Pseudofinite groups with NIP theory and definability in finite simple groups

Dugald Macpherson[*], School of Mathematics, University of Leeds, Leeds LS2 9JT, England
h.d.macpherson@leeds.ac.uk

Katrin Tent[†], Mathematisches Institut, Universität Münster, Einsteinstrasse 62, 48149 Münster, Germany
tent@math.uni-muenster.de

July 27, 2011

Abstract: We show that any pseudofinite group with NIP theory and with a finite upper bound on the length of chains of centralisers is soluble-by-finite. In particular, any NIP rosy pseudofinite group is soluble-by-finite. This generalises, and shortens the proof of, an earlier result for stable pseudofinite groups. An example is given of an NIP pseudofinite group which is not soluble-by-finite. However, if $\mathcal{C}$ is a class of finite groups such that all infinite ultraproducts of members of $\mathcal{C}$ have NIP theory, then there is a bound on the index of the soluble radical of any member of $\mathcal{C}$. We also survey some ways in which model theory gives information on families of finite simple groups, particularly concerning products of images of word maps.

1 Introduction

We consider in this paper groups G which are *pseudofinite*, that is, infinite groups which satisfy every first order sentence (in the language L_g of groups) which holds in all finite groups. Equivalently, G is elementarily equivalent to an infinite ultraproduct of finite groups. Or equivalently again, G is an infinite group with the *finite model property*: every sentence in the theory of the group has a finite model. We consider the structure of G, under the assumption that the first order theory $\mathrm{Th}(G)$ of G satisfies various generalisations of model theoretic stability.

It was shown in [21] that any stable pseudofinite group G has a definable soluble normal subgroup of finite index. This is not surprising; for by a clas-

[*]Research partially supported by EPSRC grant EP/H00677X/1

[†]Research partially supported by SFB 878

sification due to Wilson [32] (with a slight strengthening due to Ryten – see [9, Proposition 2.14]) – any infinite pseudofinite *simple* group is a group of Lie type over a pseudofinite field, and in particular interprets a pseudofinite field [27, 5.2.4, 5.3.3, 5.4.3], and so has unstable theory by Duret [5]. However, an intricate argument with centralisers was needed in [21] to bound the derived length of soluble normal subgroups.

One generalisation of stability is the notion of *simple* theory. Pseudofinite fields (and certain difference fields, that is, fields equipped with a specified automorphism) are simple, in fact supersimple of finite rank, and it follows from Wilson's classification that every simple pseudofinite group is interpretable in such a structure. Hence, every simple pseudofinite group has supersimple finite rank theory; this follows from the results of Hrushovski [12] and is made explicit in [9] (note that measurable structures are supersimple of finite rank – see e.g. [8, Corollary 3.7]). A satisfactory structure theory for pseudofinite groups with supersimple finite rank theory – under an additional assumption that $\exists^\infty$ is definable in $T^{\rm eq}$ – was initiated in [9]. The class of supersimple finite rank structures is sufficiently rich to include a lot of pseudofinite group theory, as indicated by, for example, [19, 4.11, 4.12]. Possible applications of the model theory of supersimple theories to finite simple groups are discussed in the final section of the present paper.

Another generalisation of stability of considerable current interest is that of *NIP*, or *dependent* theory. A formula $\phi(\bar{x}, \bar{y})$ has the *independence property* with respect to T if there is $M \models T$ and a set $\{\bar{a}_i : i \in \omega\} \subset M^{l(\bar{x})}$ such that for all $S \subseteq \omega$ there is $\bar{b}_S \in M^{l(\bar{y})}$ such that for all $i \in \omega$, $M \models \phi(\bar{a}_i, \bar{b}_S)$ if and only if $i \in S$. A theory T is *NIP* if no formula has the independence property with respect to T. Any simple or NIP theory is stable, and any theory which is *both* simple and NIP is stable. For groups, by the Baldwin-Saxl Theorem (see [2], or [6, Fact 0.17]) the NIP condition implies a useful chain condition: if G is an NIP group, then for every formula $\phi(x, \bar{y})$ there is a natural number n_ϕ such that every *finite* intersection of ϕ-definable groups is an intersection of n_ϕ ϕ-definable groups. By Wilson's theorem, there is no simple pseudofinite group with NIP theory, and we expected this, together with the above chain condition, to yield virtual solubility for pseudofinite groups with NIP theory. However, this is false, and in Section 3 below we give a construction of a pseudofinite group G with NIP theory which is not soluble-by-finite.

Our main theorem is the following. We say that a group G has the *centraliser chain condition* if there is a natural number $n = n(G)$ such that there do not exist subsets $F_1, \ldots, F_{n+1} \subset G$ with

$$C_G(F_1) < \ldots < C_G(F_{n+1}).$$

Theorem 1.1 *Let G be a pseudofinite group with NIP theory, and suppose that G satisfies the centraliser chain condition. Then G has a soluble definable normal subgroup of finite index.*

We obtain some information about finite groups just under an NIP assumption. Let us say that the class $\mathcal{C}$ of finite structures is an *NIP class* if every infinite ultraproduct of members of $\mathcal{C}$ has NIP theory. As a step in the proof of Theorem 1.1 we obtain the following result. Here, and throughout the paper, if G is a finite group we denote by $R(G)$ its *soluble radical*, that is, the unique largest soluble normal subgroup of G.

Proposition 1.2 *Let $\mathcal{C}$ be an NIP class of finite groups. Then there is $d = d(\mathcal{C}) \in \mathbb{N}$ such that $|G : R(G)| \leq d$ for every $G \in \mathcal{C}$.*

The notion of *rosy* theory is a common generalisation of the notions of *o-minimal* theory and *simple* (and hence also of *stable*) theory. The concept was introduced by Onshuus in [22] and developed in Adler [1]. We omit the definition of rosiness, but note that by [6, Definition 0.3], a theory T is rosy if there is an independence relation $\downfree$ on real *and imaginary* tuples which satisfies the following natural conditions :

(i) $\downfree$ is automorphism invariant.

(ii) If $c \in \mathrm{acl}(aB) \setminus \mathrm{acl}(B)$, then $a \not\downfree_B c$.

(iii) If $a \downfree_B C$ and $B \cup C \subseteq D$, then there is $a' \in \mathrm{tp}(a/BC)$ with $a' \not\downfree_B D$.

(iv) There is λ such that for any a, if $(B_i)_{i<\alpha}$ are sets with $B_i \subset B_j$ whenever $i < j$ and $a \not\downfree_{B_i} B_j$ for $i < j < \alpha$, then $\alpha < \lambda$.

(v) If $B \subseteq C \subseteq D$, then $a \downfree_B D$ if and only if $A \downfree_B C$ and $a \downfree_C D$.

(vi) $C \downfree_A B$ if and only if $c \downfree_A B$ for any finite $c \subseteq C$.

(vii) $a \downfree_C b$ if and only if $b \downfree_C a$.

A structure with an infinite descending chain of uniformly definable equivalence relations can never be rosy – see e.g. the proof of Proposition 1.3 in [6]. In particular, a field with a non-trivial definable valuation can never be rosy, and more generally a group with an infinite strictly descending chain of uniformly definable subgroups cannot be rosy. In combination with the consequence mentioned above of the Baldwin-Saxl Theorem this yields the following, for groups.

Proposition 1.3 *[6, Corollary 1.8] Any group definable in an NIP rosy theory has the centraliser chain condition.*

By Theorem 1.1, this yields immediately the following.

Corollary 1.4 *Let G be a pseudofinite group with NIP rosy theory. Then G has a soluble definable normal subgroup of finite index.*

We should not expect here to replace 'soluble' 'by 'nilpotent', since examples (involving Chapuis, Simonetta, Khelif, and Zilber) are mentioned at the end of [21] of stable pseudofinite groups which are not nilpotent-by-finite.

Theorem 1.1 is proved in Section 2. In addition to Proposition 1.3, and the classification of simple pseudofinite groups, we use the following two results.

Theorem 1.5 *[33, Wilson] There is a formula $\psi(x)$ such that for every finite groups G, we have $R(G) = \{x \in G : G \models \psi(x)\}$.*

Theorem 1.6 *[13, Khukhro] There is a function $f : \mathbb{N} \to \mathbb{N}$, such that for any $d \in \mathbb{N}$, if G is a finite soluble group with no strictly descending chain of centralisers of length $d+1$, then G has derived length at most $f(d)$.*

The final section of the paper is a discussion of some possible applications of model theory to structural questions on families of finite simple groups of fixed Lie rank. There are three main sources of applications: a generalisation of the Zilber Indecomposability Theorem for groups in supersimple theories; some still-unpublished work of Ryten showing that any family of finite simple groups is an 'asymptotic class', so that cardinalities of definable sets satisfy Lang-Weil-like uniformities; and results on generic types of groups in supersimple theories. No new results here are given, but the methods give, for example, a alternative approach to some recent results on word maps. For the Suzuki and Ree groups there is heavy dependence on a major result of Hrushovski [12].

Acknowledgement. We thank Sasha Borovik for drawing our attention to Theorem 1.6.

2 Proof of Theorem 1.1.

Proof of Proposition 1.2. Let $\mathcal{C} = \{G_i : i \in \mathbb{N}\}$ be a class of finite groups such that every non-principal ultraproduct of members of $\mathcal{C}$ has NIP theory. By Theorem 1.5, with $\psi(x)$ the formula given in that theorem, for each $i \in \omega$ we have $R(G_i) = \{x \in G_i : G_i \models \psi(x)\}$. By Łos's Theorem, ψ defines a normal subgroup, denoted $\psi(G)$, of any ultrapower G of members of $\mathcal{C}$.

Write $\bar{G}_i := G_i/R(G_i)$, and let $S_i := \mathrm{Soc}(\bar{G}_i)$, the direct product of the minimal normal subgroups of $\bar{G}_i$. By the maximality of $R(G_i)$, each minimal normal subgroup of $\bar{G}_i$ is non-abelian.

Claim 1. There is $t \in \mathbb{N}$ such that each $\bar{G}_i$ has at most t distinct minimal normal subgroups.

Proof of Claim. Suppose that the claim is false. Then for each $n \in \mathbb{N}$ there is $i_n \in \mathbb{N}$ such that $\bar{G}_{i_n}$ has distinct minimal normal subgroups $T_{i_n,1}, \ldots, T_{i_n,n}$ (and possibly others). For each such n and $j \in \{1, \ldots, n\}$, let $x_{n,j}, y_{n,j}$ be non-commuting elements of $T_{i_n,j}$. For such n and for any $w \subset \{1, \ldots, n\}$ let $z_{n,w}$ be the product of the elements $\{x_{n,j} : j \in w\}$ (the order of the product does not matter, as the $x_{n,j}$ lie in distinct minimal normal subgroups, so commute). Now $y_{n,j}z_{n,w} \neq z_{n,w}y_{n,j}$ (in $\bar{G}_{i_n}$) if and only if $j \in w$. It follows by Łos's Theorem that a non-principal ultrafilter can be chosen on $\mathbb{N}$ so that the formula $\chi(y, z)$ of form $yz \neq zy$ witnesses that $\Pi_i \bar{G}_i/\mathcal{U}$ has the independence property. Thus, as $\bar{G}_i$ is uniformly interpretable in G_i, the infinite group $\Pi_{i \in \mathbb{N}} G_i/\mathcal{U}$ does not have NIP theory, a contradiction.

By Claim 1, after partitioning $\mathbb{N}$ into finitely many sets if necessary, we may suppose that for each i, S_i is a direct product of exactly t distinct minimal normal subgroups of $\bar{G}_i$, namely $T_{i,1}, \ldots, T_{i,t}$. Each T_i is characteristically simple, so being non-abelian is a direct product of isomorphic non-abelian simple groups. Arguing as in the proof of Claim 1, we may suppose that for some $r \in \mathbb{N}$, each $T_{i,j}$ is a direct product of at most r non-abelian simple groups. Thus, we may reduce to the case when each S_i is a direct product of exactly c minimal normal subgroups of S_i, namely $S_i = R_{i,1} \times \ldots \times R_{i,c}$, where each $R_{i,c}$ is non-abelian simple.

Claim 2. There is $e \in \mathbb{N}$ such that any non-abelian simple subgroup of $\bar{G}_i$ has Lie rank at most e (where we define the Lie rank of the alternating group Alt_n to be n, and that of the sporadic simple groups to be 1).

Proof of Claim. We argue as in the proof of Claim 1. It suffices to note that for any n, a sufficiently large alternating group contains a direct product of n copies of Alt_4. Likewise, non-abelian classical simple groups of large rank contain many commuting copies of $\mathrm{PSL}_2(q)$.

Claim 3. Let $\mathcal{F}$ be a family of finite simple groups of fixed Lie rank e. Then there is $d = d(e) \in \mathbb{N}$ such that if $K \in \mathcal{F}$ and $g, h \in K \setminus \{1\}$ then g is a product of at most d copies of h and h^{-1}.

Proof of Claim. This is well-known. It follows for example from the theorem in [25] that any non-principal ultraproduct of members of $\mathcal{F}$ is a group of the same Lie type over a pseudofinite field, and so is simple.

By Claims 2 and 3 we obtain the following: there is $b \in \mathbb{N}$ such that for each i, c here is $x_{i,c} \in R_{i,c}$ such that each element of $R_{i,c}$ is a product of at most b $R_{i,c}$-conjugates of $x_{i,c}$ and $x_{i,c}^{-1}$. As $\bar{G}_i$ normalises each $T_{i,j}$, and each $T_{i,j}$ is a product of boundedly many groups of form $R_{i,c}$, it follows easily that the $T_{i,j}$ are uniformly definable in the $\bar{G}_i$. Hence also the $R_{i,j}$ are uniformly definable in $\bar{G}_i$.

To complete the proof of the proposition, it suffices to show that there is $e \in \mathbb{N}$ such that $|S_i| \leq e$ for all i. For suppose this holds. Then $C_i := C_{\bar{G}_i}(S_i) = 1$, since otherwise, as S_i is centreless, the socle of C_i would be a product of minimal normal subgroups of $\bar{G}_i$ not contained in S_i, which is impossible. Thus, $\bar{G}_i$ embeds in $\mathrm{Aut}(S_i)$, so has order at most $e!$.

So suppose for a contradiction that there is no finite upper bound on $|S_i|$. Then by the classification of finite simple groups, there is some Lie type Chev (possibly twisted, but with the Lie rank fixed) such that the $R_{i,j}$ include arbitrarily large finite simple groups of type Chev. Relabelling if necessary, we may suppose there is a subsequence $(n_i : i \in \mathbb{N})$ of $\mathbb{N}$ such that each finite simple group $R_{n_i,1}$ has Lie type Chev, and $|R_{n_i,1}| \to \infty$ as $i \to \infty$. We may suppose that $R_{n_i,1}$ is defined in $\bar{G}_{n_i}$ by the formula $\phi(x, \bar{a}_i)$.

Let $\mathcal{U}$ be a non-principal ultrafilter on $\mathbb{N}$ containing $N = \{n_i : i \in \mathbb{N}\}$, and hence all cofinite subsets of N. Put $G = \Pi_{i\in\mathbb{N}} G_i/\mathcal{U}$, and $\bar{G} := G/H$, where H is the normal subgroup of G defined by ψ. Then there is $\bar{a} \in \bar{G}$ such that

$\phi(x, \bar{a})$ defines an infinite ultrapower of groups of type Chev, and hence, by [25], a group of Lie type Chev over a pseudofinite field. Such a subgroup has the independence property, by the results of Ryten and Duret mentioned above. It follows that $\bar{G}$, and hence G, does not have NIP theory, a contradiction. $\square$

The following lemma is standard.

Lemma 2.1 *Let L be a countable language and M be a pseudofinite L-structure. Then there is an infinite class $\mathcal{C}$ of finite structures such that every infinite ultrapower of members of $\mathcal{C}$ is elementarily equivalent to M.*

Proof. We may suppose that $M = \Pi_{n\in\mathbb{N}} M_i/\mathcal{U}$ where the M_i are finite with $|M_i| \to \infty$ as $i \to \infty$. Let $\{\sigma_i : i \in \mathbb{N}\}$ list $\mathrm{Th}(M)$. Iteratively, we find a sequence $U_0 \supset U_1 \supset \ldots$ of members of $\mathcal{U}$ such that for each $i \in \mathbb{N}$, U_i contains the i smallest elements $n_{i1} < \ldots < n_{ii}$ of U_{i-1}, and such that for all $i \in \mathbb{N}$ and $j \in U_i$ with $j > n_{ii}$, $M_j \models \sigma_i$. Put $U := \bigcap_{i\in\mathbb{N}} U_i$. Then U is infinite, and by Łos's Theorem, $\mathcal{C} := \{M_i : i \in U\}$ satisfies the lemma. $\square$

Proof of Theorem 1.1. Let G be a pseudofinite group with NIP theory, such that every chain of centralisers has length at most e. Observe that there is a sentence τ_e in the language L_g of groups such that for every group H, $H \models \tau_e$ if and only if every chain of centralisers in H has length at most e. By Lemma 2.1 there is a set $\mathcal{C} := \{G_i : i \in \mathbb{N}\}$ and an ultrafilter $\mathcal{U}$ on $\mathbb{N}$ such that (after replacing G by an elementarily equivalent group if necessary) $G = \Pi_{i\in\mathbb{N}} G_i/\mathcal{U}$, and every infinite ultraproduct of members of $\mathcal{C}$ is elementarily equivalent to G. It follows that $\mathcal{C}$ is an NIP class of finite groups, so by Proposition 1.2 there is $d \in \mathbb{N}$ such that $|G_i : R(G_i)| \leq d$ for all $i \in \mathbb{N}$. Also $M_i \models \tau_e$ for cofinitely many $i \in \mathbb{N}$. Hence, by Theorem 1.6, $R(G_i)$ has derived length at most $f(e)$ for cofinitely many $i \in \mathbb{N}$. The property that the derived length is at most $f(e)$ is first order expressible by a sentence asserting that a certain word vanishes on a group. Thus, by Łos's Theorem, the normal subgroup $R(G) := \{x \in G : G \models \psi(x)\}$ is soluble of derived length at most $f(e)$, and index at most d in G. $\square$

3 A pseudofinite NIP group which is not soluble-by-finite

We here prove the following theorem.

Theorem 3.1 *There is a pseudofinite group G with NIP theory which is not soluble-by-finite.*

Proof. Fix a prime p. It is well-known that the valued field $\mathbb{Q}_p$, and hence its valuation ring $\mathbb{Z}_p$, has NIP theory. Hence, the group $H := \mathrm{SL}_2(\mathbb{Z}_p)$, which is interpretable in $\mathbb{Z}_p$, also has NIP theory. Let $\mathcal{M} := p\mathbb{Z}_p$, the maximal ideal of $\mathbb{Z}_p$. For each $k > 0$ let H_k be the congruence subgroup of H consisting of matrices $\begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix}$ which lie in H and satisfy $a, b, c, d \in p^k\mathcal{M}$. Then H_k is normal in H, and the quotient $\bar{H}_k := H/H_k$ is finite.

Let $\mathcal{U}$ be a non-principal ultrafilter on ω, and let G be the ultraproduct $\Pi\bar{H}_k/\mathcal{U}$. Then G is a pseudofinite group, and is NIP by the following lemma, since the groups $\bar{H}_k$ are uniformly interpretable in an NIP theory.

If M is a structure and $\phi(x_1, \ldots, x_m, y_1, \ldots, y_n)$ is a formula which does not have the independence property in M, then there is a greatest natural number d such that there are distinct $\bar{a}_1, \ldots, \bar{a}_d \in M$ such that for each $S \subseteq \{1, \ldots d\}$ there is $\bar{b}_S \in M^n$ with, for all $i \in \{1, \ldots, d\}$, $M \models \phi(\bar{a}_i, \bar{b}_S) \Leftrightarrow i \in S$. Such d is called the *Vapnik-Chervonenkis dimension*, or *VC-dimension*, of the family of definable sets in the $\bar{x}$-variables determined by ϕ (or just of the formula ϕ).

Lemma 3.2 *Let L, L' be first order languages, and let M be an L-structure with NIP theory. Suppose that $\{M_i : i \in I\}$ is a set of L'-structures which is uniformly interpretable in M (with I an interpretable set of M). Let J be an infinite subset of I and $\mathcal{V}$ a non-principal ultrafilter on J. Then the ultraproduct $N = \Pi_{j\in J} M_j/\mathcal{V}$ has NIP theory.*

Proof of Lemma 3.2. It suffices to observe that the VC-dimension of any L'-formula $\phi(\bar{x}, \bar{y})$ is uniformly bounded across the class of structures M_i. We leave the details as an exercise. □

Note that if a group is soluble-by-finite, then so are all its subgroups and quotients. Therefore, in order to show that G is not soluble-by-finite, we first prove the following claim.

Claim 1. The group G has a normal subgroup N such that $G/N \cong \mathrm{SL}_2(\mathbb{Z}_p)$.

Proof of Claim. We view the groups $\bar{H}_k$ and G as structures in the language $L^+ := L_g \cup \{P_i : i < \omega\}$ where the P_i are unary predicates. In $\bar{H}_k$, P_i is interpreted by H_i/H_k for $i \leq k$ and by $1 = H_k/H_k$ for $i > k$. Thus, the P_i are interpreted by a descending chain of normal subgroups of $\bar{H}_k$. The group G has by Łos's Theorem a corresponding strictly descending chain $P_0^G > P_1^G > \ldots$ consisting of normal subgroups of G. Put $N := \bigcap_{i\in\omega} P_i^G$. Compactness together with ω-saturation of G (viewed as an L^+-structure) yields that $G/N \cong \mathrm{SL}_2(\mathbb{Z}_p)$.

To complete the proof of Theorem 3.1 we now note:

Claim 2. The group $\mathrm{SL}_2(\mathbb{Z}_p)$ is not soluble-by-finite.

Proof of Claim. This must be well-known: if it were soluble-by-finite, then so would be $\mathrm{SL}_2(\mathbb{Z}) < \mathrm{SL}_2(\mathbb{Z}_p)$ and its quotient $\mathrm{PSL}_2(\mathbb{Z})$, which is a free product of a cyclic group of order two and a cyclic group of order three, and clearly not soluble-by-finite (see [26], Section 6.2). □

Remark 3.3 Let G be a pseudofinite NIP group which is not soluble-by-finite. By Lemma 2.1 $G \cong H$ for some ultraproduct $H = \Pi_{i\in\mathbb{N}} H_i/\mathcal{U}$, such that every infinite ultraproduct of the H_i is elementarily equivalent to G.

The formula $\psi(x)$ defines a non-soluble normal subgroup $\psi(H)$ of finite index in H. By the methods of Section 2, it can be shown that $\psi(H)$ has subgroups $N_1 < N_2$ which are normal in H, such that $\psi(H)/N_2$ is pro-soluble (an inverse limit of soluble groups) but not soluble, and N_1 is the union of a chain of soluble groups but is not soluble. We have not investigated the possible structure of N_2/N_1. In fact, these conclusions can be shown to hold for *any* infinite NIP group which is a non-principal ultraproduct of distinct finite groups and is not soluble-by-finite.

4 Model theory of finite simple groups

In this section we make some remarks about possible applications of model theory to finite group theory, via pseudofinite groups. As mentioned in the introduction, one generalisation of the notion of *stable* first order theory is that of *simple theory.* This notion was introduced by Shelah in [30] and developed in the 1990s in [14] and [15] and further in other papers. Many ideas first appeared in [4] and in early versions of [11]. A convenient source, mainly used below, is [31]. Simplicity theory is a context for an abstract theory of independence, given by 'non-forking', which is less powerful than the corresponding independence theory in stability theory, but stronger than that in rosy theories. In stable theories, over a suitable base, the first order type of tuples $\bar{a}$ and $\bar{b}$, combined with the knowledge that they are independent, determines the type of $\bar{a}\bar{b}$, but this is false in general in simple theories.

We emphasise the distinction between the group-theoretic notion of *simple group* and the model-theoretic notion of *group definable in a simple theory.* We also stress that our methods below only seem to have applications for families of finite simple groups *of fixed Lie rank.*

Among the simple theories are the *supersimple ones*, for which there are global model-theoretic notions of *rank* or *dimension* for definable sets. We shall only deal with supersimple finite rank theories, in which all the main notions of model-theoretic rank coincide on any definable set (though not on types). Below, we shall work with SU-rank. The SU-rank on types is an ordinal-valued rank defined by transfinite induction: for any type p over A, $\mathrm{SU}(p) \geq \alpha + 1$ if there is $B \supset A$ such that p has a forking extension q over B with $\mathrm{SU}(q) \geq \alpha$, and for limit ordinals δ, $\mathrm{SU}(p) \geq \delta$ if $\mathrm{SU}(p) \geq \beta$ for all ordinals $\beta < \delta$. If X is a set defined by a formula $\phi(x, \bar{a})$ with $\bar{a}$ from A, then $\mathrm{SU}(X)$ is the supremum (which will be the maximum in the finite rank theories considered here) of the $\mathrm{SU}(p)$ for types p over A containing the formula $\phi(x, \bar{a})$.

It can be shown that any family of finite simple groups of fixed Lie rank is uniformly interpretable in a family of finite fields, or (in the case of Suzuki and Ree groups) in a family of finite *difference fields*, that is, fields equipped with an automorphism. In fact, by [27, Ch. 5], if parameters are allowed then the groups are uniformly bi-interpretable in the (difference) fields. Thus, the groups $\mathrm{PSL}_2(q)$ are uniformly parameter bi-interpretable in the fields $\mathbb{F}_q$, the

Ree and Suzuki groups ${}^2F_4(2^{2k+1})$ and ${}^2B_2(2^{2k+1})$ are uniformly parameter bi-interpretable with the difference fields $(F_{2^{2k+1}}, x \mapsto x^{2^k})$, and the Ree groups ${}^2G_2(3^{2k+1})$ are uniformly parameter bi-interpretable with the difference fields $(\mathbb{F}_{3^{2k+1}}, x \mapsto x^{3^k})$. Now infinite ultraproducts of finite fields have supersimple SU-rank 1 theory – that is, the set defined by the formula $x = x$ has SU-rank 1 – by for example [3]. The ultraproducts of the corresponding difference fields also have supersimple SU-rank one theory, by the results of Hrushovski [12] and of Ryten (see e.g. [27, Theorem 3.5.8]). For the difference fields this rests on deep work from the 1990s in [12], and Hrushovski was clearly aware then of the supersimplicity of pseudofinite simple groups, and applications similar to some of those below.

We mention three possible lines of application to finite simple groups.

1. *Zilber Indecomposability.* The Irreducibility Theorem for linear algebraic groups was reworked by Zilber for groups of finite Morley rank. Other model-theoretic versions have appeared, but for us the following result of Wagner is convenient. See [31, 4.5.6], or, for the guise below, [10, Remark 2.5].

Theorem 4.1 (Indecomposability Theorem) *Let G be a group interpretable in a supersimple finite* SU*-rank theory, and let $\{X_i : i \in I\}$ be a collection of definable subsets of G. Then there exists a definable subgroup H of G such that:*

(i) $H \leq \langle X_i : i \in I \rangle$, and there are $n \in \mathbb{N}$, $\epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}$, and $i_1, \ldots, i_n \in I$, such that $H \leq X_{i_1}^{\epsilon_1} \ldots X_{i_n}^{\epsilon_n}$.

(ii) X_i/H is finite for each $i \in I$.

If the collection of X_i is setwise invariant under some group Σ of definable automorphisms of G, then H may be chosen to be Σ-invariant.

This has the following almost immediate application to finite simple groups. The result below can also be deduced from [20, Theorem 1], in combination with Theorem 4.4 below.

Theorem 4.2 *Let $\mathcal{C} = \{G_i : i \in \mathbb{N}\}$ be a family of finite simple groups of fixed Lie type τ, and let $\phi(x, y_1, \ldots, y_m)$ be a formula in the language of groups. Then there is a positive integer $d = d(\phi, \tau)$ with the following property: if $\bar{a}_i \in G_i^m$ for each $i \in \mathbb{N}$, and $X_i := \phi(G_i, \bar{a}_i)$ with $|X_i| > 1$ and $|X_i| \to \infty$ as $i \to \infty$, then each G_i is a product of at most d conjugates of the set $X_i \cup X_i^{-1}$.*

Proof. Suppose that this is false. Then there is a decreasing sequence of infinite subsets $(I_j : j \in \mathbb{N})$ of $\mathbb{N}$ with infinite intersection I such that for any $d \in \mathbb{N}$, and for all but finitely many $j \in I_d$, G_j is not a product of at most d conjugates of $X_j \cup X_j^{-1}$. Choose a non-principal ultrafilter $\mathcal{U}$ on $\mathbb{N}$ which contains the set I. Let $G := \Pi_{j\in\mathbb{N}} G_i/\mathcal{U}$ and $X := \Pi_{j\in\mathbb{N}} G_i/\mathcal{U}$. Then G is a simple pseudofinite group so has supersimple finite SU-rank theory, and, by Łos's Theorem, X is an infinite definable subset of G such that for each $d \in \mathbb{N}$, G is not a product of at most d conjugates of $X \cup X^{-1}$. By Theorem 4.1

(including the final assertion), G has a definable normal subgroup H which is infinite (as X/H is infinite) and is contained in a product of a bounded number of conjugates of $X \cup X^{-1}$. This is a contradiction, since by simplicity of G, $H = G$. □

Other applications of Theorem 4.1 were found in [19]. In particular, it was shown in Corollary 4.11 that certain maximal subgroups (those which are not 'subfield subgroups') of finite simple groups are uniformly definable in the groups, and hence, if also unbounded in order, they are 'uniformly maximal' [19, Proposition 4.2(ii)].

2. *Asymptotic classes.* The following definition is due to Elwes [7].

Definition 4.3 A class $\mathcal{C}$ of finite first order structures is, for some positive integer N, an *N-dimensional asymptotic class*, if the following holds.

(i) For every L-formula $\phi(\bar{x},\bar{y})$ where $l(\bar{x}) = n$ and $l(\bar{y}) = m$, there is a finite set of pairs $D \subseteq (\{0,\ldots,Nn\} \times \mathbb{R}^{>0}) \cup \{(0,0)\}$ and for each $(d,\mu) \in D$ a collection $\Phi_{(d,\mu)}$ of pairs of the form $(M,\bar{a})$ where $M \in \mathcal{C}$ and $\bar{a} \in M^m$, so that $\{\Phi_{(d,\mu)} : (d,\mu) \in D\}$ is a partition of $\{(M,\bar{a}) : M \in \mathcal{C}, \bar{a} \in M^m\}$, and

$$\big||\phi(M^n,\bar{a})| - \mu|M|^{\frac{d}{N}}\big| = o(|M|^{\frac{d}{N}})$$

as $|M| \to \infty$ and $(M,\bar{a}) \in \Phi_{(d,\mu)}$.

(ii) Each $\Phi_{(d,\mu)}$ is $\emptyset$-definable, that is to say $\{\bar{a} \in M^m : (M,\bar{a}) \in \Phi_{(d,\mu)}\}$ is uniformly $\emptyset$-definable across $\mathcal{C}$.

By the main theorem of [3], the class of finite fields is a 1-dimensional asymptotic class, and by Theorem 3.5.8 of [27] the classes of difference fields $(F_{2^{2k+1}}, x \mapsto x^{2^k})$ and $(\mathbb{F}_{3^{2k+1}}), x \mapsto x^{3^k})$ also form 1-dimensional asymptotic classes. The bi-interpretability results of Ryten mentioned above now yield the following.

Theorem 4.4 *[27, Ryten] If $\mathcal{C}$ is a family of finite simple groups of fixed Lie type, then $\mathcal{C}$ is an N-dimensional asymptotic class for some N.*

Remark 4.5 Let $\mathcal{C} = \{G_i : i \in \mathbb{N}\}$ be an asymptotic class of finite simple groups as above, and let $G^* := \Pi_{i\in\mathbb{N}} G_i/\mathcal{U}$ be an infinite ultraproduct of members of $\mathcal{C}$. Let $\phi(\bar{x},\bar{y})$ be a formula with $l(\bar{x}) = m$ and $l(\bar{y}) = n$, let $\bar{a} \in (G^*)^n$ with $\bar{a} = (\bar{a}_i)/\mathcal{U}$, and suppose that there is $U \in \mathcal{U}$ such that for all $i \in U$, $\phi(G_i^m, \bar{a}_i)$ has size approximately $\mu|G_i|^d$ (in the sense of asymptotic classes). Then it follows that $\mathrm{SU}(\phi((G^*)^m,\bar{a})) = d.\,\mathrm{SU}(G^*)$. This can be deduced from [7, 5.4], since $\mathcal{C}$ is parameter-bi-interpretable with a 1-dimensional asymptotic class (of fields or difference fields).

3. *Word maps.* Any non-trivial group word $w(x_1,\ldots,x_d)$ defines, in any group G, a map $w : G^d \to G$, the *word map* corresponding to w. It is shown

in [16] that there is a function f such that if G is a finite simple group, w is a non-trivial word, and $\epsilon > 0$, then $|w(G)| \geq |G|^{1-\epsilon}$ for sufficiently large G. In fact (and this could also be deduced from the last statement using Theorem 4.4), we have: if $\mathcal{C}$ is a family of finite simple groups of fixed Lie type, and w is a non-trivial word, then there is $\mu > 0$ such that if $G \in \mathcal{C}$ is sufficiently large then $|w(G)| \geq \mu|G|$.

Theorem 4.6 ([28]) *For every non-trivial word w there is $N = N(w)$ such that if G is a finite simple group with $|G| \geq N$ then $w(G)^3 = G$.*

This result is extended in various further directions in [17]. For example, it follows from [17, Theorem 1.7] that if $\mathcal{C}$ is a family of finite simple groups of fixed Lie type (other than the Suzuki or Ree groups) and w_1, w_2 are non-trivial words then there is N, dependent on the Lie type and w_1, w_2, such that if $G \in \mathcal{C}$ with $|G| > N$ then $w_1(G)w_2(G) = G$.

We mention a possible alternative approach, which fairly quickly yields Theorem 4.6 for families of finite simple groups of fixed Lie type together with a little further information, weaker than that in the last paragraph. It rests on the above-stated result of Larsen from [16], and some general model theory of groups in (super)simple theories. An advantage may be that Suzuki and Ree groups can be treated simultaneously with other families of finite simple groups with no extra work, though this rests on the major work of Hrushovski in [12], in combination with [27].

First, for groups definable in simple theories there is a theory of generic types, analogous to that in stable theories, developed by Pillay [23] and described in [31, Sections 4.3–4.5]. We shall consider a simple theory T, such that in any $M \models T$ there is an $\emptyset$-definable infinite group. Let κ be an infinite cardinal, sufficiently large relative to $|T|$ and to the size of any parameter sets we consider, and let $\bar{M}$ be a κ-saturated model of T, with an $\emptyset$-definable group G. Any parameter sets A, B, C will be subsets of $\bar{M}$ of much smaller size than κ, and M will always denote an elementary submodel of $\bar{M}$ of much smaller cardinality than κ. Let $\mathop{\smile\!\!\!\!\!|}$ denote the relation of non-forking (i.e. independence) in simple theories: for subsets A, B, C of $\bar{M}$, $A \mathop{\smile\!\!\!\!\!|}_C B$ denotes that A and B are independent over C in the sense of non-forking, that is, for any $\bar{a}$ from A, $\mathrm{tp}(\bar{a}/B \cup C)$ does not fork over C. If A is a set of parameters in $\bar{M}$, then $S_G(A)$ denotes the set of types over A which contain the formula $x \in G$; that is the set of maximal consistent (with T) sets of formulas in the variable x, with parameters from A, which include the formula $x \in G$. Following [31] (see Definition 4.3.2 and also Lemma 4.3.4) a type $p \in S_G(A)$ is *generic* if for any $b \in G$ and a realising p with $a \mathop{\smile\!\!\!\!\!|}_A b$, we have $ba \mathop{\smile\!\!\!\!\!|}_A b$. The group G has a certain subgroup G^o_A (the 'connected component over A'), which is the intersection of the A-type-definable subgroups of G of bounded index (that is, index less than κ), and a generic type over A is *principal* if it is realised in G^o_A. Part (i) of the following result was first proved in [24, Proposition 2.2], and (ii) is an immediate consequence.

Theorem 4.7 *Let T be a simple theory over a countable language, $\bar{M}$ an ω_1-saturated model of T with a countable elementary substructure M, and G an $\emptyset$-definable group in $\bar{M}$. Let p_1, p_2, p_3 be three principal generic types of G over M.*

(i) There are $g_1, g_2 \in \bar{M}$ such that $g_i \models p_i$ for $i = 1, 2$, $g_1 \mathop{\smile\!\!\!\!\!\!\,|}_M g_2$, and $g_1 g_2 \models p_3$.

(ii) If $r \in S_G(M)$ has realisations in G_M^o then there are $a_i \in G$ with $a_i \models p_i$ (for $i = 1, 2, 3$) such that $a_1 a_2 a_3 \models r$.

Proof. (i) See for example [31, Proposition 4.5.6], though as phrased above one must use ω_1-saturation to find the g_i in $\bar{M}$.

(ii) Choose $a_3, b \in \bar{M}$ such that $a_3 \models p_3$, $b \models r$, and $a_3 \mathop{\smile\!\!\!\!\!\!\,|}_M b$, and put $c_3 := a_3^{-1} b$. Let $p_3' := \mathrm{tp}(c_3/M)$. Then p_3' is a generic type of G over M. Indeed (repeatedly using 4.3.2 and 4.3.4 of [31]), $\mathrm{tp}(a_3^{-1}/M)$ is generic, so as $a_3^{-1} \mathop{\smile\!\!\!\!\!\!\,|}_M b$, we find $\mathrm{tp}(a_3^{-1}/Mb)$ is generic, so $\mathrm{tp}(a_3^{-1}b/Mb)$ is generic. As $\mathrm{tp}(a_3^{-1}/M)$ is generic and $a_3^{-1} \mathop{\smile\!\!\!\!\!\!\,|}_M b$ we also get $a_3^{-1}b \mathop{\smile\!\!\!\!\!\!\,|}_M b$, and this forces that $\mathrm{tp}(a_3^{-1}b/M)$ is generic. Also, by the assumptions on p_3 and r, p_3' has realisations in G_M^o so is principal.

It follows by (i) that there are $a_1, a_2 \in \bar{M}$ such that $a_1 \models p_1$, $a_2 \models p_2$, and $a_1 a_2 = c_3$. Hence $a_1 a_2 a_3 = b \models r$. □

Lemma 4.8 *[31] In the context above, assume that T is a finite SU-rank supersimple theory (so all definable sets have finite SU-rank), and let A be a parameter set. Then*

(i) If $p \in S_G(A)$ then p is generic if and only if $\mathrm{SU}(p) = \mathrm{SU}(G)$.

(ii) If X is an A-definable subset of G, then $\mathrm{SU}(G) = \mathrm{SU}(X)$ if and only if some generic type $p \in S_G(A)$ contains a formula defining X.

Proof. (i) See [31, P.168].

(ii) Immediate from (i) and the definition of SU-rank for types and formulas.
□

Theorem 4.9 *Let $\mathcal{C}$ be a family of finite simple groups of fixed Lie type, and let $w_i(x_1, \ldots, x_{d_i})$ be non-trivial words, for $i = 1, 2, 3$.*

(i) There is $N = N(\mathcal{C}, w_1, w_2, w_3) \in \mathbb{N}$ such that if $H \in \mathcal{C}$ with $|H| > N$ then $w_1(H)w_2(H)w_3(H) = H$.

(ii) $|H \setminus w_1(H)w_2(H)| = o(|H|)$ for sufficiently large $H \in \mathcal{C}$.

(iii) $|w_1(H)w_2(H)|/|H| \to 1$ as $|H| \to \infty$, for $H \in \mathcal{C}$.

Proof. (i) Suppose (i) is false. Then there is an infinite ultraproduct G^* of members of $\mathcal{C}$ such that $w_1(G^*)w_2(G^*)w_3(G^*)$ is a proper subset of G^*. We view G^* as an elementary submodel of a κ-saturated model T, in the manner described above. Then G^* is ω_1-saturated, and has a countable elementary substructure M. By the result of Larsen [16] mentioned above, there is $\mu > 0$ such that if $H \in \mathcal{C}$ is sufficiently large then $|w_i(H)| \geq \mu|H|$ for $i = 1,2,3$. It follows from Remark 4.5 that $SU(w_i(G^*)) = SU(G^*)$ for each i (and likewise, $SU(w_i(G)) = SU(G)$). Hence, by Lemma 4.8, there is for each $i = 1,2,3$ a generic type p_i of G over M containing the formula $x \in w_i(G)$. As all models of $T := \mathrm{Th}(G)$ are simple in the group-theoretic sense, a very saturated model of T cannot have a proper subgroup of bounded index, so $G = (G)^o_M$ and all generic types of G over M are principal.

Let r be any type over M realised in $G^* \setminus w_1(G^*)w_2(G^*)w_3(G^*)$. Then by Theorem 4.7(ii), and ω_1-saturation of G^*, there are $a_1, a_2, a_3, b \in G^*$ such that $a_i \models p_i$ and $b \models r$ and $a_1a_2a_3 = b$. In particular, $a_i \in w_i(G^*)$, so $b \in w_1(G^*)w_2(G^*)w_3(G^*)$, which is a contradiction.

(ii) Again, suppose this is false. Then by Theorem 4.4 there is $\nu > 0$ and infinitely many groups $H \in \mathcal{C}$ such that $|H \setminus w_1(H)w_2(H)| > \nu|H|$. Then, by Remark 4.5, we may choose an infinite ultraproduct G^* of members of $\mathcal{C}$ such that $\mathrm{SU}(G^* \setminus w_1(G^*)w_2(G^*)) = \mathrm{SU}(G^*)$. Again let M be a countable elementary substructure of G^*. By Lemma 4.8 for $i = 1,2,3$ there are generic types p_i of G^* over M such that p_1 contains the formula $x \in w_1(G^*)$, p_2 contains the formula $x \in w_2(G^*)$, and p_3 contains the formula $x \in G^* \setminus w_1(G^*)w_2(G^*)$. As in (i), the p_i are all principal. By ω_1-saturation and Theorem 4.7(i) there are $a_1, a_2 \in G^*$ such that $a_1 \models p_1$, $a_2 \models p_2$, and $a_3 := a_1a_2 \models p_3$. In particular, $a_i \in w_i(G^*)$ for $i = 1,2$ so $a_3 \in w_1(G^*)w_2(G^*)$, which is a contradiction.

(iii) This is immediate from (ii). □

Remark 4.10 1. Part (i) above is of course just a restatement of a special case of Theorem 4.6. Part (iii) was proved in [29]. We do not know whether these model-theoretic methods can yield the stronger assertion that if $\mathcal{C}$ is a family of finite simple groups of fixed Lie rank and w_1, w_2 are non-trivial words, then $w_1(G)w_2(G) = G$ for sufficiently large $G \in \mathcal{C}$. The latter (already proved except in the case of Suzuki and Ree groups in [17]) has recently been proved in [18] with $\mathcal{C}$ replaced by the class of *all* non-abelian finite simple groups.

2. It should be possible to strengthen the asymptotic statements in (ii), (iii), by working with tighter error terms in the definition of 'asymptotic class', in the manner of [3] rather than with the o-notation. More precisely, Theorem 4.4 should still hold if, in Definition 4.3, the condition

$$\big||\phi(M^n, \bar{a})| - \mu|M|^{\frac{d}{N}}\big| = o(|M|^{\frac{d}{N}})$$

is replaced by, for some constant c,

$$\big||\phi(M^n, \bar{a})| - \mu|M|^{\frac{d}{N}}\big| \leq c|M|^{\frac{d}{N}-\frac{1}{2}}.$$

We have not checked this.

3. If $w(x_1, \ldots, x_d)$ is a non-trivial word, and $\mathcal{C}$ is a class of finite simple groups of fixed Lie type, then w defines the word map $w : G^d \to G$ for $G \in \mathcal{C}$.

Theorem 4.4 is applicable in the class $\mathcal{C}$ to the formula $\phi(x_1, \ldots, x_d, y)$ which says $w(x_1, \ldots, x_d) = y$, and hence yields information on the distribution of the solution sets.

References

[1] H. Adler, 'A geometric introduction to forking and thorn-forking', J. Math. Logic 9 (2009), 1–20.

[2] J. Baldwin, J. Saxl, 'Logical stability in group theory', J. Austral. Math. Soc. 21 (1976), 267–276.

[3] Z. Chatzidakis, L. van den Dries, A.J. Macintyre, 'Definable sets over finite fields', J. Reine Angew. Math. 427 (1992), 107–135.

[4] G. Cherlin, E. Hrushovski, *Finite structures with few types*, Annals of Mathematics Studies No. 152, Princeton University Press, Princeton, 2003.

[5] J-L. Duret, 'Les corps faiblement algébraiquement clos non séparablement clos ont la propriété d'indépendance', *Model theory of Algebra and Arithmetic* (Eds. L. Pacholski et al.), Springer Lecture Notes vol. 834, 1980, pp. 135–157.

[6] C. Ealy, K. Krupinski, A. Pillay, 'Superrosy dependent groups having finitely many satisfiable generics', Ann. Pure Appl. Logic 151 (2008), 1–21.

[7] R. Elwes, 'Asymptotic classes of finite structures', J. Symb. Logic 72 (2007), 418–438.

[8] R. Elwes, H.D. Macpherson, 'A survey of asymptotic classes and measurable structures', in *Model Theory with Applications to Algebra and Analysis, Vol. 2* (Eds. Z. Chatzidakis, H.D. Macpherson, A. Pillay, A.J. Wilkie), London Math. Soc. Lecture Notes 350, Cambridge University Press, 2008, pp. 125–159.

[9] R. Elwes, E. Jaligot, H.D. Macpherson, M.J. Ryten, 'Groups in supersimple and pseudofinite theories', Proc. London Math. Soc., to appear.

[10] R. Elwes, M. Ryten, 'Measurable groups of low dimension', Math. Logic Quarterly 54 (2008), 374-386.

[11] E. Hrushovski, 'Pseudofinite fields and related structures', in *Model theory and applications* (Eds. L. Bélair, Z. Chatzidakis, P. D'Aquino, D. Marker, M. Otero, F. Point, A. Wilkie), Quaderni di Matematica, vol. 11, Caserta, 2005, 151–212.

[12] E. Hrushovski, 'The elementary theory of the Frobenius automorphism', preprint, arXiv:math/0406514v1 [math.LO].

[13] E.I. Khukhro, 'On solubility of groups with bounded centralizer chains', Glasgow Math. J. 51 (2009), 49–54.

[14] B. Kim, 'Forking in simple unstable theories', J. London Math. Soc. 57 (1998), 257–267.

[15] B. Kim, A. Pillay, 'Simple theories', Ann. Pure Appl. Logic 88 (1997) 149–164.

[16] M. Larsen, 'Word maps have large image', Isr. J. Math. 139 (2004), 149–156.

[17] M. Larsen, A. Shalev, 'Word maps and Waring type problems', J. Amer. Math. Soc 22 (2009), 437–466.

[18] M. Larsen, A. Shalev, P. Tiep, 'Waring problem for finite simple groups', Ann. Math., to appear.

[19] M.W. Liebeck, H.D. Macpherson, K. Tent, 'Primitive permutation groups of bounded orbital diameter', Proc. London Math. Soc. (3) 100 (2010), 216–248.

[20] M.W. Liebeck, N. Nikolov, A. Shalev, 'Product decompositions in finite simple groups', arXiv:1107.1528v1.

[21] H.D. Macpherson, K. Tent, 'Stable pseudofinite groups, J. Alg. 312 (2007), 550–561.

[22] A. Onshuus, 'Properties and consequences of thorn-independence', J. Symb. Logic 71 (2006), 1–21.

[23] A. Pillay, 'Definability and definable groups in simple theories', J. Symb. Logic 63 (1998), 788–796.

[24] A. Pillay, T. Scanlon, F. Wagner, 'Supersimple fields and division rings', Math. Research Letters 5 (1998), 473–483.

[25] F. Point, 'Ultraproducts and Chevalley groups', *Arch. Math. Logic* **38** (1999) 355–372.

[26] D.J.S. Robinson, *A course in the theory of groups*, 2nd edition, Springer, 1996.

[27] M.J. Ryten, *Results around asymptotic and measurable groups*, Ph.D. thesis, University of Leeds, 2007. http://www.logique.jussieu.fr/modnet/ preprint no. 123.

[28] A. Shalev, 'Word maps, conjugacy classes, and a non-commutative Waring-type theorem, Ann. Math. 170 (2009), 1383–1416.

[29] A. Shalev, 'Mixing and generation in simple groups', J. Alg. 319 (2008), 3075–3086.

[30] S. Shelah, 'Simple unstable theories', Ann. Pure Appl. Logic 19 (1980), 177–203.

[31] F. Wagner, *Simple theories*, Kluwer, Dordrecht, 2000.

[32] J.S. Wilson, 'On pseudofinite simple groups', J. London Math. Soc.) 51 (1995), 471–490.

[33] J.S. Wilson, 'First-order characterization of the radical of a finite group', J. Symb. Logic 74 (2009), 1429–1435.