induction, $G \neq [U' + (H_i \cap H_j)] \cup \bigcup_{k \neq i,j} U_k + H_k$.

After reordering, we may assume that H_1 is $\sqsubseteq$-maximal. That is, for all $i \neq 1$, $H_1 \cap H_i$ is of infinite index in H_1. Let $\pi \colon G \to G/H_1$ be the quotient map restricted to G. Now, as H_1 has infinite index in G, $X = \pi(U_1 + H_1) = \pi U_1 \neq G/H_1$ by Lemma 5.8. Let $h \in (G/H_1) \setminus X$. Then $\pi^{-1}\{h\}$ is disjoint from $U_1 + H_1$. As $G = \bigcup_{i=1}^{n} U_i + H_i$, $\pi^{-1}\{h\}$ is covered by $\bigcup_{i=2}^{n} U_i + H_i$. But $\pi^{-1}\{h\}$ is a coset of H_1, say

[5] See Propositions A.1 and A.2.

$c+H_1$. So $H_1 = \bigcup_{i=2}^{n}(-c+U_i+H_i)\cap H_1$. We can express each $(-c+U_i+H_i)\cap H_1$ as an F-set where the submodule that appears is $H_1\cap H_i$. As $H_1\cap H_i$ has infinite index in H_1, we see that this is impossible by induction. $\square$

Corollary 5.10. *Suppose $U_1,\dots,U_n \in \mathrm{Groupless}(M)$ and $H_1,\dots,H_n \leq G$ are submodules of M. Let I be the set of indices i such that H_i has finite index in G. If $G = \bigcup_{i=1}^{n}(U_i+H_i)$, then $G = \bigcup_{i\in I}(U_i+H_i)$.*

Proof. Note that by Lemma 5.9, $I \neq \emptyset$. Let $K = \bigcap_{i\in I} H_i$, and $X = \bigcup_{i\in I} U_i + H_i$. Then K is of finite index in G and X is a finite union of cosets of K. Suppose that $G\setminus X \neq \emptyset$, and $a \in G\setminus X$. We would have $a+K \subset G\setminus X \subset \bigcup_{j\notin I} U_j + H_j$, so that $K = \bigcup_{j\notin I}[(U_j-a)+H_j]\cap K$. Each $[(U_j-a)+H_j]\cap K$ is an F-set where the submodule that appears is $H_j\cap K$. As $H_j\cap K$ has infinite index in K, this contradicts Lemma 5.9. $\square$

Proposition 5.11. *Suppose $U, V_1,\dots,V_\ell \in \mathrm{Groupless}(M)$ and $G, H_1,\dots,H_\ell$ are submodules of M. Then the set*

$$X := \{(c_0,c_1,\dots c_l)\in M^{\ell+1} \colon c_0+U+G \subset \bigcup_{i=1}^{\ell}(c_i+V_i+H_i)\}$$

is a generalised F-set.

Proof. Clearly c_0+U+G is covered by the union on the righthand side of the displayed inclusion if and only if c_0+u+G is covered for all $u\in U$. But by Corollary 5.10, if this happens at all, it will already happen with those indices i such that $H_i\cap G$ has finite index in G. Thus, we may and do assume that $H_i\cap G$ is of finite index in G for each i. Let $K := \bigcap_{i=1}^{\ell}(H_i\cap G)$, and denote by π the reduction modulo K map. It is not hard to see that $c_0+U+G \subset \bigcup_{i=1}^{\ell}(c_i+V_i+H_i)$ if and only if $\pi c_0 + \pi(U+G) \subset \bigcup_{i=1}^{\ell}(\pi c_i + \pi(V_i+H_i))$. Note that as πG and the πH_i's are finite sets, $\pi(U+G)$ and the $\pi(V_i+H_i)$'s are groupless F-sets in M/K. That is, we are in the groupless case. By Lemma 5.7, the set

$$Y = \{(d_0,d_1,\dots,d_l)\in (M/K)^{\ell+1} \colon d_0+\pi(U+G) \subset \bigcup_{i=1}^{\ell}(d_i+\pi(V_i+H_i))\}$$

is a generalised F-set. Hence $X = \pi^{-1}(Y) \in \mathcal{F}^*(M^{\ell+1})$, as desired. $\square$

We combine Propositions 5.3 and 5.11 to obtain:

Proposition 5.12. *Suppose $T, S_1,\dots,S_\ell \in \mathrm{Orb}_M$ and $L, G, H_1,\dots,H_\ell \leq M$ are submodules. Then the set*

$$X := \{c\in M \colon (c+T+G)\cap L \subset \bigcup_{i=1}^{\ell}[(c+S_i+H_i)\cap L]\}$$

is quantifier-free definable in $(M,\mathcal{F})$.

Proof. Let $U_1, \ldots, U_n \in \text{Groupless}(L)$ and $Y_J \in \mathcal{F}^*(M \times L^{|J|})$ for each $J \subset \{1, \ldots, n\}$, be given by Proposition 5.3 applied to T, G, and L. Similarly, for $i \leq \ell$, let $V_{i1}, \ldots V_{im_i} \in \text{Groupless}(L)$ and $Z_{iJ} \in \mathcal{F}^*(M \times L^{|J|})$ for each $J \subset \{1, \ldots, m_i\}$, be given by that proposition applied to S_i, H_i, and L. Then $c \in X$ if and only if $(c + T + G) \cap L$ is empty or
$(*)$ *there exist*

- *non-empty* $J \subset \{1, \ldots, n\}$, $I \subset \{1, \ldots, \ell\}$, *and* $J_i \subset \{1, \ldots, m_i\}$ *for each* $i \in I$*; and,*
- *tuples* $(c_j)_{j \in J} \in L^{|J|}$ *and* $(d_{ij})_{j \in J_i} \in L^{|J_i|}$ *for each* $i \in I$*;*

such that

(i) $(c, c_j)_{j \in J} \in Y_J$, $(c, d_{ij})_{j \in J_i} \in Z_{iJ_i}$ *for each* $i \in I$*; and,*
(ii) $\displaystyle\bigcup_{j \in J}(c_j + U_j + (G \cap L)) \subset \bigcup_{i \in I} \bigcup_{j \in J_i} (d_{ij} + V_{ij} + (H_i \cap L))$.

As all the Y_J's and Z_{iJ_i}'s are generalised F-sets, and as condition (ii) is given by a generalised F-set relation (by Proposition 5.11), the set of $c \in M$ for which $(*)$ holds is a generalised F-set. It is therefore quantifier-free definable. Finally the set of $c \in M$ such that $(c + T + G) \cap L$ is empty is quantifier-free definable (it is the complement of a generalised F-set – see Remark 5.4). $\square$

Theorem 5.13. *Suppose M is a finitely generated R-module. Then* $\text{Th}(M, \mathcal{F})$ *admits quantifier elimination.*

Proof. We need to show that the projection of a quantifier-free definable set is again quantifier-free definable. As F-sets are preserved under intersections and unions, it is sufficient to show that $\pi[(U + G) \setminus \bigcup_{i=1}^{\ell}(V_i + H_i)]$ is quantifier-free definable; where $U, V_1, \ldots V_\ell \in \text{Groupless}(M^{m+n})$, $G, H_1, \ldots H_\ell \leq M^{m+n}$ are submodules, and $\pi \colon M^{m+n} \to M^m$ is the projection map. Now, $\pi[(U + G) \setminus \bigcup_{i=1}^{\ell}(V_i + H_i)]$ is just $\pi(U + G) \setminus X$ where

$$X = \{c \in M^m \colon (U + G)_c \subset \bigcup_{i=1}^{\ell}(V_i + H_i)_c\}$$

where for any $Z \subset M^{m+n}$ and $c \in M^m$, $Z_c := \pi^{-1}(c) \cap Z$. It suffices to show that X is quantifier-free definable.

For any $b \in M^{m+n}$ and $\delta > 0$, the F-cycle $C(b; \delta)$ is a cycle-free groupless F-set in $(M')^{m+n}$ for some finite extension M' of M. Indeed, let $b = (b_1, \ldots, b_{m+n})$, and let M' be obtained from M by a finite sequence of splitting extensions such that for all $i \leq m + n$, there is $a_i \in M'$ with $F^\delta a_i - a_i = b_i$. Then $F^\delta a - a = b$, where $a = (a_1, \ldots, a_{m+n})$. As in Lemma 2.7, $C(b; \delta) = -a + S(F^\delta a; \delta)$, which is cycle-free and groupless in $(M')^{m+n}$. Hence, there is some finitely generated R-module M' extending M, such that $U, V_1, \ldots V_\ell \in \text{Orb}_{(M')^{m+n}}$.

Let $X' = \{c \in (M')^m \colon (U + G)_c \subset \bigcup_{i=1}^{\ell}(V_i + H_i)_c\}$. Then $X = X' \cap M^m$. So it suffices to show that X' is quantifier-free definable in the F-structure $(M', \mathcal{F})$. But

$c \in X'$ if and only if

$$(U+G) \cap (c \times (M')^n) \subset \bigcup_{i=1}^{\ell} (V_i + H_i) \cap (c \times (M')^n)$$

if and only if

$$[(-c,0)+U+G] \cap (0 \times (M')^n) \subset \bigcup_{i=1}^{\ell} [(-c,0)+V_i+H_i] \cap (0 \times (M')^n).$$

It follows from Proposition 5.12 applied to the finitely generated R-module $(M')^{m+n}$ (in which $U, V_1, \dots, V_\ell$ are now cycle-free groupless), that the set of $(-c,0)$'s for which this last displayed inclusion holds is quantifier-free definable. Hence X' is quantifier-free definable. □

6. Stability

In this section we show that the theory of an F-structure is stable. Fix a finitely generated R-module M. We begin by introducing a stratification by complexity of the cycle-free groupless F-sets of M:

Definition 6.1. Suppose $\delta > 0$. We define the class of cycle-free groupless F-sets in M *of order* δ, denoted by $\mathrm{Orb}_M(\delta)$ to be those F-sets in Orb_M that are finite unions of sets of the form $c + S(a_1, \dots, a_n; \delta_1, \dots, \delta_n)$, where each δ_i divides δ. Moreover, given $N \leq M$ a submodule, $\mathrm{Orb}_M^N(\delta)$ is the class of all $S \in \mathrm{Orb}_M(\delta)$ such that $S \subset N$.

Remark 6.2.
(a) Note that $\mathrm{Orb}_M = \bigcup_{\delta>0} \mathrm{Orb}_M(\delta)$. In fact, we can restrict this union to be over all δ a multiple of γ, where $\gamma > 0$ is fixed and given.
(b) Any $S \in \mathrm{Orb}_M(\delta)$ can be expressed as a cycle-free groupless F-set whose F-orbits only involve δ. Indeed, if $\delta = r\delta_i$ then
$$S(a_i; \delta_i) = \bigcup_{\ell=0}^{r-1} S(F^{\ell\delta_i} a_i; \delta).$$
(c) For $S \subset M$, $S \in \mathrm{Orb}_M(\delta)$ if and only if $S = \bigcup_{i=1}^{\ell} F^{B_i}\overline{a}_i$ for some sequence of tuples $\overline{a}_1, \dots, \overline{a}_\ell$ from M and δ-closed sets $B_1, \dots, B_\ell$. Indeed, this follows from the argument for Lemma 3.4.
(d) Suppose $S \in \mathrm{Orb}_M(\delta)$. There are $S_1, \dots, S_\ell \in \mathrm{Orb}_M(\delta)$ and $d_1, \dots, d_\ell \in S$ such that $S = \bigcup_{j=1}^{\ell} d_j + S_j$. This follows from the proof of Lemma 5.1 (a). Notice that if $c + S \subset N$ for some $c \in M$ and $N \leq M$, then each $S_i \subset N$ (and so in $\mathrm{Orb}_M^N(\delta)$) – since $c + d_i \in N$ (as $d_i \in S$) and $c + d_i + S_i \subset N$.

Let us fix $\delta_M > 0$ as in Section 4; it is the least positive integer such that F^{δ_M} fixes the set $F^\infty M$ pointwise (see page 14). We have the following control over intersections in this class.

Lemma 6.3. *Suppose $N \leq M$ is a submodule and $S, T \in \mathrm{Orb}_M^N(\delta)$, where δ is a multiple of δ_M. There exist $R_1, \dots R_\ell \in \mathrm{Orb}_M^N(\delta)$, such that for all $x, y \in N$ there is an $I \subset \{1, \dots, \ell\}$ and $z_i \in N$ for each $i \in I$, such that*

$$(x+S) \cap (y+T) = \bigcup_{i \in I} z_i + R_i.$$

Proof. It suffices to prove this for $N = M$. Indeed, as in part (d) of Remark 6.2, we rewrite $R_i = \bigcup_{j=1}^{\ell_i} d_{ij} + R_{ij}$, where each $d_{ij} \in R_i$ and $R_{ij} \in \mathrm{Orb}_M(\delta)$. Then as $(x+S) \cap (y+T) \subset N$ (if $x, y \in N$), each $z_i + R_i \subset N$, and hence each $z_i + d_{ij} \in N$ and each $R_{ij} \in \mathrm{Orb}_M^N(\delta)$ – yielding the desired result. Secondly, as

$$(x+S) \cap (y+T) = y + ((x-y+S) \cap T),$$

we may assume that $y = 0$. Finally, taking finite unions, we may assume that $S = c + S(a_1, \dots a_n; \delta)$ and $T = d + S(b_1, \dots b_m; \delta)$.

Write $S = c + F^{\delta\mathbb{N}^n}\overline{a}$ and $T = d + F^{\delta\mathbb{N}^m}\overline{b}$, where $\overline{a} = (a_1, \dots, a_n)$, $\overline{b} = (b_1, \dots, b_m)$. For all x, $(x+S) \cap T = x + c + F^{D(x)}\overline{a}$, where

$$D(x) := \{\overline{r} \in \mathbb{N}^n : \text{for some } \overline{s} \in \mathbb{N}^m, (\overline{r}, \overline{s}) \in \delta\mathbb{N}^{(n+m)} \cap \log_{(\overline{a}, -\overline{b})}[d-c-x]\}$$

By Theorem 4.3, we have δ_M-basic sets $B_1, \dots B_{\ell'} \subset \mathbb{N}^{(n+m)}$ depending only on $(\overline{a}, -\overline{b})$ (and hence only on S and T), and $J \subset \{1, \dots, \ell'\}$, such that,

$$\log_{(\overline{a}, -\overline{b})}[d-c-x] = \bigcup_{j \in J} \overline{r}_j \oplus B_j,$$

for some $\overline{r}_j \in \mathbb{N}^{(n+m)}$. For each $1 \leq i \leq \ell'$, let $C_i = \delta\mathbb{N}^{(n+m)} \cap B_i$. Note that C_i is either empty or δ-closed. We may arrange the indices so that for some $0 \leq \ell \leq \ell'$, C_i is nonempty if and only if $i \leq \ell$. Now let $I \subset J$ be those indices $i \leq \ell$ for which $\overline{r}_i \in \delta\mathbb{N}^{(n+m)}$. It follows that for all $i \leq \ell'$, $\delta\mathbb{N}^{(n+m)} \cap (\overline{r}_i \oplus B_i) = \overline{r}_i \oplus C_i$ if $i \in I$, and empty otherwise. We have

$$\delta\mathbb{N}^{(n+m)} \cap \log_{(\overline{a}, -\overline{b})}[d-c-x] = \bigcup_{i \in I} \overline{r}_i \oplus C_i.$$

Let $\pi \colon \mathbb{N}^{(n+m)} \to \mathbb{N}^n$ be the projection map, Then

$$D(x) = \bigcup_{i \in I} \pi\overline{r}_i \oplus \pi C_i,$$

where $\pi C_1, \dots, \pi C_\ell$ are δ-closed sets that depend only on S and T. Now,

$$(x+S) \cap T = \bigcup_{i \in I} x + c + F^{(\pi\overline{r}_i)_\circ}\overline{a}_\circ + F^{\pi C_i^\circ}\overline{a}^\circ,$$

where $F^{(\pi\overline{r}_i)_\circ}\overline{a}_\circ + F^{\pi C_i^\circ}\overline{a}^\circ$ is the canonical form of $F^{(\pi\overline{r}_i \oplus \pi C_i)}\overline{a}$. As $\pi C_1^\circ, \dots, \pi C_\ell^\circ$ are also δ-closed, each $F^{\pi C_i^\circ}\overline{a}^\circ \in \mathrm{Orb}_M(\delta)$, and they depend only on S and T. $\square$

Definition 6.4. Fix $\delta > 0$. An *exponential F-set of order δ* is a set of the form $F^B\overline{a}$ for some $\overline{a} \in M^n$ and δ-closed $B \subset \mathbb{N}^n$. We denote the class of exponential F-sets of order δ by $\mathrm{Exp}_M(\delta)$. Given $N \leq M$ a submodule, $\mathrm{Exp}_M^N(\delta)$ is the class of all $S \in \mathrm{Exp}_M(\delta)$ such that $S \subset N$.

Remark 6.5. Note that $\mathrm{Exp}_M^N(\delta) \subset \mathrm{Orb}_M^N(\delta)$, and that every set in $\mathrm{Orb}_M^N(\delta)$ is a finite union of sets in $\mathrm{Exp}_M^N(\delta)$. Hence Lemma 6.3 is true of the class $\mathrm{Exp}_M^N(\delta)$ as well. Also, note that for any $c, a_1, \ldots, a_n \in M$ and any $\delta_1, \ldots, \delta_n \in \mathbb{N}$ dividing δ, $c + S(a_1, \ldots, a_n; \delta_1, \ldots, \delta_n) \in \mathrm{Exp}_M(\delta)$.

The purpose of introducing these exponential F-sets is that they admit a well-defined notion of dimension. Suppose δ is a multiple of δ_M and $S \in \mathrm{Exp}_M(\delta)$. Then $S = F^B\overline{a}$ for some tuple $\overline{a}$ and some δ-closed set B. Now suppose that for some other tuple $\overline{b}$ and δ-closed set C, $S = F^C\overline{b}$. Denote by $[B]_{\overline{a}}$ and $[C]_{\overline{b}}$ the set of $\overline{a}$-equivalence and $\overline{b}$-equivalence classes of B and C respectively. Let $X := \log_{(\overline{a},-\overline{b})} 0 \cap (B \times C)$. Then $X \subset B \times C$ is a δ-closed relation (as δ_M divides δ). Moreover, X induces a δ-definable bijection between $[B]_{\overline{a}}$ and $[C]_{\overline{b}}$. In particular, $(\mathrm{RM}[B]_{\overline{a}}, \mathrm{dM}[B]_{\overline{a}}) = (\mathrm{RM}[C]_{\overline{b}}, \mathrm{dM}[C]_{\overline{b}})$, where Morley rank and degree are computed in $(\mathbb{N}, 0, \sigma, P_\delta)$. We can therefore make the following definition:

Definition 6.6. Fix $\delta > 0$ a multiple of δ_M, and let $S \in \mathrm{Exp}_M(\delta)$. The *$\delta$-dimension of S* (respectively, *δ-degree of S*), denoted by $\dim_\delta S$ (respectively $\deg_\delta S$), is the Morley rank (respectively Morley degree) of $[B]_{\overline{a}}$, where $B \subset \mathbb{N}^n$ is any δ-closed set and $\overline{a}$ is any n-tuple of elements from M such that $S = F^B\overline{a}$.

Remark 6.7.
(a) *δ-dimension and δ-degree are preserved under translation.* Indeed, $c + F^B\overline{a} = F^{(0\times B)}(c, \overline{a})$ and the δ-definable bijection between B and $0 \times B$ induces a δ-definable bijection between $[B]_{\overline{a}}$ and $[0 \times B]_{(c,\overline{a})}$.
(b) *If $S \subset T$ then* $(\dim_\delta S, \deg_\delta S) \leq (\dim_\delta T, \deg_\delta T)$. Indeed, if $T = F^B\overline{a}$ and $S = F^C\overline{b}$, then we can write $S = F^D\overline{a}$ where $D \subset B$ is the δ-closed set $D := \{\overline{r} \in B : \text{ for some } \overline{s} \in C, (\overline{r}, \overline{s}) \in \log_{(\overline{a},-\overline{b})} 0\}$.

The key property of this notion of dimension that we will make use of is contained in the following lemma.

Lemma 6.8. *Suppose $\delta > 0$ is a multiple of δ_M and $N \leq M$ is a submodule. Suppose $S, T \in \mathrm{Exp}_M^N(\delta)$ with $\dim_\delta S = \dim_\delta T$. There are $R_1, \ldots, R_\ell \in \mathrm{Exp}_M^N(\delta)$, such that for all $i \leq \ell$, $(\dim_\delta R_i, \deg_\delta R_i) < (\dim_\delta T, \deg_\delta T)$, and such that the following holds: if $c + S \subset T$ for some $c \in N$, then there exist $I \subset \{1, \ldots, \ell\}$ and $b_i \in N$ for each $i \in I$, such that* $[T \setminus (c + S)] \subset \bigcup_{i\in I} b_i + R_i$.

Proof. It suffices to do this for $N = M$. Indeed, if $T \in \mathrm{Exp}_M^N(\delta)$ and $T \setminus (c + S)$ is contained in $\bigcup_{i\in I} b_i + R_i$, then $[T \setminus (c+S)] \subset \bigcup_{i\in I}(b_i + R_i) \cap N$. Using Lemma 5.2, we can write $(b_i + R_i) \cap N = \bigcup_{j=1}^{\ell_i} b_{ij} + R_{ij}$, where each $b_{ij} \in N$ and $R_{ij} \in \mathrm{Orb}_M^N$. The R_{ij}'s come from a finite collection that depends only on R_i and N. Inspecting the proof of Lemma 5.2, and observing that F^{δ_M} also fixes $F^\infty N$ pointwise, we actually find these R_{ij}'s in $\mathrm{Orb}_M^N(\delta)$. Taking finite unions, we find the R_{ij}'s in $\mathrm{Exp}_M^N(\delta)$. So we assume that $N = M$.

Let $T = F^B\overline{a}$ and $S = F^C\overline{b}$, where B and C are δ-closed. If $c + S \subset T$ then $c + S = F^{D(c)}\overline{a}$, where $D(c) := \{\overline{r} \in B : \text{ for some } \overline{s} \in C, (\overline{r}, \overline{s}) \in \log_{(\overline{a},-\overline{b})} c\}$. By the uniformity in our description of $\log_{(\overline{a},-\overline{b})} c$ from Theorem 4.3, we obtain that there is a uniformly δ-definable family of δ-closed subsets of B, $(D_{\overline{t}})_{\overline{t}}$ such that for each c with $c + S \subset T$, there is a $\overline{t}$ with $c + S = F^{D_{\overline{t}}}\overline{a}$.

Let $d = \dim_\delta T$ and $r = \deg_\delta T$. The next step is to show that there is a uniformly δ-definable family of δ-definable sets $(X_{\overline{t}})_{\overline{t}}$, such that for each c with

$c+S \subset T$, there is a $\overline{t}$ with $[T \setminus (c+S)] = F^{X_{\overline{t}}\overline{a}}$ and $(\mathrm{RM}, \mathrm{dM})(X_{\overline{t}}) < (d,r)$. Let $\hat{B}$ and $\hat{D}_{\overline{t}}$, for each $\overline{t}$, denote the saturation with respect to $\overline{a}$-equivalence of the sets B and $D_{\overline{t}}$ respectively. Let $Y_{\overline{t}} := \hat{B} \setminus \hat{D}_{\overline{t}}$. Finally, using Corollary A.3 of the appendix, we find a uniformly definable family of δ-definable subsets $X_{\overline{t}} \subset Y_{\overline{t}}$ with $[X_{\overline{t}}]_{\overline{a}} = [Y_{\overline{t}}]_{\overline{a}}$ and $(\mathrm{RM}, \mathrm{dM})(X_{\overline{t}}) = (\mathrm{RM}, \mathrm{dM})([Y_{\overline{t}}]_{\overline{a}})$.[6] Now let c be such that $c+S \subset T$, and $\overline{t}$ such that $c+S = F^{D_{\overline{t}}\overline{a}}$. Then $F^{X_{\overline{t}}\overline{a}} = F^{Y_{\overline{t}}\overline{a}} = T \setminus (c+S)$. Moreover, as $(\mathrm{RM}, \mathrm{dM})([B]_{\overline{a}}) = (d,r)$ and $\mathrm{RM}([D_{\overline{t}}]_{\overline{a}}) = \dim_\delta S = d$, we have that

$$(d,r) > (\mathrm{RM}, \mathrm{dM})([B]_{\overline{a}} \setminus [D_{\overline{t}}]_{\overline{a}}) = (\mathrm{RM}, \mathrm{dM})(X_{\overline{t}}),$$

as desired.

There exists a finite union of δ-varieties, V, such that for each $\overline{t}$, $X_{\overline{t}} \subset V_{\overline{t}}$ and $(\mathrm{RM}, \mathrm{dM})(V_{\overline{t}}) = (\mathrm{RM}, \mathrm{dM})(X_{\overline{t}})$.[7] So for every c with $c+S \subset T$, there is a $\overline{t}$ such that $[T \setminus (c+S)] \subset F^{V_{\overline{t}}\overline{a}}$ and $(\dim_\delta, \deg_\delta)(F^{V_{\overline{t}}\overline{a}}) < (d,r)$. Finally, by Lemma 4.2, $(V_{\overline{t}})_{\overline{t}}$ is a uniform family of unions of disjoint-translates of fixed δ-varieties, and hence $(F^{V_{\overline{t}}\overline{a}})_{\overline{t}}$ is a uniform family of unions of translates of fixed sets in $\mathrm{Exp}_M(\delta)$. This completes the proof of the lemma. $\square$

We are now in a position to prove the stability of F-structures. But before doing so, we introduce some terminology regarding elementary extensions of F-structures.

Definition 6.9. Let $({}^*M, {}^*\mathcal{F})$ be an elementary extension of $(M, \mathcal{F})$. If $X \in \mathcal{F}(M)$, then by ${}^*X$ we mean the interpretation of X in $({}^*M, {}^*\mathcal{F})$. By an *F-set in ${}^*M$* we will mean a finite union of sets of the form $\alpha + {}^*X$ where $X \in \mathcal{F}(M)$ and $\alpha \in {}^*M$.

Remark 6.10.
(a) F-sets in ${}^*M$ are preserved under intersections. Moreover, if A is an F-set in ${}^*M$ and $G \leq M$ is a submodule, then $A \cap {}^*G$ is an F-set in ${}^*G$. Indeed, the former is obtained from transfer by Corollary 5.5, and the latter is obtained from transfer by Remark 5.6.
(b) Every definable set in $({}^*M, {}^*\mathcal{F})$ is a boolean combination of F-sets in ${}^*M$. Indeed, by quantifier elimination, every definable subset of ${}^*M^n$ is a boolean combination of fibres $({}^*X)_c$ where $X \in \mathcal{F}(M^{(m+n)})$ and $c \in {}^*M^m$. Now $({}^*X)_c$ is the projection onto the last n co-ordinates of $({}^*X) \cap (c \times {}^*M)$, and
$$({}^*X) \cap (c \times {}^*M) = (c, 0) + [(-c, 0) + {}^*X] \cap {}^*(0 \times M).$$
Hence $({}^*X) \cap (c \times {}^*M)$ is an F-set in ${}^*M^{(m+n)}$ (it is a translate of an intersection of such). Hence $({}^*X)_c$ is an F-set in ${}^*M^n$.

Theorem 6.11. *Let M be a finitely generated R-module and $({}^*M, {}^*\mathcal{F})$ an elementary extension of the F-structure $(M, \mathcal{F})$. Every 1-type over ${}^*M$ is ${}^*M$-definable. That is, $\mathrm{Th}(M, \mathcal{F})$ is stable.*

Proof. By the above remark, it suffices to show that for any $U \in \mathrm{Groupless}(M)$ and $G \leq M$ a submodule, the set $D_{U,G}(p) := \{a \in {}^*M : p(x) \vdash x \in a + {}^*U + {}^*G\}$ is ${}^*M$-definable. Let π denote reduction modulo G and $N := M/G$. If $p = \mathrm{tp}(\alpha/{}^*M)$, then we set $p/G := \mathrm{tp}(\pi\alpha/{}^*N)$. If we know that $D_{\pi(U),0}(p/G)$ is ${}^*N$-definable, then $D_{U,G}(p)$ is ${}^*M$-definable. Thus it suffices to show that for any $U \in \mathrm{Groupless}(M)$ the set $D_U(p) := D_{U,0}(p)$ is ${}^*M$-definable. Now, there exists a finitely generated R-module M' extending M, such that $U \in \mathrm{Orb}^M_{M'}$. Moreover, for some $\delta > 0$ a multiple of $\delta_{M'}$, $U \in \mathrm{Orb}^M_{M'}(\delta)$. Finally, U is a finite union of sets from $\mathrm{Exp}^M_{M'}(\delta)$.

[6] The uniformity comes from the fact that Corollary A.3 holds for *any* model of $\mathrm{Th}(\mathbb{N}, 0, \sigma, P_\delta)$.
[7] See Proposition A.6.

Hence, fixing a finitely generated R-module M' extending M, and fixing $\delta > 0$ a multiple of $\delta_{M'}$, it suffices to show that for all $S \in \operatorname{Exp}^M_{M'}(\delta)$, the set

$$D_S(p) = \{a \in {}^*M : p(x) \vdash x \in a + {}^*S\}$$

is ${}^*M$-definable.

If for all T in $\operatorname{Exp}^M_{M'}(\delta)$ the sets $D_T(p)$ are empty, then they are certainly ${}^*M$-definable. So, we may assume that some $D_T(p) \neq \varnothing$. Let $T \in \operatorname{Exp}^M_{M'}(\delta)$ have minimal $(\dim_\delta, \deg_\delta)$ (among the sets in $\operatorname{Exp}^M_{M'}(\delta)$) with the property that for some $b \in {}^*M$, $p(x) \vdash x \in b + {}^*T$. Fix such a choice of b. We prove that for all $S \in \operatorname{Exp}^M_{M'}(\delta)$, $D_S(p)$ is b-definable. For $S \in \operatorname{Exp}^M_{M'}(\delta)$, let $R_1, \dots, R_\ell \in \operatorname{Exp}^M_{M'}(\delta)$ be such that for any $x, y \in {}^*M$, $(x + {}^*S) \cap (y + {}^*T) = \bigcup_{i \in I} x_i + {}^*R_i$ for some $I \subset \{1, \dots, \ell\}$ and $x_i \in {}^*M$ (these exist by Lemma 6.3 and transfer). Let J be the set of indices $j \leq \ell$ such that $\dim_\delta R_j = \dim_\delta T$. We claim that

$$D_S(p) = \{a : (\exists y) \bigvee_{j \in J} y + {}^*R_j \subseteq (a + {}^*S) \cap (b + {}^*T)\}.$$

This would prove that $D_S(p)$ is b-definable, as desired.

For one direction, suppose that $a \in D_S(p)$. Then $p(x) \vdash x \in (a + {}^*S) \cap (b + {}^*T)$. Now $(a + {}^*S) \cap (b + {}^*T) = \bigcup_{i \in I} c_i + {}^*R_i$ for some $c_i \in {}^*M$ and $I \subset \{1, \dots, \ell\}$. As $p(x)$ is consistent, $I \neq \varnothing$. As $p(x)$ is complete, $p(x) \vdash x \in c_i + {}^*R_i$ for some $i \in I$. By minimality of $(\dim_\delta, \deg_\delta)(T)$, $\dim_\delta R_i = \dim_\delta T$. Conversely, suppose that for some some $c \in {}^*M$ and some $j \in J$, $c + {}^*R_j \subseteq (a + {}^*S) \cap (b + {}^*T)$. If $a \notin D_S(p)$, then $p(x) \vdash x \in b + ({}^*T \setminus [(c - b) + {}^*R_j])$. By Proposition 6.8 and transfer, there are $d_1, \dots, d_m \in {}^*M$ and $R'_1, \dots, R'_m \in \operatorname{Exp}^M_{M'}(\delta)$, such that

$${}^*T \setminus [(c - b) + {}^*R_j] \subset \bigcup_{i=1}^m d_i + {}^*R'_i;$$

and for each $i \leq m$, $(\dim_\delta R'_i, \deg_\delta R'_i) < (\dim_\delta T, \deg_\delta T)$. Now for some $i \leq m$, $p(x) \vdash x \in b + d_i + {}^*R'_i$, contradicting the minimal choice of T. $\square$

Remark 6.12. The proof of Theorem 6.11 yields a stronger conclusion: $\operatorname{Th}(M, \mathcal{F})$ is superstable. As we will not make use of this fact, we provide only an outline of the argument here. For $G \leq M$ a submodule we define $d(G) := \dim_{\mathbb{Q}}(G \otimes \mathbb{Q})$. For $U \in \operatorname{Groupless}(M)$ we define $d_G(U)$ to be, essentially, $\dim_\delta(\pi U)$ for an appropriate δ where $\pi : M \to M/G$ is the quotient map. We say "essentially" because πU need not belong to $\operatorname{Exp}_{M/G}(\delta)$ for any δ. Rather, we choose a finitely generated R-module $M' \geq M/G$ and $\delta > 0$ a multpile of $\delta_{M'}$, for which $\pi U \in \operatorname{Orb}_{M'}(\delta)$. We then choose an expression of πU as a finite union of elements of $\operatorname{Exp}_{M'}(\delta)$, and define $d_G(U)$ to be the maximal δ-dimension of the sets that appear in this expression. It is a routine matter to check that $d_G(U)$ is well-defined. For a 1-type $p \in S(A)$ over an elementary substructure A of ${}^*M$, we define $R(p)$ to be the minimum, with respect to the lexicographic order, of $\langle d(G), d_G(U)\rangle$ for which $D_{U,G}(p) \neq \emptyset$. Using the techniques of the proof of Theorem 6.11 one then shows that if $A \preceq {}^*M$ is an elementary substructure and $p \in S({}^*M)$ forks over A, then $R(p) < R(p \restriction A)$. Consequently, there is no infinite forking chain and $\operatorname{Th}(M, \mathcal{F})$ is superstable. The details of this routine, though lengthy, argument are left to the reader.

7. Mordell-Lang for Isotrivial Semiabelian Varieties

In this section we prove Theorems B, C, and D. Our strategy is to first prove Theorem B using some particular properties of F-sets in the algebro-geometric context of Example 2.2. We then apply the theory of F-structures developed in the previous sections, to deduce the stability of the structure induced on a finitely generated $\mathbb{Z}[F]$-submodule of a semiabelian variety over a finite field. Together with some further analysis, this will allow us to obtain the desired uniformity in the Mordell-Lang statement.

For the rest of this section we work in the following context: *G is a semiabelian variety over a finite field $\mathbb{F}_q$ of characteristic p, $F\colon G \to G$ is the algebraic endomorphism induced by the q-power Frobenius map $x \mapsto x^q$, and $R = \mathbb{Z}[F]$ is the subring of the endomorphism ring of G generated by F.* As pointed out in Example 2.2, $R = \mathbb{Z}[F]$ does satisfy the required properties stated at the begining of Section 2. Unlike in that section, we do not yet fix a finitely generated regular extension, K of $\mathbb{F}_q$, and consider only finitely generated R-submodules of $G(K)$. Instead, we let $\mathcal{U}$ *be any fixed algebraically closed field of characteristic* p, and we considering arbitrary finitely generated R-submodules of $G(\mathcal{U})$.

For the sake of readability, if the context is unambigious, we will identify a variety X over $\mathcal{U}$ with its $\mathcal{U}$-rational points (instead of writing $X(\mathcal{U})$).

The following lemma says that we can resolve cycles into orbits within the class of finitely generated R-submodules of $G(\mathcal{U})$.

Lemma 7.1. *Suppose $\Gamma \leq G(\mathcal{U})$ is a finitely generated R-submodule. Then for any $U \in \mathrm{Groupless}(\Gamma)$ there exists a finitely generated R-submodule $\Gamma' \leq G(\mathcal{U})$ extending Γ, such that $U \in \mathrm{Orb}_{\Gamma'}$.*

Proof. As in the proof of Lemma 2.7, it suffices to show that for any $b \in \Gamma$ and $\delta > 0$, there is a finitely generated $\Gamma' \leq G(\mathcal{U})$ extending Γ such that for some $a \in \Gamma'$, $F^\delta a - a = b$. But $(F^\delta - 1)\colon G \to G$ is an isogeny, and hence $(F^\delta - 1)(x) = b$ has a solution in $G(\mathcal{U})$. Let Γ' be the R-submodule generated over Γ by some such solution $a \in G(\mathcal{U})$. □

Lemma 7.2. *Let $\Gamma \leq G(\mathcal{U})$ be a finitely generated R-submodule, $\overline{a} = (a_1, \ldots, a_m)$ a tuple of elements of Γ, $\delta > 0$, and $\Lambda \leq \Gamma$ a submodule. Let $K \subset \mathcal{U}$ be a finitely generated field extension of $\mathbb{F}_q$ such that $\Gamma \leq G(K)$ and let $r > 0$ be such that $K \cap \mathbb{F}_q^{\mathrm{alg}} = \mathbb{F}_{q^r}$.*

(a) *The Zariski closure of $S(\overline{a}; \delta) + \Lambda$ is defined over $\mathbb{F}_{q^r} \cap \mathbb{F}_{q^\delta}$.*

(b) $S(\overline{a}; r) + \Lambda \subset \overline{S(\overline{a}; \delta) + \Lambda}$.

Proof. Let $A := S(\overline{a}; \delta) + \Lambda$. Then $F^\delta A \subset A$, and hence $F^\delta(\overline{A}) = \overline{A}$. It follows that $\overline{A}$ is defined over $\mathbb{F}_{q^\delta}$. As it is the Zariski closure of some points in $G(K)$, it is also defined over K. So $\overline{A}$ is defined over $\mathbb{F}_{q^r} \cap \mathbb{F}_{q^\delta}$, proving part (a).

For part (b), we may assume that δ is a multiple of r. Indeed, letting $\delta' = \delta r$, we see that $S(\overline{a}; \delta') + \Lambda \subset S(\overline{a}; \delta) + \Lambda$, and so the Lemma would follow once we know that $S(\overline{a}; r) + \Lambda \subset \overline{S(\overline{a}; \delta') + \Lambda}$.

We proceed by induction on m. For $m = 1$, note that as $\Lambda \subset G(K)$ and $F\Lambda \subset \Lambda$, $\overline{\Lambda}$ is defined over $K \cap \mathbb{F}_q^{\mathrm{alg}} = \mathbb{F}_{q^r}$. Hence, $Y := \{d \in G : d + \overline{\Lambda} \subset \overline{A}\}$ is over $\mathbb{F}_{q^r}$, and so $F^r Y = Y$. But $S(a; \delta) \subset Y$ and so $S(a; r) \subset Y$, as δ is a multiple of r. It follows that $S(a; r) + \Lambda \subset \overline{A}$, as desired. Now suppose $m > 1$.

Let $B := S(a_2, \ldots, a_m; \delta) + \Lambda$. By part (a), $\overline{B}$ is defined over $\mathbb{F}_{q^r}$. So $Z := \{d \in G : d + \overline{B} \subset \overline{A}\}$ is over $\mathbb{F}_{q^r}$, and $F^r Z = Z$. Again, as $S(a_1; \delta) \subset Z$, $S(a_1; r) \subset Z$. On the other hand, by the induction hypothesis, $S(a_2, \ldots, a_m; r) + \Lambda \subset \overline{B}$. Hence, $S(\overline{a}; r) + \Lambda = S(a_1; r) + S(a_2, \ldots, a_m; r) + \Lambda \subset S(a_1; r) + \overline{B} \subset \overline{A}$, as desired. □

Corollary 7.3. *Suppose $\Gamma \leq G(\mathcal{U})$ is a finitely generated R-module, $A \in \mathcal{F}(\Gamma)$, and $X \subset G$ is a closed subvariety. Let $\Sigma := \bigcup_{n \geq 0} F^n A$, and suppose that $\Sigma \subset X$. Then there exists $B \in \mathcal{F}(\Gamma)$ such that $\Sigma \subset B \subset X$.*

Proof. Taking finite union we may assume that $A = U + \Lambda$, where $U \in \mathrm{Groupless}(\Gamma)$ and $\Lambda \leq \Gamma$ is a submodule. Moreover, by Lemma 7.1, there is a $\Gamma' \leq G(\mathcal{U})$ such that $U \in \mathrm{Orb}_{\Gamma'}$. Now if we find $B' \in \mathcal{F}(\Gamma')$ such that $\Sigma \subset B' \subset X$, then letting $B := B' \cap \Gamma \in \mathcal{F}(\Gamma)$, we would have $\Sigma \subset B \subset X$. So we may assume that $\Gamma' = \Gamma$, and that $A = S + \Lambda$ for some $S \in \mathrm{Orb}_\Gamma$ and $\Lambda \leq \Gamma$ a submodule.

Let $K \subset \mathcal{U}$ be a finitely generated field extension of $\mathbb{F}_q$ such that $\Gamma \leq G(K)$. Let $r > 0$ be such that $K \cap \mathbb{F}_q^{\mathrm{alg}} = \mathbb{F}_{q^r}$. Note that

$$\Sigma = \bigcup_{n \geq 0} F^n A = \bigcup_{n \geq 0} F^{rn}(A \cup FA \cup \cdots \cup F^{(r-1)}A).$$

Moreover, for each $0 \leq i < r$, $F^i A$ is again of the form $S_i + \Lambda$. Hence it suffices to prove the following statement: *For all $S \in \mathrm{Orb}_\Gamma$ and $\Lambda \leq \Gamma$ a submodule, if $\Sigma' := \bigcup_{n \geq 0} F^{rn}(S + \Lambda) \subset X$, then there exists $B \in \mathcal{F}(\Gamma)$ such that $\Sigma' \subset B \subset X$.* Taking finite unions, we may assume that $S = b + S(\overline{a}; \delta)$ where $b, \overline{a}$ are from Γ and $\delta > 0$ is a multiple of r (see Remark 6.2).

Let $B := S(b, \overline{a}; r) + \Lambda$. Then it is not hard to see, using that δ is a multiple of r, that $\Sigma' \subset B$. We are left to show that $B \subset X$. Fix $n \geq 0$. Then

$$\begin{aligned} F^{rn}b + S(\overline{a}; r) + \Lambda &\subset F^{rn}b + \overline{S(\overline{a}; r) + \Lambda} \\ &\subset F^{rn}b + \overline{S(\overline{a}; \delta) + \Lambda} \\ &= F^{rn}[b + \overline{S(\overline{a}; \delta) + \Lambda}] \\ &= F^{rn}(\overline{S + \Lambda}) \subset \overline{\Sigma'} \subset X, \end{aligned}$$

where the second inclusion is by part (b) of Lemma 7.2, and the equality following it is by part (a) of that Lemma. It follows that $B \subset X$. □

Lemma 7.4. *Suppose $K \subset \mathcal{U}$ is a finitely generated regular field extension of $\mathbb{F}_q$, $\Gamma \leq G(K)$ is a finitely generated R-module, $X \subset G$ is a closed subvariety, and $r > 0$. We can view Γ as a $\mathbb{Z}[F^r]$-submodule of $G(\mathcal{U})$ as well. If $A \subset \Gamma$ is an F^r-set with $A \subset X$, then there exists $B \in \mathcal{F}(\Gamma)$ with $A \subset B \subset X$.*

Proof. We may assume that $A = U + \Lambda$ where U is a groupless F^r-set and Λ is a $\mathbb{Z}[F^r]$-submodule of Γ. Let $H \leq G$ be the Zariski closure of Λ in G. Then H is defined over $\mathbb{F}_q^{\mathrm{alg}}$ (every algebraic subgroup of G is) and over K (it has a Zariski-dense intersection with $G(K)$), and so over $\mathbb{F}_q$. It follows that $H \cap \Gamma$ is a $\mathbb{Z}[F]$-submodule of Γ. Moreover, by definition, every groupless F^r-set is an F-set. So $B := U + H \cap \Gamma$ is an F-set. Clearly $A \subset B$. Moreover, if $A \subset X$, then for each $a \in U$, $a + H \cap \Gamma \subset \overline{a + \Lambda} \subset X$. Hence $B \subset X$. □

Lemma 7.5. *Suppose $\Gamma \leq G(\mathcal{U})$ is a finitely generated R-submodule. Let $K \subset \mathcal{U}$ be a finitely generated field extension of $\mathbb{F}_q$ such that $\Gamma \leq G(K)$.*

(a) *The F-pure hull of Γ in $G(K)$ – i.e., the set of $g \in G(K)$ such that $F^n g \in \Gamma$ for some n – is a finitely generated group. In particular, Γ itself is a finitely generated group.*
(b) *For all $n \geq 0$, $\Gamma / F^n\Gamma$ is a finite set.*
(c) *There exists $m > 0$, such that $\Gamma \setminus F\Gamma \subset G(K) \setminus G(K^{q^m})$.*

Proof. Part (a) is clear in the case when G is an abelian variety, since in that case $G(K)$ is itself a finitely generated group. For the general case, we can choose $\mathcal{R} \subset K$ an integrally closed ring that is finitely generated over $\mathbb{F}_q$ (as a ring), and such that $\Gamma \leq G(\mathcal{R})$. Now $G(\mathcal{R})$ is a finitely generated group, and since $K^q \cap \mathcal{R} = \mathcal{R}^q$, it is F-pure in $G(K)$. Hence the F-pure hull of Γ in $G(K)$, Γ', is a subgroup of $G(\mathcal{R})$. It follows that Γ' is itself a finitely generated group.

Recall that the multiplication by q^n map on $G(K)$ is equal to $F^n \circ V^n$, where $V \colon G(K) \to G(K)$ is the Verschiebung map. As Γ' is F-pure in $G(K)$, it follows that V restricts to an endomorphism of Γ', and that $q^n\Gamma' \subset F^n\Gamma'$. Now $\Gamma'/q^n\Gamma'$, being a finitely generated $\mathbb{Z}/q^n\mathbb{Z}$-module, is finite. Hence $\Gamma'/F^n\Gamma'$ is finite for all n. Now consider Γ itself, and let n be arbitrary. As Γ' is a finitely generated group, for some $N > 0$, $F^N\Gamma' \subset \Gamma$. So $\Gamma'/F^n\Gamma$ is a quotient of the finite group $\Gamma'/F^{n+N}\Gamma'$. Hence $\Gamma/F^n\Gamma$ is finite, establishing part (b).

Finally, for (c), let $N > 0$ again be such that $F^N\Gamma' \subset \Gamma$, and let $m = N + 1$. Then $\Gamma \cap G(K^{q^m}) \subset F^m\Gamma' \subset F\Gamma$. It follows that $\Gamma \setminus F\Gamma \subset G(K) \setminus G(K^{q^m})$. □

Remark 7.6. In what follows we will implicitly use the following fact: *Let L be a field possibly equipped with additional structure. Suppose Y is a variety defined over L, $\Upsilon \subseteq Y(L)$ is a set definable in L, and $\{X_b\}_{b\in B}$ is an algebraic family of subvarieties of Y defined over L. Then the condition that $X_b(L) \cap \Upsilon$ is Zariski-dense in X_b is a type-definable condition on b.* Indeed, $X_b(L) \cap \Upsilon$ is Zariski-dense in X_b if and only if for ever proper algebraic subset V of X_b over L, there exists $a \in X_b(L) \cap \Upsilon \setminus V(L)$. The remark follows once one observes that V being a proper algebraic subset of X_b is a definable (in $(L, +, \times, 0, 1)$) property of b and the parameters for V. This set is clearly definable in $(L^{\mathrm{alg}}, +, \times, 0, 1)$ and is therefore constructible by quantifier elimination. As quantifier-free formulae are preserved in substructures, the quantifier-free definition in L^{alg} serves also to define this set in L.

The following proposition was shown in [1] using a Hilbert scheme argument, and is also a very special case of Hrushovski's function field Mordell-Lang Theorem in positive characteristic [2]. We present an elementary model-theoretic argument that appeared in unpublished notes of the first author.

Proposition 7.7. *Suppose $\Gamma \leq G(\mathcal{U})$ is a finitely generated group and $X \subset G$ is a closed subvariety such that $X \cap \Gamma$ is Zariski-dense in X. Then for some $\gamma \in G(\mathcal{U})$, $\gamma + X$ is defined over $\mathbb{F}_q^{\mathrm{alg}}$.*

Proof. Let $K \subset \mathcal{U}$ be a finitely generated field extension of $\mathbb{F}_q$ such that $\Gamma \leq G(K)$. Note that X is defined over K, since it has a dense intersection with $G(K)$. Let $L \subset \mathcal{U}$ denote the separable algebraic closure of K. Since K is a finitely generated extension of $\mathbb{F}_q$, we have that $\bigcap_{n\geq 0} L^{q^n} = \mathbb{F}_q^{\mathrm{alg}}$. Finally, let ${}^*L$ be an ω_1-saturated elementary extension of L (as a field), and let $k = \bigcap_{n\geq 0} ({}^*L)^{q^n}$.

We claim that $(({}^*L)^{\mathrm{alg}}, k)$ is an elementary extension of $(L^{\mathrm{alg}}, \mathbb{F}_q^{\mathrm{alg}})$ as pairs of fields. Indeed, it suffices to show that L^{alg} is algebraically disjoint from k over $\mathbb{F}_q^{\mathrm{alg}}$.[8] This in turn reduces to showing that L is *linearly* disjoint from k over $\mathbb{F}_q^{\mathrm{alg}}$, which is what we do: Let $B_n \subset L$, for $n > 0$, be an increasing chain of finite sets such that each B_n is a linear basis for L over L^{q^n}. Then $B := \bigcup_{n>0} B_n$ is a linear basis for L over $\mathbb{F}_q^{\mathrm{alg}}$. We need to show that B is linearly independent over k. For this, it suffices to show that for each $n > 0$, B_n is linearly independent over k. But it follows immediately from $L \preceq {}^*L$, that $({}^*L)^{q^n}$ is linearly disjoint from L over L^{q^n}. Hence B_n is linearly independent over $({}^*L)^{q^n}$, and so over k.

Now fix $n > 0$. As Γ is a finite union of cosets of $F^n\Gamma$, and $X(L) \cap \Gamma$ is Zariski-dense in X, for some $\gamma \in \Gamma$, $(\gamma + X)(L) \cap F^n\Gamma$ is Zariski-dense in $\gamma + X$. Hence $(\gamma+X)(L)\cap G(L^{q^n})$ is Zariski-dense in $\gamma+X$. Now this is a type-definable property of γ (see Remark 7.6), say by a partial type $p_n(x)$. Note that $p_m(x)$ implies $p_n(x)$ for $m \geq n$. Hence, $\bigcup_{n>0} p_n(x)$ is consistent. It follows by saturation of ${}^*L$, that there is ${}^*\gamma \in G({}^*L)$ such that $({}^*\gamma + X)({}^*L) \cap G({}^*L^{q^n})$ is Zariski-dense in ${}^*\gamma + X$ for all n. By saturation again, $({}^*\gamma + X)(k)$ is Zariski-dense in ${}^*\gamma + X$. It follows that ${}^*\gamma + X$ is defined over k.

In particular, we have shown that some translate of X by an element of $G(({}^*L)^{\mathrm{alg}})$ is defined over k. This can be witnessed by a first-order sentence (with parameters from K), true of $(({}^*L)^{\mathrm{alg}}, k)$. By transfer, it is true of $(L^{\mathrm{alg}}, \mathbb{F}_q^{\mathrm{alg}})$. As $L^{\mathrm{alg}} \subset \mathcal{U}$, this proves the proposition. □

We are now ready to prove the main result of this section: a version of the absolute Mordell-Lang conjecture for isotrivial semiabelian varieties in positive characteristic. This proof is based on an argument that was first presented by the second author in the e-print [9].

Theorem 7.8. *Suppose G is a semiabelian variety over a finite field $\mathbb{F}_q$, $F\colon G \to G$ is the algebraic endomorphism induced by the q-power Frobenius map, $R = \mathbb{Z}[F]$ is the subring of the endomorphism ring of G generated by F, $\mathcal{U}$ is an algebraically closed field, and $K \subset \mathcal{U}$ is a finitely generated regular field extension of $\mathbb{F}_q$.*

If $X \subseteq G$ is a closed subvariety, and $\Gamma \leq G(K)$ is a finitely generated R-submodule, then $X(K) \cap \Gamma \in \mathcal{F}(\Gamma)$. Moreover, the submodules of Γ that appear are of the form $H(K) \cap \Gamma$ where $H \leq G$ is an algebraic subgroup over $\mathbb{F}_q$.

Proof. We first observe that the "moreover" clause follows from the main statement. Indeed, if $\Lambda \leq \Gamma$ is a submodule that appears in the expression of $X \cap \Gamma$ as an F-set, then replacing Λ by $H \cap \Gamma$, where H is the Zariski closure of Λ in G, does not change $X \cap \Gamma$ (see the proof of Lemma 7.4). Moreover, H is defined over $\mathbb{F}_q$, as it is defined over both K and $\mathbb{F}_q^{\mathrm{alg}}$.

We proceed by induction on $\dim X$. When $\dim X = 0$ the theorem is trivially true. Suppose $0 < d := \dim X$. We may assume that X is irreducible. Moreover, as $X \cap \Gamma = (\overline{X \cap \Gamma}) \cap \Gamma$, we may also assume that $X \cap \Gamma$ is Zariski-dense in X.

[8]See, for example, Poizat [7].

Next, we argue that we may assume X is over $\mathbb{F}_q$. By Proposition 7.7 there is some $\gamma \in G(\mathcal{U})$ such that $\gamma + X$ is defined over $\mathbb{F}_q^{\mathrm{alg}}$. Let $\Gamma' = \Gamma < \gamma >$ be the R-submodule of $G(\mathcal{U})$ generated by Γ and γ. Let K' be a finitely generated field extension of $\mathbb{F}_q$ such that $\Gamma' \leq G(K')$. Let $r > 0$ be such that $K' \cap \mathbb{F}_q^{\mathrm{alg}} = \mathbb{F}_{q^r}$. So K' is a regular extension of $\mathbb{F}_{q^r}$ and we can view Γ' as a $\mathbb{Z}[F^r]$-submodule of $G(K')$. Moreover, $\gamma+X$ is now defined over both $\mathbb{F}_q^{\mathrm{alg}}$ and K' (the latter since it has a dense intersection with $G(K')$) – and hence over $\mathbb{F}_{q^r}$. Assuming the result in this case we obtain $(\gamma+X)\cap\Gamma'$ is an F^r-set, and so $X\cap\Gamma' = -\gamma+((\gamma+X)\cap\Gamma')$ is also an F^r-set in Γ'. Note that Γ is a $\mathbb{Z}[F^r]$-submodule of Γ', and hence $X \cap \Gamma = (X \cap \Gamma') \cap \Gamma$ would be an F^r-set in Γ (by part (b) of Proposition 3.9). But by Lemma 7.4, this would in turn imply that $X \cap \Gamma$ is an F-set in Γ.

Finally, we may also assume that X has a trivial stabilizer. Let $H = \mathrm{Stab}_G(X)$ be the stabilizer of X in G as an algebraic group. Then H is defined over $\mathbb{F}_q$. Let $\pi : G \to G/H =: \hat{G}$ be the quotient map. Set $\hat{\Gamma} := \pi(\Gamma)$ and $\hat{X} := \pi(X)$. Then $\mathrm{Stab}_{\hat{G}}(\hat{X})$ is trivial. Assuming the result in this case, we have that $\hat{X} \cap \hat{\Gamma} \in \mathcal{F}(\hat{\Gamma})$ and $\pi(X \cap \Gamma) = \hat{X} \cap \hat{\Gamma}$. Using the fact that the kernel of $\pi\restriction_\Gamma$ stabilizes $X \cap \Gamma$, we have $X \cap \Gamma = \pi\restriction_\Gamma^{-1}(\hat{X} \cap \hat{\Gamma})$. So, it would follow that $X \cap \Gamma \in \mathcal{F}(\Gamma)$.

With these reductions in place, we claim that for some $N > 0$, if $\xi \in \Gamma \setminus F\Gamma$, then $(\xi + X) \cap G(K^{q^N})$ is *not* Zariski-dense in $\xi + X$. Suppose this were false, and let $(\xi_i)_{i\in\omega}$ be a sequence of points in $\Gamma \setminus F\Gamma$, and $(n_i)_{i\in\omega}$ a strictly increasing sequence of positive integers, such that $(\xi_i+X)\cap G(K^{q^{n_i}})$ is Zariski-dense in ξ_i+X. Using part (c) of Lemma 7.5, choose $m > 0$ such that $\Gamma \setminus F\Gamma \subset G(K) \setminus G(K^{q^m})$. Hence, each $\xi_i \in G(K)\setminus G(K^{q^m})$. Let ${}^*K$ be an ω_1-saturated elementary extension of K. Using Remark 7.6 and saturation, we obtain ${}^*\xi \in G({}^*K) \setminus G({}^*K^{q^m})$ such that $({}^*\xi + X)(k)$ is Zariski-dense in ${}^*\xi + X$, where $k = \bigcap_{n\geq 0} {}^*K^{q^n}$. It follows that ${}^*\xi + X$ is defined over k. But as X is defined over $\mathbb{F}_q \subset k$, we obtain that for all $\sigma \in \mathrm{Aut}(({}^*K)^{\mathrm{alg}}/k)$, $\sigma({}^*\xi) - {}^*\xi$ stabilises X. As $\mathrm{Stab}\, X$ is trivial, this means that σ fixes ${}^*\xi$. Hence, ${}^*\xi \in G(k) \subset G({}^*K^{q^m})$, which is a contradiction.

Now let $\xi \in \Gamma \setminus F\Gamma$, and choose coset representative $\eta_1, \dots \eta_\ell$ for $F^N\Gamma$ in $F\Gamma$. Then each $\xi + \eta_i \in \Gamma \setminus F\Gamma$, and hence $(\xi + \eta_i + X) \cap F^N\Gamma$ is not Zariski-dense in $(\xi+\eta_i+X)$. It follows that $\dim \overline{(\xi + X) \cap F\Gamma} = \dim(\bigcup_{i=1}^{\ell} \overline{(\xi + \eta_i + X) \cap F^N\Gamma}) < d$. By induction, $(\xi+X)\cap F\Gamma$ is an F-set in $F\Gamma$, and hence in Γ. We have shown that for all $\xi \in \Gamma \setminus F\Gamma$, $(\xi + X) \cap F\Gamma \in \mathcal{F}(\Gamma)$.

We now finish the proof. Note that because $\bigcap_{n\geq 0} F^nG(K) = G(\mathbb{F}_q)$, we can write $\Gamma = (G(\mathbb{F}_q) \cap \Gamma) \cup \bigcup_{n\geq 0} F^n(\Gamma \setminus F\Gamma)$. Fix coset representatives $\gamma_1, \dots, \gamma_\ell$ for the *nonzero* cosets of $F\Gamma$ in Γ. We have,

$$\begin{aligned} X\cap\Gamma &= X\cap(G(\mathbb{F}_q)\cap\Gamma)\cup\bigcup_{n\geq 0}[X\cap F^n(\Gamma\setminus F\Gamma)] \\ &= (X(\mathbb{F}_q)\cap\Gamma)\cup\bigcup_{n\geq 0}F^n(X\cap(\Gamma\setminus F\Gamma)) \\ &= (X(\mathbb{F}_q)\cap\Gamma)\cup\bigcup_{n\geq 0}F^n[\bigcup_{i=1}^{\ell}(\gamma_i+((-\gamma_i+X)\cap F\Gamma))] \end{aligned}$$

where the second equality uses the fact that X is defined over $\mathbb{F}_q$, and hence is fixed by powers of F. For each $i\leq\ell$, $\gamma_i\in\Gamma\setminus F\Gamma$, and so $(-\gamma_i+X)\cap F\Gamma\in\mathcal{F}(\Gamma)$. So $A_i := \bigcup_{i=1}^{\ell}(\gamma_i+((-\gamma_i+X)\cap F\Gamma))$ is an F-set. By Corollary 7.3, there exists $B\in\mathcal{F}(\Gamma)$ such that $\bigcup_{n\geq 0}F^n[\bigcup_{i=1}^{\ell}A_i]\subset B\subset X$. Hence $X\cap\Gamma=(X(\mathbb{F}_q)\cap\Gamma)\cup B$ is an F-set. □

By Lemma 7.1 we can even express $X(K)\cap\Gamma$ in terms of F-orbits and submodules (that is, without F-cycles) if we allow ourselves to pass to finitely generated R-submodules of $G(\mathcal{U})$ that extend Γ. The following example shows that in order to get rid of the F-cycles, one does, in general, have to pass to such extensions.

Example 7.9. Let C be a curve over $\mathbb{F}_q$ with geometric genus $g\geq 2$, $C(\mathbb{F}_q)\neq\emptyset$, and $\mathrm{Aut}(C)=\{\mathrm{id}_C\}$. We consider C as a subvariety of its Jacobian G over $\mathbb{F}_q$. We assume that $G(\mathbb{F}_q)$ is non-trivial (this is the case if $q>4^g$). Let $K:=\mathbb{F}_q(C)$, and let $\alpha:=\mathrm{id}_C$ be the identity on C thought of as an element of $C(K)\subset G(K)$. Let $\gamma:=F\alpha-\alpha$ and $\Gamma\leq G(K)$ be the $\mathbb{Z}[F]$-submodule generated by γ.

We observe that $\alpha\notin\Gamma$. Indeed, to say that $\alpha\in\Gamma$ is to say that there is some $\psi\in\mathbb{Z}[F]$ with $\alpha=\psi\circ(F-1)\alpha$, or what is the same, $(1-\psi(F-1))\alpha=0$. As α is the generic point of C and C generates its Jacobian, the annihilator of α is trivial. Thus, $1-\psi(F-1)=0$ and ψ is the inverse of $F-1$. But $F-1$, having the non-trivial kernel $G(\mathbb{F}_q)$, is not even invertible in $\mathrm{End}(G)$.

As every rational function between smooth curves is regular, we see that $C(K)$ may be identified with the set of regular functions from C to itself defined over $\mathbb{F}_q$. The constant maps comprise the set $C(\mathbb{F}_q)$. Every nonconstant map $\psi: C\to C$ factors as $\psi=\phi\circ F^m$ where $\phi: C\to C$ is separable. Using the Riemann-Hurwitz formula and the fact that the genus of C is at least two, one sees that ϕ must be an automorphism, but we have assumed that the only such automorphism is α. Hence, $\psi\in S(\alpha;1)$. We have shown that $C(K)=C(\mathbb{F}_q)\cup S(\alpha;1)$.

Set $X:=-\alpha+C$. So $X(K)=(-\alpha+C(\mathbb{F}_q))\cup\{0\}\cup(-\alpha+S(F\alpha;1))$. Note that $X(K)\cap\Gamma=\{0\}\cup(-\alpha+S(F\alpha;1))=\{0\}\cup C(\gamma;1)$. Thus, $X(K)\cap\Gamma$ is a groupless F-set in Γ, but cannot be expressed as a *cycle-free* groupless F-set in Γ. It is only cycle-free in $G(K)$.

Corollary 7.10. $\mathrm{Th}(\mathcal{U},+,\times,\Gamma)$ *is stable.*

Proof. Denote by Γ_{ind} the structure whose universe is Γ and whose relations are sets of the form $D\cap\Gamma^n$, where $D\subset G(\mathcal{U})^n$ is definable (with parameters) in $(\mathcal{U},+,\times)$. By Theorem 7.8, every definable set in Γ_{ind} is definable in $(\Gamma,\mathcal{F})$. That is, the structure induced on Γ by $(\mathcal{U},+,\times,\Gamma)$ is a reduct of $(\Gamma,\mathcal{F})$. By Theorem 6.11, Γ_{ind} is stable. By a result of Pillay's (namely Lemma 2.9 of [6] and the discussion following it) $(\mathcal{U},+,\times,\Gamma)$ is stable. □

Remark 7.11. Note that we can, in a certain sense, drop the assumption in Theorem 7.8 that $\Gamma \leq G(K)$, where K is a *regular* extension of $\mathbb{F}_q$. If $\Gamma \leq G(\mathcal{U})$ is any finitely generated $\mathbb{Z}[F]$-submodule, then $\Gamma \leq G(K')$ where K' is a finitely generated regular extension of $\mathbb{F}_{q^r}$ for some $r > 0$. Viewing Γ as an F^r-structure, we would obtain that $X \cap \Gamma$ is an F^r-set. It follows that in Corollary 7.10, Γ can be taken to be any finitely generated $\mathbb{Z}[F]$-submodule of $G(\mathcal{U})$.

Our final goal is to obtain a uniform version of Theorem 7.8. We will require some further observations about F-structures in this geometric context. We begin, however, with a lemma that holds in any F-structure, and that was essentially proved in Section 5.

Lemma 7.12. *For each $i \leq \ell$ suppose*

- $U_i = S_i + H_i$ *where* $S_i \in \text{Groupless}(\Gamma)$ *and* $H_i \leq \Gamma$ *is a submodule;*
- *for each* $i \leq \ell$, $V_i = \bigcup_{j=1}^{m_i} T_{ij} + K_{ij}$, *where* $T_{ij} \in \text{Groupless}(\Gamma)$ *and* K_{ij} *is a submodule of* H_i *of finite index;*
- *for each* $i \leq \ell$, $W_i = \bigcup_{j=1}^{n_i} R_{ij} + L_{ij}$, *where* $R_{ij} \in \text{Groupless}(\Gamma)$ *and* L_{ij} *is a submodule of* H_i *of infinite index.*

If there exists $A \in \mathcal{F}(\Gamma)$ *with* $\displaystyle\bigcup_{i=1}^{\ell} U_i \setminus (V_i \cup W_i) \subset A$, *then* $\displaystyle\bigcup_{i=1}^{\ell} U_i \setminus V_i \subset A$.

Proof. Fix $i \leq \ell$. We need to show that $U_i \setminus V_i \subset A$. Fix $d \in S_i$. Since by assumption $U_i \subset A \cup V_i \cup W_i$, we have that

$$d + H_i = [A \cap (d + H_i)] \cup [V_i \cap (d + H_i)] \cup [W_i \cap (d + H_i)].$$

Now by Corollary 5.10, $d + H_i = [A \cap (d + H_i)] \cup [V_i \cap (d + H_i)]$. Hence $U_i \subset A \cup V_i$, and so $U_i \setminus V_i \subset A$, as desired. □

Next we consider elementary extension. We let $*$ denote an elementary extension of the entire universe. In particular, if $\Gamma \leq G(\mathcal{U})$ is any finitely generated $\mathbb{Z}[F]$-submodule, then $({}^*\mathcal{U},+,\times,{}^*\Gamma,{}^*\mathcal{F})$ is an elementary extension of $(\mathcal{U},+,\times,\Gamma,\mathcal{F})$. Recall that every definable set in $({}^*\Gamma,{}^*\mathcal{F})$ is a boolean combination of F-sets in ${}^*\Gamma$; where an *F-set in* ${}^*\Gamma$ is by definition a finite union of sets of the form $\gamma + {}^*U + {}^*\Lambda$, where $\gamma \in {}^*\Gamma$, $U \in \text{Groupless}(\Gamma)$, and $\Lambda \leq \Gamma$ is a submodule.[9] We will call finite unions of such sets *groupless F-sets in* ${}^*\Gamma$ if no submodules appear, and *cycle-free groupless F-sets in* ${}^*\Gamma$ if the U's are in Orb_Γ.

What does Theorem 7.8 tell us about the nonstandard situation? First of all, by the more general form described in Remark 7.11, there is some $r > 0$ such that if $X \subset G$ is a subvariety over $\mathcal{U}$ then $X(\mathcal{U}) \cap \Gamma$ is an F^r-set in Γ. By uniform definability of types applied to the stable $\text{Th}(\mathcal{U},+,\times,\Gamma)$, as X varies in an algebraic family, $X(\mathcal{U}) \cap \Gamma$ will be uniformly *definable* in the F^r-structure on Γ. We cannot directly conclude that it is uniformly an F^r-set. Nevertheless, it follows that for $Z \subset G$ defined over ${}^*\mathcal{U}$, $Z({}^*\mathcal{U}) \cap {}^*\Gamma$ is a boolean combination of F^r-sets in ${}^*\Gamma$. This will be used in what follows.

[9]See Definition 6.9 and Remark 6.10.

Lemma 7.13. *Suppose $B \subset A$ are groupless F-sets in ${}^*\Gamma$. Then there exists a finitely generated $\mathbb{Z}[F]$-submodule $\Gamma' \leq G(\mathcal{U})$, extending Γ, such that every irreducible component of the Zariski closure of $A \setminus B$ is a translate, by an element of ${}^*(\Gamma')$, of a variety defined over $\mathbb{F}_q^{\mathrm{alg}}$.*

Proof. We may assume that the Zariski closure of $A \setminus B$ is irreducible. Indeed, if Z is an irreducible component of $\overline{A \setminus B}$, then $(A \setminus B) \cap Z({}^*\mathcal{U})$ is Zariski-dense in Z, and $(A \setminus B) \cap Z({}^*\mathcal{U}) = (A \setminus B) \cap (Z({}^*\mathcal{U}) \cap {}^*\Gamma)$. As pointed out in the above discussion, $Z({}^*\mathcal{U}) \cap {}^*\Gamma$ is a boolean combination of F^r-sets, for some $r > 0$. Hence $(A \setminus B) \cap Z({}^*\mathcal{U})$ is a finite union of sets of the form $A' \setminus B'$, where A' and B' are groupless F^r-sets in ${}^*\Gamma$, and hence groupless F-sets in ${}^*\Gamma$. Moreover, one of the $A' \setminus B'$ is Zariski-dense in Z. This allows us to make the desired reduction. We may also assume that A and B are cycle-free. Indeed, this is the case if we pass to an extension $\Gamma' \leq G(\mathcal{U})$, and the form of the lemma allows us to do so.

With these reductions in place we show that some translate of $\overline{A \setminus B}$, by an element of ${}^*\Gamma$, is defined over $\mathbb{F}_q^{\mathrm{alg}}$. Fixing an arbitrary multiple of δ_Γ, $\delta > 0$, it suffices to prove this when both A and B are finite unions of translates of sets of the form ${}^*S$ where $S \in \mathrm{Exp}_\Gamma(\delta)$. We proceed by induction on the maximum $(\dim_\delta, \deg_\delta)$ of the exponential F-sets that appear in A. If the maximum $\dim_\delta$ is zero then A is finite and the lemma is trivial.

Let Z be the Zariski closure of $A \setminus B$. Write $A \setminus B$ as a finite union of translates of sets of the form ${}^*(S(\overline{a}_i; \delta)) \setminus B_i$. As Z is irreducible, one of the terms in this union will be Zariski-dense in Z, and hence we may assume that $A = {}^*(S(\overline{a}; \delta))$. Moreover, using Lemma 6.8 and induction, we can assume that the exponential F-sets that appear in B are of $(\dim_\delta, \deg_\delta)$ strictly less than that of $S(\overline{a}; \delta)$.

Now, $F^\delta(A \setminus B) = F^\delta A \setminus F^\delta B = [F^\delta A \setminus (B \cup F^\delta B)] \cup [(B \cap F^\delta A) \setminus F^\delta B]$. Taking Zariski closures, and using the fact that Z is irreducible, we have that $F^\delta Z$ is either the Zariski closure of $(B \cap F^\delta A) \setminus F^\delta B$, or of $F^\delta A \setminus (B \cup F^\delta B)$. In the former case, by induction (and Remarks 6.5 and 6.7), $F^\delta Z$, and hence Z is a translate of a subvariety defined over $\mathbb{F}_q^{\mathrm{alg}}$. In the latter case, we have that $F^\delta Z = \overline{F^\delta A \setminus (B \cup F^\delta B)} \subset \overline{A \setminus B} = Z$, where we are using the fact that $A = {}^*(S(\overline{a}; \delta))$, and hence $F^\delta A \subset A$. It follows that Z is fixed by F^δ, and hence is defined over $\mathbb{F}_q^{\mathrm{alg}}$. □

Proposition 7.14. *Suppose $K \subset \mathcal{U}$ is a finitely generated regular field extension of $\mathbb{F}_q$ and $\Gamma \leq G(K)$ is a finitely generated $\mathbb{Z}[F]$-submodule. Let X be a closed subvariety of G over ${}^*\mathcal{U}$. Then $X({}^*\mathcal{U}) \cap {}^*\Gamma$ is an F-set in ${}^*\Gamma$.*

Proof. By Noetherian induction on X, we may and do assume that X is irreducible, that $X({}^*\mathcal{U}) \cap {}^*\Gamma$ is Zariski-dense in X, and that X has a trivial stabilizer.

We have already pointed out that $X({}^*\mathcal{U}) \cap {}^*\Gamma$ is definable in $({}^*\Gamma, {}^*\mathcal{F})$. We write

$$X({}^*\mathcal{U}) \cap {}^*\Gamma = \bigcup_{i=1}^{\ell} [a_i + {}^*S_i + {}^*H_i \setminus (\bigcup_{j=1}^{m_i} b_{ij} + {}^*T_{ij} + {}^*H_{ij})]$$

for appropriate submodules (the H's) and groupless F-sets (the S's and T's) from Γ, and translating parameters (the a's and b's) from ${}^*\Gamma$. After rewriting the H_i and the H_{ij}'s as a finite union of cosets of $\bigcap\{H_{ij} : [H_i : H_{ij}] < \omega\}$, we can assume that each H_{ij} is either of infinite index in H_i or is equal to H_i. For each $i \leq \ell$, set

- $U_i := a_i + {}^*S_i + {}^*H_i$;

- $V_i := \bigcup\{b_{ij} + {}^*T_{ij} + {}^*H_{ij} : \text{where } H_{ij} = H_i\}$; and,
- $W_i := \bigcup\{b_{i,j} + {}^*T_{ij} + {}^*H_{ij} : \text{where } [H_i : H_{ij}] \text{ is infinite}\}$.

We have $X({}^*\mathcal{U}) \cap {}^*\Gamma = \bigcup_{i=1}^{\ell} U_i \setminus (V_i \cup W_i)$. By transfer from the standard model, Lemma 7.12, and Theorem 7.8, we obtain $X({}^*\mathcal{U}) \cap {}^*\Gamma \supset \bigcup_{i=1}^{\ell}(U_i \setminus V_i)$. Hence, $X({}^*\mathcal{U}) \cap {}^*\Gamma = \bigcup_{i=1}^{\ell}(U_i \setminus V_i)$

As X is irreducible and $X({}^*\mathcal{U}) \cap {}^*\Gamma$ is Zariski-dense in X, $X = \overline{U_i \setminus V_i}$ for some i. Note that H_i stabilises $U_i \setminus V_i$, and hence stabilises X. As X has trivial stabiliser, H_i is trivial. So U_i and V_i are *groupless* F-sets in ${}^*\Gamma$. By Lemma 7.13, for some finitely generated $\mathbb{Z}[F]$-submodule $\Gamma' \leq G(\mathcal{U})$ extending Γ, and some $\gamma \in {}^*(\Gamma')$, $\gamma + X$ is defined over $\mathbb{F}_q^{\mathrm{alg}} \subset \mathcal{U}$. But then $(\gamma + X)({}^*\mathcal{U}) \cap {}^*(\Gamma') = {}^*((\gamma + X)(\mathcal{U}) \cap \Gamma')$, and $(\gamma + X)(\mathcal{U}) \cap \Gamma'$ is an F^r-set for some $r > 0$. Hence $X({}^*\mathcal{U}) \cap {}^*(\Gamma')$ is an F^r-set in ${}^*(\Gamma')$, and so $X({}^*\mathcal{U}) \cap {}^*\Gamma = (X({}^*\mathcal{U}) \cap {}^*(\Gamma')) \cap {}^*\Gamma$ is an F^r-set in ${}^*\Gamma$ (see Remark 6.10). The groupless part of this will be groupless F-sets in ${}^*\Gamma$. Moreover, if $H \leq \Gamma$ is a $\mathbb{Z}[F^r]$-submodule such that ${}^*H$ appears in the expression of $X({}^*\mathcal{U}) \cap {}^*\Gamma$ as an F^r-set, then we can replace ${}^*H$ by ${}^*(H')$ where $H' = \overline{H}(\mathcal{U}) \cap \Gamma$. As $\overline{H}$ is defined over $\mathbb{F}_q$ (using the regularity of K over $\mathbb{F}_q$), H' is a $\mathbb{Z}[F]$-submodule of Γ. Hence, we have expressed $X({}^*\mathcal{U}) \cap {}^*\Gamma$ as an F-set in ${}^*\Gamma$, as desired. □

Corollary 7.15. *Suppose $K \subset \mathcal{U}$ is a finitely generated regular field extension of $\mathbb{F}_q$ and $\Gamma \leq G(K)$ is a finitely generated $\mathbb{Z}[F]$-submodule. Suppose $\{X_b\}_{b \in B}$ is an algebraic family of closed subvarieties of G. There are $A_1, \ldots, A_\ell \in \mathcal{F}(\Gamma)$ such that for any $b \in B$ there exist $I \subset \{1, \ldots, \ell\}$ and points $(\gamma_i)_{i \in I}$ from Γ, such that* $X_b(K) \cap \Gamma = \bigcup_{i \in I} \gamma_i + A_i$.

Proof. If this failed, we could find an elementary extension $({}^*\mathcal{U}, +, \times, {}^*\Gamma, {}^*\mathcal{F})$ of $(\mathcal{U}, +, \times, \Gamma, \mathcal{F})$, and a parameter $b \in B({}^*\mathcal{U})$ for which $X_b({}^*\mathcal{U}) \cap {}^*\Gamma$ is not expressible as an F-set in ${}^*\Gamma$. This contradicts Proposition 7.14. □

Appendix A. $\mathbb{N}$ with successor and congruence predicates.

Proposition A.1. *Let T be given by the following system of axioms in the language $\mathcal{L}_1 = \{0, \sigma\}$.*

(a) $(\forall x, y)\sigma(x) = \sigma(y) \to x = y$
(b) $(\forall x)\sigma(x) \neq 0$
(c$_n$) $(\forall x)\sigma^n(x) \neq x$
(d) $(\forall y)(\exists x)\sigma(x) = y \ \vee \ y = 0$

Then

(1) *T is uncountably categorical.*
(2) $T = \mathrm{Th}(\mathbb{N}, 0, \sigma)$
(3) *T eliminates quantifiers.*
(4) *T is strongly minimal.*
(5) *If $A \subset M \models T$ is a subset of a model of T and $a \in M$, then $a \in \mathrm{acl}(A)$ if and only if $\sigma^n(a) = \sigma^m(b)$ for some $n, m \in \mathbb{N}$ and $b \in A \cup \{0\}$.*
(6) *If $A \subset M \models T$ is a subset of a model of T, then $\mathrm{acl}^{eq}(A) = \mathrm{dcl}^{eq}(A)$.*
(7) *T is trivial.*

(8) *T has definable Skolem functions.*

Proof. First of all, if $(N, 0, \sigma) \models T$ is any model, then for $n < 0$ a negative integer we define $\sigma^n(x) := \begin{cases} y & \text{if } \sigma^{-n}(y) = x \text{ and} \\ 0 & \text{if no such } y \text{ exists.} \end{cases}$

We define an equivalence relation $\sim$ on N by $x \sim y \Leftrightarrow \sigma^n(x) = y \ \vee \ \sigma^n(y) = x$ for some $n \in \mathbb{N}$. In any model of T the class $[0]_\sim$ must be isomorphic to $(\mathbb{N}, 0, \sigma)$ while all other classes are isomorphic to $(\mathbb{Z}, \sigma)$. If M_1 and M_2 are two models of T of the same uncountable cardinality κ, then as each $\sim$-class has size $\aleph_0$, the sets $M_1/\sim$ and $M_2/\sim$ have cardinality κ. Let $\langle a_i : i < \kappa \rangle$ list representatives of the $\sim$-classes of M_1 with $a_0 = 0$ and $\langle b_i : i < \kappa \rangle$ likewise list representatives of the $\sim$ classes in M_2. Then $M_1 = \{\sigma^n(a_0) : n \in \mathbb{N}\} \sqcup \{\sigma^m(a_i) : m \in \mathbb{Z}, i < \kappa\}$ while $M_2 = \{\sigma^n(b_0) : n \in \mathbb{N}\} \sqcup \{\sigma^m(b_i) : m \in \mathbb{Z}, i < \kappa\}$ and the map given by $\sigma^n(a_i) \mapsto \sigma^n(b_i)$ gives an isomorphism. This proves part (1).

For part (2), we note that Axiom scheme (c_n) implies that every model of T is infinite. This together with uncountable categoricity implies that T is complete. As $(\mathbb{N}, 0, \sigma) \models T$, we have $\mathrm{Th}(\mathbb{N}, 0, \sigma) = T$.

For part (3), let $(N, 0, \sigma) \models T$ be a saturated model of T, $A \subset N$ a small subset, and $a, b \in N$ be two elements with the same quantifier-free type over A. We show that they must have the same complete type. As 0 is named already we may without loss of generality assume that $0 \in A$. If for some $n, m \in \mathbb{N}$ and $c \in A$ we have $\sigma^n(a) = \sigma^m(c)$, then $\sigma^n(b) = \sigma^m(c)$ as well. In light of the injectivity of σ, we would have $a = b$. Otherwise, we have that $[a]_\sim \notin \{[c]_\sim : c \in A\}$ (and, of course, $[b]_\sim \notin \{[c]_\sim : c \in A\}$ as well). As in the proof of uncountable categoricity, we see that there is an automorphism of M fixing A and taking a to b. It follows that $\mathrm{tp}(a/A) = \mathrm{tp}(b/A)$.

Part (4) follows from quantifier elimination. Part (5) follows from the fact that $N := \{\sigma^n(0) : n \in \mathbb{N}\} \cup \{\sigma^n(b) : n \in \mathbb{Z}, b \in A \setminus \mathbb{N}\}$ is an elementary submodel of M. This also gives part (6) since $\mathrm{acl}^{eq}(A) \subset N^{eq}$ and visibly $N \subset \mathrm{dcl}(A)$.

For part (7), let $(N, 0, \sigma) \models T$ be a saturated model of T and $a, b, c \in N$. If c is not independendent from $\{a, b\}$, then by strong minimality $c \in \mathrm{acl}(a, b) \setminus \mathrm{acl}(0)$. So by part (5), either $c \in \mathrm{acl}(a)$ (and hence c is not independent from a) or $c \in \mathrm{acl}(b)$ (and hence c is not independent from b). Thus, T is trivial.

For part (8), by quantifier elimination it suffices to show that if x is a singleton variable, y is an r-tuple of variables, and $\phi(x; y)$ a conjunction of atomic and negated atomic formulas, then there is a definable function f taking arguments y such that $T \vdash (\forall y)[\phi(f(y); y) \leftrightarrow (\exists x)\phi(x; y)]$. Write

$$\phi = \bigwedge_{i=1}^{n} \psi_i(x; y) \ \& \ \bigwedge_{j=1}^{m} \neg\vartheta_j(x, y) \ \& \ \rho(y)$$

where each ψ_i and ϑ_j is of the form $\sigma^a(x) = \sigma^b(y_\ell)$ or $\sigma^a(x) = \sigma^b(0)$ and $\rho(y)$ is a conjuntion of formulae of the form $\sigma^a(y_\ell) = \sigma^b(0)$ or $\neg(\sigma^a(y_\ell) = \sigma^b(0))$, for some $a, b \in \mathbb{N}$ and $\ell \leq r$. If $n > 0$, then write ψ_1 as either $\sigma^a(x) = \sigma^b(0)$ or $\sigma^a(x) = \sigma^b(y_\ell)$ for some $a, b \in \mathbb{N}$ and $\ell \leq r$. We define $f(y) := \sigma^{b-a}(0)$ or $\sigma^{b-a}(y_\ell)$ depending on the form of ψ_1. If $n = 0$, then let B be the supremum of the values of a and b for which ϑ_j is of the form $\sigma^a(x) = \sigma^b(0)$ or $\sigma^a(x) = \sigma^b(y_\ell)$ for some $j \leq m$. We define $f(y)$ to $\sigma^{B+1}(y_i)$ for the least i such that $\phi(\sigma^{B+1}(y_i); y)$ holds and to be $\sigma^{B+1}(0)$ if there is no such i. We check that f works. If $n > 0$, $T \vdash \psi_1(x; y) \to x = f(y)$. As

ϕ implies ψ_1, it follows that $T \vdash (\exists x)\phi(x;y) \leftrightarrow \phi(f(y);y)$. Suppose $n = 0$. As T is complete, we need only check that f works in the standard model. Take any $y \in \mathbb{N}^r$ and let z be the maximal element of the set $\{\sigma^{B+1}(0), \sigma^{B+1}(y_1), \ldots, \sigma^{B+1}(y_r)\}$. As $\rho(y)$ does not refer to x, if we assume that $(\exists x)\phi(x,y)$ holds (as we may and do), then $\rho(y)$ holds. Certainly, we have $\neg(\sigma^a(z) = \sigma^b(0))$ and $\neg(\sigma^a(z) = \sigma^b(y_i))$ for all $a, b \leq B$ and $i \leq r$. Thus, $\phi(f(y);y)$ holds. □

Recall that for each $\delta > 0$, $P_\delta(x)$ is the predicate $x \equiv 0 \bmod \delta$.

Proposition A.2. *Let* $0 < \delta \in \mathbb{N}$. *There is a natural, definable, bi-interpretation of the structures* $(\mathbb{N}, 0, \sigma)$ *and* $(\mathbb{N}, 0, \sigma, P_\delta)$. *With respect to these interpretations the* 1*-closed sets correspond to the* δ*-closed sets.*

Proof. By "definable" we just mean that the universe of each structure is interpreted as a definable set in (the home sort of) the other structure – as opposed to being interpreted as a definable set in the imaginary sorts.

For the sake of distinguishing these structures, we write $(\mathbb{N}, 0, S, P_\delta)$ instead of $(\mathbb{N}, 0, \sigma, P_\delta)$. In $(\mathbb{N}, 0, S, P_\delta)$ we interpret $(\mathbb{N}, 0, \sigma)$ as $(P_\delta, S^\delta, 0)$, where the co-ordinate map is the bijection $P_\delta(\mathbb{N}) \to \mathbb{N}$ given by $\delta a \mapsto a$. An equation of the form $x = \sigma^r(y)$ is interpreted as $x = S^{r\delta}(y)$ & $x \equiv 0 \bmod \delta$ & $y \equiv 0 \bmod \delta$, which are δ-equations. It follows that every 1-closed set is interpreted as a δ-closed set.

We now describe how $(\mathbb{N}, 0, S, P_\delta)$ is interpreted in $(\mathbb{N}, 0, \sigma)$. The universe is $\mathbb{N} \times \{0, \sigma(0), \ldots, \sigma^{\delta-1}(0)\}$, where the co-ordinate map is the bijection $\langle a, b\rangle \mapsto a\delta + b$. We take $\langle 0, 0\rangle$ to represent 0 and $\mathbb{N} \times \{0\}$ to represent P_δ. We interpret S on $\mathbb{N} \times \{0, \sigma(0), \ldots, \sigma^{\delta-1}(0)\}$ by

$$S(\langle x, y\rangle) = \begin{cases} \langle x, \sigma(y)\rangle & \text{if } y < \delta - 1 \text{ and} \\ \langle \sigma(x), 0\rangle & \text{if } y = \delta - 1 \end{cases}$$

The δ-equations $x \equiv q \bmod \delta$ (for $q < \delta$) and $x = S^r(y)$ are interpreted by closed relations in $(\mathbb{N}, 0, \sigma)$. In the first case, it is just $\mathbb{N} \times \{q\}$. In the second case, for each $i < \delta$ we write $(i + r) = p_i\delta + s_i$ with $s_i < \delta$. Then $x = S^r(y)$ is interpreted as

$$\{(\langle n_1, m_1\rangle, \langle n_2, m_2\rangle) : \bigvee_{i<\delta} m_2 = i \ \&\ m_1 = s_i \ \&\ n_1 = \sigma^{p_i}(n_2)\}.$$

It follows that every δ-closed set is interpreted in $(\mathbb{N}, 0, \sigma)$ as a 1-closed set.

Finally, one notes that the compositions of these interpretations produce definably isomorphic self-interpretations of $(\mathbb{N}, 0, \sigma)$ and of $(\mathbb{N}, 0, S, P_\delta)$. For example, and this is the less trivial of the two cases, the induced self-interpretation of $(\mathbb{N}, 0, S, P_\delta)$ yields the definable isomorphism $f : \mathbb{N} \longrightarrow \delta\mathbb{N} \times \{0, \delta, 2\delta, \ldots, (\delta - 1)\delta\}$ given by

$$f(n) = (x, y) \iff (x \equiv 0 \bmod \delta) \ \wedge\ \bigvee_{i=0}^{\delta-1} [(y = i\delta) \wedge (S^i x = n)] \tag{1}$$

□

As a consequence of this bi-interpretation, $\mathrm{Th}(\mathbb{N}, 0, \sigma, P_\delta)$ is of finite Morley rank (the universe has rank 1 and degree δ). The following corollary was used in Lemma 6.8.

Corollary A.3. *Fix $\delta > 0$ and $T := \mathrm{Th}(\mathbb{N}, 0, \sigma, P_\delta)$. Suppose $M \models T$, $A \subseteq M$, E is an A-definable equivalence relation on M^n, and $X \subseteq M^n$ is A-definable. There is an A-definable set $Y \subseteq X$ with $Y/E = X/E$ and* $(\mathrm{RM}, \mathrm{dM})(Y) = (\mathrm{RM}, \mathrm{dM})(X/E)$.

Proof. We show that this is true for any theory T satisfying: *T is a totally transcendental theory admitting weak elimination of imaginaries, having definable Skolem functions and for which definable and algebraic closure in T^{eq} agree on real elements.* By Proposition A.1 this is true of $\mathrm{Th}(\mathbb{N}, 0, \sigma)$; via the bi-interpretation of Proposition A.2 it is also true of $\mathrm{Th}(\mathbb{N}, 0, \sigma, P_\delta)$.

We work by induction on $(\mathrm{RM}, \mathrm{dM})(X/E)$. Using $\mathrm{acl}^{eq}(A) = \mathrm{dcl}^{eq}(A)$, we may break X/E into $d := \mathrm{dM}(X/E)$ A-definable sets $W_1, \ldots, W_d$ of Morley rank $\mathrm{RM}(X/E)$ and degree 1. Setting $X_i := \{x \in X : x/E \in W_i\}$, we see that it suffices to consider the case that $d = 1$.

As T admits weak EI, there is an A-definable function $f : X \to M^m/\mathrm{Sym}(m)$ such that $xEy \Leftrightarrow f(x) = f(y)$. Let $\pi : M^m \to M^m/\mathrm{Sym}(m)$ be the quotient map. Let $R \subseteq X \times M^m$ be defined by $(x, y) \in R \Leftrightarrow f(x) = \pi(y)$. By the existence of Skolem functions, there is an A-definable function $g : M^m \to M^n$ such that for any $y \in M^m$ if $M \models (\exists z)R(z, y)$, then $M \models R(g(y), y)$.

Let $Z := g(\pi^{-1}(f(X))$. Note that $Z/E = X/E$. Let $U \subseteq Z$ be an A-definable subset of Z with $\mathrm{RM}(Z) = \mathrm{RM}(U)$ and $\mathrm{dM}(U) = 1$. As f is finite-to-one when restricted to Z, we have that $\mathrm{RM}(Z) = \mathrm{RM}(Z/E)$ and $\mathrm{RM}(U) = \mathrm{RM}(U/E)$. Thus, $\mathrm{RM}(X/E \setminus U/E) < \mathrm{RM}(X/E)$. By induction, there is some A-definable subset $V \subseteq f^{-1}(X/E \setminus U/E)$ with $V/E = (X/E \setminus U/E)$ and $\mathrm{RM}(V) = \mathrm{RM}(X/E \setminus U/E)$. Set $Y := U \cup V$. □

Definition A.4. Fix $\delta > 0$. Let $X \subset \mathbb{N}^n$ be an $\mathcal{L}_\delta$-definable set, $\alpha \in \mathbb{N}^n$ an n-tuple of natural numbers less than δ. By the *α-residue class of X* we mean the $\mathcal{L}_\delta$-definable set $X_\alpha := \{x \in X : \bigwedge_{i=1}^n x_i \equiv \alpha_i \mod \delta\}$.

Note that we can write X as a finite disjoint union of its α-residue classes, as α ranges over all n-tuples of natural numbers less than δ.

Lemma A.5. *Let f denote the definable isomorphism between $(\mathbb{N}, 0, \sigma, P_\delta)$ and the self-interpretation induced by Proposition A.2. Suppose X is an $\mathcal{L}_\delta$-definable set. If $f(X)$ is δ-closed then X is δ-closed.*

Proof. Taking finite unions we may assume that $X \subset \mathbb{N}^n$ is of a fixed residue class. That is, $X = X_\alpha$ for some $\alpha = (\alpha_1, \ldots, \alpha_n)$ with each $\alpha_i < \delta$. Using equation (1), we see that $f(X) = (-\alpha + X) \times \{\delta\alpha\}$. Hence, if $f(X)$ is δ-closed, then so is X. □

If $V \subset \mathbb{N}^n$ is a δ-variety then V can written as a finite disjoint union of its residue classes, V_α for $\alpha \in {}^n\delta$, each of which is again a δ-variety. Moreover, the interpretation of each V_α in $(\mathbb{N}, 0, \sigma)$ is a 1-variety (this can be seen by inspecting the interpretation given in Proposition A.2). Note that the interpretation of an arbitrary δ-variety is not always a 1-variety.

Proposition A.6. *Fix $\delta > 0$. Let $X \subset \mathbb{N}^{n+m}$ be any $\mathcal{L}_\delta$-definable set. There is a finite union of δ-varieties $V \subset \mathbb{N}^{n+m}$ such that for any $b \in \mathbb{N}^m$ with $X_b \neq \varnothing$, one has $X_b \subset V_b$ and* $(\mathrm{RM}, \mathrm{dM})(V_b) = (\mathrm{RM}, \mathrm{dM})(X_b)$.

Proof. By Proposition A.1 $\mathrm{Th}(\mathbb{N}, 0, \sigma)$ admits quantifier elimination. From the bi-interpretation of Proposition A.2, this is also true of $\mathrm{Th}(\mathbb{N}, 0, \sigma, P_\delta)$. We write

$X = \bigcup_{i=1}^{\ell}(D_i \setminus \bigcup_{j=1}^{k_i} C_{ij})$ where each D_i and C_{ij} is a δ-variety and $C_{ij} \subsetneq D_i$. It suffices to consider the case when $\ell = 1$, and we assume $X = D \setminus (\bigcup_{j=1}^{k} C_j)$.

Let $\Sigma := \{\alpha^1, \ldots, \alpha^\ell\} \subset \mathbb{N}^{n+m}$ be the set of all distinct tuples of numbers strictly less than δ. We can write $X = \bigsqcup_{i=1}^{\ell}[D_{\alpha^i} \setminus \bigcup_{j=1}^{k}(C_j)_{\alpha^i}]$. Taking finite unions, we may assume that for some $\alpha \in \Sigma$, $D = D_\alpha$ and each $C_j = (C_j)_\alpha$. That is, D and the C_j's are of a *fixed residue class*.

If $b \in \mathbb{N}^m$ with $X_b \neq \varnothing$, then D_b is again a δ-variety and each $(C_j)_b \subsetneq D_b$ is a proper δ-subvariety. Moreover, D_b and the $(C_j)_b$'s are still of a fixed residue class. Hence their interpretations in $(\mathbb{N}, 0, \sigma)$ are varieties. Using part (5) of Proposition A.1 it is not hard to see that in $(\mathbb{N}, 0, \sigma)$ every proper subvariety of a variety has strictly smaller Morley rank. It follows that for each j, $\mathrm{RM}(C_j)_b < \mathrm{RM}\, D_b$. Hence, $(\mathrm{RM}, \mathrm{dM})(D_b) = (\mathrm{RM}, \mathrm{dM})(X_b)$, and we can take $V = D$. □

References

[1] D. Abramovich and J.F. Voloch. Toward a proof of the Mordell-Lang conjecture in characteristic p. *International Mathematics Research Notices*, (5):103–115, 1992.

[2] E. Hrushovski. The Mordell-Lang conjecture for function fields. *Journal of the American Mathematical Society*, 9(3):667–690, 1996.

[3] S. Lang. *Abelian varieties.* Number 7 in Interscience tracts in pure and applied mathematics. Interscience Publishers, New York, 1959.

[4] S. Lang. *Fundamentals of diophantine geometry.* Springer Verlag, New York, 1983.

[5] R. Moosa and T. Scanlon. The Mordell-Lang conjecture in positive characteristic revisited. Preprint, 2003.

[6] A. Pillay. The model-theoretic content of Lang's conjecture. In E. Bouscaren, editor, *Model theory and algebraic geometry*, volume 1696 of *Lecture Notes in Math.*, pages 101–106. Springer Verlag, Berlin, 1998.

[7] B. Poizat. Paires de structures stables. *Journal of Symbolic Logic*, 48(2):239–249, 1983.

[8] P. Samuel. Compléments à un article de Hans Grauert sur la conjecture de Mordell. *Inst. Hautes Études Sci. Publ. Math.*, (29):55–62, 1966.

[9] T. Scanlon. The absolute Mordell-Lang conjecture in positive characteristic. E-print available at `http://math.berkeley.edu/~scanlon/papers/MLf7a.pdf`, 1998.

[10] T. Scanlon. Uniformity in the Mordell-Lang conjecture. E-print available at `http://arxiv.org/pdf/math.LO/0105238`, 2001.

Massachusetts Institute of Technology, Department of Mathematics, 77 Mass. Ave., Cambridge, MA 02139-4307, USA

E-mail address: `moosa@math.mit.edu`

University of California, Berkeley, Department of Mathematics, Evans Hall, Berkeley, California 94720-3840, USA

E-mail address: `scanlon@math.berkeley.edu`