Model theory of pseudofinite and profinite groups

Dugald Macpherson

October 7, 2015

1 Lecture I: Introduction, model theory of simple pseudofinite groups

Pseudofinite groups and fields.

Convention: We let $L_{\mathrm{gp}} := (\cdot, ^{-1}, 1)$ be the first order language of groups. Unless otherwise mentioned, any first order language L is assumed to be countable.

Definition 1.1. *A* pseudofinite group *is an infinite group which satisfies every first order sentence of L_{gp} which is true of all finite groups.*

N.B. The sentence (for abelian groups, so written additively) expressing 'if the map $x \mapsto px$ is injective then it is surjective' is true in all finite groups but false in the p-adic integers $(\mathbb{Z}_p, +)$.

Remark 1.2. A group G is pseudofinite if and only if it is elementarily equivalent to a non-principal ultraproduct of distinct finite groups.

In fact, the above definition, and this remark, make sense with 'group' replaced by 'field', 'ring', 'graph', L-structure, etc.

We briefly review ultraproducts. Fix a countable language L, and a family $\{M_i : i \in \omega\}$ of L-structures. Let $\mathcal{U}$ be a non-principal ultrafilter on ω. (An *ultrafilter* on ω is a family of subsets of ω closed under finite intersections and supersets, containing ω and omitting $\emptyset$, and maximal subject to this; it is *principal* if it has the form $\{X \subseteq \omega : a \in X\}$ for some $a \in \omega$, and is *non-principal* otherwise.) Define $M^* := \Pi_{i\in\omega} M_i$ (the Cartesian product of the M_i.) We say that some property P holds *almost everywhere* or *for almost all* i if

$$\{i : P \text{ holds for } M_i\} \in \mathcal{U}.$$

For $a = (a_i)_{i\in\omega}$ and $b = (b_i)_{i\in\omega}$, put $a \sim b$ if $\{i : a_i = b_i\} \in \mathcal{U}$. Then $\sim$ is an equivalence relation. Put $M = M^*/\sim$. Define relations etc. of L to hold of a tuple of M if they hold coordinatewise (in M_i) for almost all i. This is well-defined, and the resulting M is called the *ultraproduct* of the M_i with respect to $\mathcal{U}$, and here denoted $\Pi_{i\in\omega} M_i/\mathcal{U}$. The key fact about ultraproducts is

Theorem 1.3 (Los's Theorem)**.** *In the above notation, for any sentence σ, $M \models \sigma$ if and only if σ holds of M_i for almost all i.*

We also remark that the ultraproduct M will be ω_1-saturated: any type over any countable subset of M will be realised in M.

Our goals in this and the next section are the following.
(I) Describe 'tame' pseudofinite groups.
(II) Use model theory of tame pseudofinite structures to gain information on finite groups.

There are some well-known easily stated questions on pseudofinite groups, still open as far as I know, e.g.

Question 1.4. Is there a finitely generated pseudofinite group?

Question 1.5. (Zilber) Can a pseudofinite group have $\mathrm{SO}_3(\mathbb{R})$ (or any compact simple real Lie group) as a quotient? More generally, it would be interesting to identify positive sentences of L_{gp} which hold in all finite groups but not of all groups.

There is a beautiful model theory of pseudofinite *fields* originating with Ax in 1968.

Theorem 1.6 ([1])**.** *A field F is pseudofinite if and only if*
(i) F is perfect
(ii) F is quasifinite *(that is, inside a fixed algebraic closure, F has a unique extension of each finite degree), and*
(iii) F is pseudo-algebraically closed *(PAC), that is, every absolutely irreducible variety which is defined over F has an F-rational point.*

It is easily seen that (i) and (ii) hold of all finite fields, and are first-order expressible ((ii) needs some work). (iii) is expressible by a conjunction of first order sentences (this is not completely obvious) each of which, by the Lang-Weil estimates, holds in sufficiently large finite fields, and so each must hold of any pseudofinite field.

Ax also identified the complete theories of pseudofinite fields. If F is a field, then $\mathrm{Abs}(F)$ denotes the intersection of F with the algebraic closure of its prime subfield.

Theorem 1.7 ([1])**.** *If F_1, F_2 are pseudofinite fields, then $F_1 \equiv F_2$ (that is, they are elementarily equivalent) if and only if F_1, F_2 have the same characteristic and $Abs(F_1) = Abs(F_2)$.*

This, with further information in [1], was used to prove a uniform partial quantifier elimination in finite fields (and hence in pseudofinite fields: any formula $\phi(\bar{x})$ in the language L_{rings} of rings is equivalent in the theory of finite fields to a boolean combination of sentences of the form $\exists y g(\bar{x}, y) = 0$, where $g(\bar{X}, Y) \in \mathbb{Z}[\bar{X}, Y]$. This can be converted into a model completeness result

after the language is expanded by constants (see [5]). It is also known that any complete theory of pseudofinite fields has elimination of imaginaries over constants naming an elementary submodel.

We now consider *simple* groups which are pseudofinite. (Warning: we consider both simple groups and simple theories, and the word may occur twice in the same sentence with both meanings!)

Theorem 1.8 (Wilson [43])**.** *A pseudofinite group G is simple if and only if G is a simple group of Lie type (possibly twisted) over a pseudofinite field.*

Remark 1.9. Actually, in [43] the statement is just that G is *elementarily equivalent* to such a group of Lie type; the assertion as given uses also work of Ryten [38] discussed later.

Also, Ugurlu [41] has shown that one can replace 'simple' by 'definably simple of finite centraliser dimension', that is, groups G with the property that there is n such that for any $Y \subset G$ there is $Y_0 \subseteq Y$ with $|Y_0| \leq n$ and $C_G(Y) = C_G(Y_0)$.

The proof of $\Leftarrow$ is straightforward, as finite simple groups of fixed Lie type τ are *boundedly simple*: there is $d = d(\tau) \in \omega$ such that if G is such a group and $g, h \in G$ with $h \neq 1$, then g is a product of at most d conjugates of h and h^{-1}.

For $\Rightarrow$, Wilson first reduces to the case $G \equiv \Pi S_i/\mathcal{U}$ (a non-principal ultraproduct of finite simple groups S_i), and then analyses the possibilities for the S_i. It is easily seen that $H = \Pi_{n \geq 5} \operatorname{Alt}(n)/\mathcal{U}$ is not simple, since finite alternating groups contain 3-cycles, and elements of increasingly large support, when written as products of 3-cycles, require increasingly many 3-cycles. The problem is that, naively, H might have an elementary substructure which is a simple group. To eliminate such possibilities, it suffices to show that, uniformly, H has an $\emptyset$-definable conjugacy-invariant family of elements of small support, and also such a family of increasingly large support. Similar arguments work, e.g., for ultraproducts of finite simple groups of increasingly large Lie rank.

The groups of Lie type each correspond to a Dynkin diagram. For twisted groups, such as ${}^2E_6(q)$, ${}^2F_4(q)$, etc., the Dynkin diagram has a symmetry which yields a 'graph automorphism' of the corresponding untwisted group, essentially by permuting the root groups. One takes a product σ of a graph automorphism and an appropriate 'field automorphism' (arising from a power of the Frobenius), and, roughly speaking, takes the fixed points of σ in the untwisted group (this description is not accurate – see [3] for details.)

Stable theories and generalisations.

We consider here *stable theories*, and the (orthogonal) generalisations *simple* and *NIP* of stable. There are further notions, such as the common generalisation NTP2 of simple and NIP, and many others, and I believe pseudofinite groups satisfying these further properties have not been closely investigated.

Below, given a complete theory T, we let $\bar{M}$ denote a 'sufficiently saturated' model of T.

Definition 1.10. Let T be a complete theory. A formula $\phi(\bar{x}, \bar{y})$ is *unstable* (for T) if there are $\bar{a}_i \in \bar{M}^{|x|}$ and $\bar{b}_i \in \bar{M}^{|y|}$ (for all $i \in \omega$) such that for any $i, j \in \omega$, $\bar{M} \models \phi(\bar{a}_i, \bar{b}_j)$ if and only if $i < j$.

The theory T is *stable* if no formula is unstable for T.

Several other conditions are equivalent to stability. For example, for $A \subset \bar{M}$ let $S_n(A)$ be the set of all n-types over A. Then T is λ-*stable* (for λ an infinite cardinal) if for all $A \subset \bar{M}$ with $|A| \leq \lambda$ we have $|S_1(A)| \leq \lambda$, and T is stable if and only if it is λ-stable for some infinite λ.

A theory Y is stable if and only if there is an 'independence relation' $A \downarrow_C B$ (read 'A is independent from B over C') satisfying a number of natural axioms (suggested by linear independence in vector spaces, or algebraic independence in fields) such as *symmetry*: $A \downarrow_C B \Leftrightarrow B \downarrow_C A$. One of these axioms is

local character: for any $\bar{a}$ and B there is countable $B_0 \subset B$ such that $\bar{a} \downarrow_{B_0} B$.

Another is *stationarity*: Given $\bar{c}$ and $A \subseteq B$ there are at most $2^{\aleph_0}$ possibilities for $\mathrm{tp}(\bar{c}'/B)$ where $\bar{c}' \models \mathrm{tp}(\bar{c}/A)$ and $\bar{c}' \downarrow_A B$.
In a stable theory, the independence is given by *non-forking* (not defined here).

Definition 1.11. A formula $\phi(\bar{x}, \bar{y})$ has the *tree property* (with respect to T) if for some $k \in \omega$ the following hold: there are $\bar{a}_\eta \in \bar{M}^{|\bar{y}|}$ for all $\eta \in {}^{<\omega}\omega$ such that for any $\eta \in {}^{<\omega}\omega$ the set $\{\phi(\bar{x}, \bar{a}_{\eta i}) : i \in \omega\}$ is k-inconsistent (that is, any intersection of size k is inconsistent), and for any $\sigma \in {}^{\omega}\omega$, the set $\{\phi(\bar{x}, \bar{a}_\eta) : \eta \text{ restricts } \omega\}$ is consistent.

The theory T is *simple* if no formula has the tree property.

There is a characterisation of simplicity like the above one for stability, via an independence relation $\downarrow$, except that the 'stationarity' axiom is weakened to the 'independence theorem', also called 'type amalgamation'. Simplicity is a proper generalisation of stability. Within the class of simple theories is that of *supersimple* theories, characterised among simple theories by a strengthening of the local character condition on $\downarrow$: a simple theory T is *supersimple* if and only if, given any $\bar{a}$ and B, there is *finite* $B_0 \subseteq B$ such that $\bar{a} \downarrow_{B_0} B$. For supersimple theories, there is a notion of ordinal-valued *rank* on definable sets (or types), known as SU-rank, which we do not here define.

Definition 1.12. A formula $\phi(\bar{x}, \bar{y})$ has the *independence property* (for T) if there are $\bar{b}_i \in \bar{M}^{|\bar{y}|}$ for $i \in \omega$ such that for every $S \subset \omega$ there is $\bar{a}_S \in \bar{M}^{|\bar{x}|}$ such that, for each i, we have $\phi(\bar{a}_S, \bar{b}_i)$ if and only if $i \in S$.

A complete theory T has the *independence property* if some formula has the independence property for T. We say T is *NIP* if it does not have the independence property. NIP theories are also called *dependent* theories.

Example 1.13. Examples of ω-stable theories include algebraically closed fields, and (hence), for an algebraically closed field K, the K-rational points of an algebraic group defined over K. Separably closed fields which are not algebraically closed are stable but not ω-stable. Abelian groups (and more generally, modules, in the usual language of modules over a fixed ring) are stable, as are free groups.

Any o-minimal structure is NIP but not stable, as is $\mathbb{Q}_p$, the theory of any non-trivially valued algebraically closed field (in a language defining the valuation), and many other henselian valued fields.

Pseudofinite fields are not stable. For example, if F is a pseudofinite field of odd characteristic, and $\phi(x,y)$ is the formula $\exists z(z^2 = x - y)$, then ϕ has the independence property. However, pseudofinite fields have simple theory. In fact, more is true: they are supersimple (a strengthening of simple) of finite SU-rank. The well-known theory ACFA (algebraically closed fields equipped with a generic automorphism) has all its completions supersimple, of SU-rank ω. Groups such as $\mathrm{PSL}_n(F)$ (where F is a pseudofinite field) will have supersimple finite rank theory.

Suppose that G is a group definable in an NIP theory T, and let $\phi(x,\bar{y})$ be any formula. By the Baldwin-Saxl Theorem ([2], see also [42]), there is $n_\phi \in \omega$ such that any finite intersection of n_ϕ definable subgroups of G (i.e. a subgroup of form $\bigcap_{i=1}^t \phi(G,\bar{a}_i)$, where the $\phi(G,\bar{a}_i)$ are subgroups of G) is an intersection of at most n_ϕ of them. If in addition T is *stable*, then (essentially because T cannot have the 'strict order property'), this ensures that G has the descending chain condition on intersections of ϕ-definable subgroups of G – there is a fixed bound on the lengths of such chains. In particular, we may apply this to the formula $\phi(x,y)$ expressing $xy = yx$. If T is NIP then there is n_ϕ such that for any finite $F \subset G$ there is $F_0 \subset F$ with $|F_0| \leq n_\phi$ such that $C_G(F) = C_G(F_0)$, and if in addition G is stable then any chain of centralisers has bounded length.

Theorem 1.14. *(1) (Easy consequence of [5].) Any pseudofinite field has supersimple rank 1 theory.*

(2) (From [16], resting on earlier work of Chatzidakis, Hrushovski and Peterzil (see [6] and [7]) Let p be a prime, and let $m,n \in \omega$ with $m \geq 1, n > 1$, and $(m,n) = 1$. Let $\mathcal{C}_{m,n,p}$ be the class of finite difference fields *(fields equipped with an automorphism) of form $(\mathbb{F}_{p^{kn+m}}, \mathrm{Frob}^k)$ where $k \in \omega$. Then any non-principal ultraproduct of $\mathcal{C}_{m,n,p}$ has supersimple rank 1 theory. For us, this has particular interest for $(m,n,p) = (1,2,2)$ and $(m,n,p) = (1,2,3)$.*

Corollary 1.15 (Hrushovski)**.** *Any simple pseudofinite group has supersimple finite rank theory.*

This follows from Theorem 1.14 because the groups are interpretable in the corresponding fields or difference fields. In fact, more is true, namely

Theorem 1.16 (Ryten)**.** *Any family of finite simple groups of any fixed Lie type (other than Suzuki and Ree groups) is uniformly bi-interpretable (over parameters) with the corresponding family of finite fields.*

(ii) The Ree groups ${}^2F_4(2^{2k+1})$ and the Suzuki groups ${}^2B_2(2^{2k+1})$ are uniformly parameter bi-interpretable with the difference fields $(\mathbb{F}_{2^{2k+1}}, x \mapsto x^{2^k})$, and the Ree groups ${}^2G_2(3^{2k+1})$ are uniformly parameter bi-interpretable with $(\mathbb{F}_{3^{2k+1}}, x \mapsto x^{3^k})$.

Remark 1.17. Theorem 1.16 was recently used by Nies and Tent [32] to show that

(1) finite simple groups are log-compressible, i.e., if G is a finite simple group, there is a sentence ϕ with unique model G, such that ϕ has length $O(\log|G|)$, and more generally

(2) for any finite group G there is such a sentence ϕ of length $O((\log|G|)^3)$.

2 Generalised stability for pseudofinite groups, applications

We aim here to give structural results for pseudofinite groups with stable, or more generally simple or NIP, theory. We then discuss 'asymptotic classes' of groups, and some possible lines of application.

Recall that the (soluble) *radical* $R(G)$ of a group G is the subgroup generated by the soluble normal subgroups of G. Always $R(G) \lhd G$, and if G is finite then $R(G)$ is soluble.

Theorem 2.1 ([27])**.** *(1) Let $\mathcal{C}$ be a class of finite groups such that all ultraproducts of members of $\mathcal{C}$ are NIP. Then there is $d \in \omega$ such that $|G : R(G)| \leq d$ for each $G \in \mathcal{C}$.*

(2) If G is pseudofinite NIP group with a fixed finite bound on the lengths of centraliser chains (e.g. if G is stable) then G has an $\emptyset$-definable soluble subgroup of finite index.

Remark 2.2. In (2), the conclusion is false without some assumption like that on centralisers. A counterexample is given in Section 3 (see Remark 3.7.

The proof makes essential use of part (2) of the following theorem of Wilson.

Theorem 2.3. *(1) [44] There is an sentence σ of L_{gp} such that if G is a finite group then $G \models \sigma$ if and only if G is soluble.*

(2) [45] There is a formula $\psi(x)$ such that if G is a finite group then $\psi(G) = R(G)$.

Question 2.4. Are there analogues of Theorem 2.3(1) with 'nilpotent' replacing 'soluble', and of (2) with the Fitting subgroup in place of $R(G)$?

Sketch Proof of Theorem 2.1. (1) Let $G \in \mathcal{C}$. Let $\psi(x)$ be as in Theorem 2.3(2). For $G \in \mathcal{C}$ let $\bar{G} = G/R(G)$, and put $S := \mathrm{Soc}(\bar{G})$ (the direct product of the minimal normal subgroups). Then $S = T_1 \times \ldots \times T_k$, where the T_i are non-abelian finite simple groups.

Claim 1. There is a bound on k as G ranges through $\mathcal{C}$. Indeed, for each i pick $x_i \in T_i \setminus Z(T_i)$ and $y_i \in T_i$ with $[x_i, y_i] \neq 1$. For $w \subset \{1, \ldots, k\}$ put $z_w = \Pi_{j \notin w} y_j$. Then $[x_j, z_w] = 1 \Leftrightarrow j \in w$. Hence, the NIP assumption forces a bound on k.

Claim 2. There is a bound on the Lie rank of any T_i (or on t if $T_i = \mathrm{Alt}_t$). This is proved essentially as in Claim 1, as otherwise some T_i contains increasingly large direct powers of PSL_2 or of Alt_4.

Claim 3. The T_i have bounded size. If this was false, then groups $G \in \mathcal{C}$ would contain arbitrarily large finite simple groups of fixed Lie rank (by Claims 1 and 2 and the classification of finite simple groups) so some ultraproduct would be a simple pseudofinite group, and (e.g. by Theorem 1.16) would interpret a

pseudofinite field. But as noted in Examples 1.13, pseudofinite fields do not have NIP theory.

By Claim 3, $|S|$ is bounded, and it follows easily that $|G : R(G)|$ is bounded.

(2) We may suppose that $G = \Pi G_i/\mathcal{U}$ (an ultraproduct of finite groups), where each non-principal ultraproduct of the G_i is elementarily equivalent to G. Thus by (1) there is a finite bound on $|G_i : R(G_i)|$. By stability of G and the remarks before Theorem 1.14, there is some $e \in \omega$ such that every centraliser chain in G has length at most e, and hence the same holds for any G_i. By a result of Kukhro [20], there is a function f such that each group $R(G_i)$ has derived length at most $f(e)$. It follows that $R(G)$ (also defined by ψ) is soluble.

Example 2.5. *[26]*

(1) There is an ω-stable pseudofinite group G which is not nilpotent-by-finite. It has form $(\mathbb{C}, +) \rtimes \Gamma$ for some infinite but 'small' $\Gamma \leq (\mathbb{C}^*, \cdot)$.

(2) The 'Mekler construction' gives, for any odd prime p, examples of pseudofinite ω-stable groups which are nilpotent of class 2 and exponent p but not finite-by-abelian-by-finite.

Next, we discuss pseudofinite groups with simple theory. Here, note that the examples (even supersimple of finite rank) include simple groups of Lie type over pseudofinite fields (by Corollary 1.15) and also, for odd primes p, infinite extraspecial p-groups of exponent p, that is, groups G of exponent p such that $G' = Z(G) = \Phi(G) \cong C_p$, where $\Phi(G)$ is the Frattini subgroup of G. Extraspecial p-groups have SU rank 1, and are finite-by-abelian but not abelian-by-finite. They have infinite descending chains of centralisers, and do not have a smallest finite index definable subgroup.

Consider a class $\mathcal{C}$ of finite groups with all ultraproducts of $\mathcal{C}$ having simple theory. For $G \in \mathcal{C}$, $R(G)$ is uniformly $\emptyset$-definable (by [45]) and $\mathrm{Soc}(G/R(G))$ is a product of boundedly many non-abelian finite simple groups of bounded Lie rank (by variants of the proofs of Claims 1 and 2 above).

Question 2.6. In this setting, must $R(G)$ have bounded derived length, as G ranges through $\mathcal{C}$?

I suspect this question has a negative answer, but if we assume all ultraproducts of $\mathcal{C}$ are *supersimple*, then the answer is positive, by the following results of Milliet [29], a significant strengthening of results in [13].

Theorem 2.7. *If G is a pseudofinite group with supersimple theory, then $R(G)$ is definable and soluble (and likewise, if we assume G has finite SU-rank, then* $\mathrm{Fitt}(G)$ *is definable and nilpotent).*

Thus, if G is pseudofinite with superstable theory then G has soluble radical $R(G)$, and if $S = \mathrm{Soc}(G/R(G))$, then $S = T_1 \times \ldots \times T_k$ where the T_i are non-abelian finite of pseudofinite simple groups. If $\bar{S}$ denotes the preimage of S in G then $G/\bar{S}$ embeds in $\mathrm{Aut}(T_1 \times \ldots \times T_k)$.

We have not discussed much properties of SU-rank, but note that finite groups have SU-rank 0, and that if G has supersimple theory of finite SU-rank and $H \leq G$ is definable, than $\mathrm{SU}(G) = \mathrm{SU}(H) + \mathrm{SU}(G/H)$, where G/H

denotes the interpretable set of left cosets of H in G. There is some information on supersimple pseudofinite groups of small SU-rank, namely

Theorem 2.8. *(1) If G is pseudofinite supersimple of SU-rank 1 then G is finite-by-abelian-by-finite,*

(2) If G is pseudofinite supersimple of SU-rank 2 then G is soluble-by-finite.

Certain infinite (monomial) SU-rank versions of these have recently been proved by Wagner. These proofs are without the classification of finite simple groups, and it would be interesting to try without CFSG to recover PSL_2 under a rank 3 assumption. Using CFSG, a classification is given in [13] of structure (G, X) which are supersimple of finite rank, with $\mathrm{SU}(X) = 1$, and with the group G acting definably and primitively on the set X.

Applications

1. First, we mention a version of the well-known 'Zilber Indecomposability Theorem' for groups of finite Morley rank, itself a generalisation of a classical result on algebraic groups.

Theorem 2.9 (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.

Theorem 2.10. *Let $\mathcal{C}_\tau$ be the family of finite simple groups of fixed Lie type τ (possibly twisted), and let $\phi(x, \bar{y})$ be an L_{gp}-formula. Then there is $d = d(\phi, \tau)$ such that if $G \in \mathcal{C}_\tau$, $\bar{a} \in G^{|\bar{y}|}$, and $X = \phi(G, \bar{a})$ satisfies $|X| > d$, then G is a product of at most d conjugates of $X \cup X^{-1}$.*

2. Next, we recall the following result of [35]. We do not give background on generic types.

Corollary 2.11. *Let $\mathcal{C}_\tau$ be as in Theorem 2.10, and let $\phi_i(x, \bar{y})$ be formulas for $i = 1, 2, 3$. Then there is $\mu \in \mathbb{Q}^{>0}$ such that for any sufficiently large $G \in \mathcal{C}_\tau$ and $\bar{a}_1, \bar{a}_2, \bar{a}_3 \in G^{|\bar{y}|}$, if $|\phi(G, \bar{a}_i)| \geq \mu |G|$ for each i, then*

$$\phi_1(G, \bar{a}_1).\phi_2(G, \bar{a}_2).\phi_3(G, \bar{a}_3) = G.$$

The proof shows in addition that $\frac{\phi_1(G,\bar{a}_1).\phi_2(G,\bar{a}_2)|}{|G|} \to 1$ as $|G| \to \infty$. We remark that the same result follows from Nikolov-Pyber [31], where it is rapidly derived from a result of Gowers.

In particular, if $w(x_1, \ldots, x_d)$ is a non-trivial group word, then w defines a map $G^d \to G$ by evaluation, and we denote the image of w by $w(G)$. Then, using a result of Larsen [21], Corollary 2.11 yields

Theorem 2.12. *Let w_1, w_2, w_3 be non-trivial group words, and $\mathcal{C}_\tau$ a family of finite simple groups of fixed lie type. Then $w_1(G)w_2(G)w_3(G) = G$ for sufficiently large $G \in \mathcal{C}_\tau$.*

Remark 2.13. There has been considerable recent literature on word maps, with much stronger results proved. For example, by [23], if w_1, w_2 are non-trivial words, and G is *any* sufficiently large finite simple group, then $w_1(G)w_2(G) = G$. This holds even for quasisimple groups.

3. Asymptotic classes.

Definition 2.14. Let $\mathcal{C}$ be a class of finite L-structures. Then $\mathcal{C}$ is an *N-dimensional asymptotic class* if the following hold.

(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 $D \subseteq (\{0, \dots, Nn\} \times \mathbb{R}^{>0}) \cup \{(0,0)\}$ 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

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

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 $\mathcal{C}$.

This notion was developed in dimension 1 in

The class of all finite fields is, by the main theorem of [5], a *1-dimensional asymptotic class* in the sense of [25]. Likewise, by [38] the classes of difference fields of form $(\mathbb{F}_{2^{2k+1}}, x \mapsto x^{2^k})$ and $(\mathbb{F}_{3^{2k+1}}, x \mapsto x^{3^k})$ are 1-dimensional asymptotic classes. This yields

Theorem 2.15. *[38] Let $\mathcal{C}_\tau$ be the class of all finite simple groups of fixed Lie type τ. Then $\mathcal{C}_\tau$ is an N-dimensional asymptotic class for some N (and the values of μ in the definition are rational).*

Applications of this have not been properly explored, but for example it could be used to obtain uniformity results for fibres of word maps for finite simple groups of fixed Lie type.

4. We know that classes $\mathcal{C}_\tau$ of finite simple groups of fixed Lie type are uniformly definable in finite (difference) fields. In fact, much more is definable.

Proposition 2.16. *Let $\mathcal{C}_\tau$ be a class of finite simple groups $G(q)$ of fixed Lie type τ, and let $V(\lambda)$ be an irreducible $\mathbb{F}_q G(q)$-module of restricted weight λ, with the action of $G(q)$ on $V(\lambda)$ given by $\rho(q)$. Then the structures $(G(q), V_\lambda(q), \rho(q))$ are uniformly definable in the field $\mathbb{F}_q$ or in corresponding difference fields.*

We also consider pairs (G, H) where G is a finite simple group of Lie type and H is a maximal (proper) subgroup of G (named by a unary predicate). This is equivalent to considering the group G together with a definable primitive action of G on a set X, namely the set of left cosets of H in G. (A permutation group G on X is *primitive* if there is no proper non-trivial G-invariant equivalence relation on X; this is equivalent to point stabilisers being maximal subgroups.) If $G = G(q)$ is a simple group of Lie type and $q = (q')^r$, then a *subfield subgroup* of G is one of the form $G(q')$ (so of the same Lie type), embedded naturally. Such subgroups can be maximal if r is prime.

Theorem 2.17. *[22] Let τ be a fixed Lie type, and let $\mathcal{C}_{\tau,d}$ be the set of pairs (G, H) where G is a finite simple group of Lie type τ, H is a maximal subgroup of G, and if H is a subfield subgroup then the corresponding field extension has degree at most d. Then*

(1) the class $\mathcal{C}_{\tau,d}$ is uniformly definable in the corresponding family of fields or difference fields, that is, there are finitely many tuples of formulas which serve (with suitable choice of parameters) to define all such pairs;

(2) any non-principal ultraproduct of such a family $\mathcal{C}_{\tau,d}$ will be a pair (G^*, H^*) with supersimple finite rank theory, such that H^* is maximal in G^*.

The last assertion in (2) above follows from the remaining assertions, together with an argument using Theorem 2.9. This was used in [22] to give a description of all ω-saturated pseudofinite primitive permutation groups, that is ω-saturated pseudofinite pairs (G, H) with H maximal in G. Essentially, this is equivalent to describing families $\mathcal{F}_d$ of finite primitive permutation groups G on sets X such that, for every orbit E of G on the set $X^{[2]}$ of unordered 2-subsets of X, the graph on X with edge set E is connected of diameter at most d.

3 Profinite groups with NIP theory

Recall that a *profinite group* is an inverse limit of finite groups, or equivalently, is a compact totally disconnected Hausdorff topological group. In such a group, open subgroups all have finite index, though the converse is false in general. Profinite groups arise heavily in model theory. For example, if G is a sufficiently saturated group definable in an NIP theory T, then the intersection G^o of the definable subgroups of G of finite index is an $\emptyset$-definable normal subgroup of G of index at most $2^{\aleph_0}$; the quotient G/G^o has naturally the structure of a profinite group and is an important invariant of T.

How should we view a profinite group G model-theoretically? It is a fixed structure, but in model theory we naturally consider all models of its theory, and other models will in general not be profinite.

There have been several approaches. One is that of Newelski [30] and Krupinski [17], who consider *profinite structures* (G, H), where G is a profinite group (or, more generally, some other kind of inverse limit) and $H \leq \mathrm{Aut}(G)$ preserves the inverse system, so fixes setwise each open subgroup. Another approach is

that of Chatzidakis [4], who considers profinite groups as infinitely sorted structures, with sort n consisting essentially of the disjoint union of all the finite quotients by open subgroups of index at most n.

In [28] we take a different approach, viewing a system of basic open subgroups as something which should be uniformly definable (so that, for example, as with o-minimal structures, the property of a definable function $G \to G$ being continuous at a point is definable). So we present a profinite group G as a 2-sorted structure $\mathcal{G} = (G, I)$, where G is a group (with the L_{gp}-language on G), $(I, \leq)$ is a partially ordered set, and there is a binary relation $K \subseteq G \times I$ so that the family $\{K_i : i \in I\}$ is a system of basic open subgroups of G; here, for $i \in I$, $K_i := \{g \in G : (g, i) \in K\}$, and we write $i \leq j$ if and only if $K_i \supseteq K_j$. We say that the profinite group $\mathcal{G} = (G, I)$ is *full* if every open subgroup of G has form K_i for some $i \in I$. The corresponding 2-sorted language is referred to as L_{prof}.

Theorem 3.1. *[28] Let $\mathcal{G} = (G, I)$ be a full profinite group. Then $\mathrm{Th}(\mathcal{G})$ is NIP if and only if G has an open normal subgroup N with $N = P_1 \times \ldots \times P_t$, where each P_i is a compact p_i-adic analytic group (for distinct primes $p_1, \ldots, p_t$).*

Corollary 3.2. *If $\mathcal{G} = (G, I)$ is a full profinite group with NIP theory, then $\mathcal{G}$ is strongly NIP. Furthermore, there is an NIP theory in which $\mathcal{G}$ is definable, and in which the closed subgroups of G are uniformly definable.*

We first discuss p-adic analytic groups. Recall first the p-adic field $\mathbb{Q}_p$. Fix a prime p and define the map $v_p : \mathbb{Q} \to \mathbb{Z}$, where if $q \in \mathbb{Q}$ with $q = p^m a/b$ (where $a, b \in \mathbb{Z}$ with $b \neq 0$ and $(p, a) = (p, b) = 1$), we put $v_p(q) = m$ (and $v_p(0) = \infty$). The map v_p is a *valuation*, that is, $v_p(x) = \infty$ if and only if $x = 0$, $v_p(xy) = v_p(x) + v_p(y)$, and $v_p(x+y) \geq \mathrm{Min}\{v_p(x), v_p(y)\}$. Now for $x \in \mathbb{Q}$ define $|x|_p := p^{-v_p(x)} \in \mathbb{R}$. The $|-|_p$ is a norm on $\mathbb{Q}$, and we may complete $\mathbb{Q}$ with respect to this norm in the usual way to obtain the p-adic field $\mathbb{Q}_p$. The map v_p extends to a valuation $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$. Define $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}$, the valuation ring (called the ring of p-adic integers). This has a unique maximal ideal $p\mathbb{Z}_p$, with residue field $\mathbb{F}_p$. The whole valuation structure $(\mathbb{Q}_p, \mathbb{Z}_p; \mathbb{Z}, v_p)$ is definable in the field $(\mathbb{Q}_p, +, \cdot)$. It has NIP theory, as do certain expansions by analytic functions.

If $V \subset \mathbb{Z}_p^r$ is non-empty and open, and $f = (f_1, \ldots, f_s) : V \to \mathbb{Z}_p^s$ is a function, and $y \in V$, then f is *analytic at y* if there are $F_1, \ldots, F_s \in \mathbb{Q}_p[[X_1, \ldots, X_r]]$ for $i = 1, \ldots, s$ and $h \in \mathbb{N}$ such that $f_i(y + p^h x) = F_i(x)$ for each $i = 1, \ldots, s$ and $x \in \mathbb{Z}_p^r$. We say f is *analytic on V* if it is analytic at every point of V. If X is a topological space, then a *p-adic chart of dimension n* of X is a triple (U, ϕ, n) where U is an open subset of X, and ϕ is a homeomorphism from U onto an open subset of $\mathbb{Z}_p^n$. The charts $c = (U, \phi, n)$ and $d = (V, \psi, m)$ of X are *compatible* if, putting $W := U \cap V$, the maps $\psi \circ \phi^{-1}|_{\phi(W)}$ and $\phi \circ \psi^{-1}|_{\psi(W)}$ are analytic on $\phi(V)$ and $\phi(W)$ respectively. There is a natural notion of (p-adic) *atlas* on the topological space X, consisting of a covering by compatible charts, and an equivalence relation *compatibility* of atlases: two atlases A and B of X are compatible if every chart of A is compatible with every chart of B. Finally,

a $\mathbb{Q}_p$-*analytic manifold structure* on X is an equivalence class of compatible atlases on X, and such a structure is called a *p-adic analytic manifold*.

If G is a topological group, then G is a *p-adic analytic group*, or *p-adic Lie group*, if G has the structure of a p-adic analytic manifold such that the maps $G \times G \to G$ and $G \to G$, given by group multiplication and inversion respectively, are analytic.

Example 3.3. Examples of compact p-adic analytic profinite groups include

(i) $(\mathbb{Z}_p, +)$, with the open subgroups all having form $p^k\mathbb{Z}_p$ for some $k \in \omega$, so indexed by ω;

(ii) $\mathrm{SL}_2(\mathbb{Z}_p)$;

(iii) there is a natural exponential map exp defined on $p\mathbb{Z}_p$ (for $p > 2$ – the argument needs adapting for $p = 2$). It is an isomorphism $(p\mathbb{Z}_p, +) \to (1 + p\mathbb{Z}_p, \cdot)$, and its graph is a p-adic analytic group which is analytically isomorphic to $(\mathbb{Z}_p, +)$, but this isomorphism is not definable in the pure field $\mathbb{Q}_p$, that is, is not semialgebraic.

The group $C_p wr \mathbb{Z}_p$ can naturally be viewed as a pro-p group, but is not p-adic analytic.

Question 3.4. Is there a compact p-adic analytic group which is not abstractly isomorphic to a semialgebraic group? (There may be well-known examples.)

Question 3.5. How much of Theorem 3.1 holds without the assumption of fullness?

Without the 'full' assumption, we can say much less, but at least have the following. A group is *prosoluble* if it is an inverse limit of finite soluble groups.

Proposition 3.6. *Let $\mathcal{G} = (G, I)$ be NIP profinite. Then G has an open prosoluble definable normal subgroup.*

Proof. Let $\mathcal{C} = \{G/K_i : i \in I\}$. Then $\mathcal{C}$ is a collection of finite groups which are *uniformly* definable in an NIP theory, so any ultraproduct of $\mathcal{C}$ is NIP. Hence, by Theorem 2.1(1), the members of $\mathcal{C}$ have a uniformly definable soluble radical of bounded index. The result follows easily.

The following is an easy corollary of the proof of Theorem 3.1. There is an ordinal valued notion of rank in NIP theories, known as *dp-rank*, and structures of finite dp-rank are said to be *strongly NIP*.

Remark 3.7. We give an example (*cf.* Theorem 2.1(2)) of an NIP pseudofinite group which is not soluble by finite. Let $G = \mathrm{SL}_2(\mathbb{Z}_p)$, and for each $k > 0$ let G_k be the open normal subgroup of G of form

$$G_k := \{\begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} : a, b, c, d \in p^k\mathbb{Z}_p\},$$

a *congruence subgroup* of G. Then the groups G_k are uniformly definable in the NIP structure $\mathbb{Q}_p$, so the quotients G/G_k are uniformly interpretable. Let $\mathcal{U}$ be a non-principal ultrafilter on ω, and put

$$G^* := \Pi_{k\in\omega}(G/G_k)/\mathcal{U}.$$

Then G^* is an NIP pseudofinite group. By ω_1-saturation of ultraproducts, it has a normal subgroup N such that $G^*/N \cong G$. In particular, G^* is not soluble-by-finite.

We discuss further profinite groups, and in particular pro-p groups (inverse limits of finite p-groups). First, if G is profinite and $X \subset G$ then $\bar{X}$ denotes the topological closure of X in G. We says that G is *finitely generated* if there is finite $F \subset G$ such that $G = \overline{\langle F \rangle}$. The following major result was proved much earlier in the pro-p case by Serre.

Theorem 3.8. *Let G be a finitely generated profinite group, and $H \leq G$. Then H is open in G if and only if $|G : H|$ is finite.*

Definition 3.9. (i) The profinite group G has *rank* r, if r is finite and minimal such that every closed subgroup of G is r-generated.

(ii) A pro-p group G is *powerful* if: either p is odd and $G/\overline{G^p}$ is abelian, where $G^p = \langle \{x^p : x \in G\} \rangle$, or $p = 2$ and $G/\overline{G^4}$ is abelian.

(iii) The pro-p group G has a series of closed normal subgroups defined by: $G = P_1(G) \geq P_2(G) \geq \ldots$, where $P_{n+1}(G) := \overline{P_n(G)^p [P_n(G), G]}$.

(iv) The powerful pro-p group G is *uniformly powerful* if it is finitely generated and $|G/P_2(G)| = |P_i(G)/P_{i+1}(G)|$ for each i.

The following major body of results is an amalgam of work of Lazard, Lubotsky, Mann and Shalev.

Theorem 3.10. *Let G be a pro-p group. Then the following are equivalent.*

(i) G is a p-adic analytic group

(ii) G is finitely generated and has a powerful subgroup of finite index.

(iii) G has finite rank.

(iv) G has polynomial subgroup growth, that is, there is $\alpha > 0$ such that for each $n > 0$, G has at most n^α subgroups of index n.

(v) G does not involve arbitrarily large wreath products of the form $C_p \mathrm{wr} C_{p^n}$.

(vi) G is isomorphic to a closed subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$ for some suitable d.

Proof. See for example Theorem 5.11 of [19] (and the main theorem of [40] for (v)). □

Next, we describe an important enrichment of the structure $\mathbb{Z}_p$, due to Denef and van den Dries [8]. Let $\nu = (\nu_1, \ldots, \nu_m) \in \mathbb{N}^m$, put $X = (X_1, \ldots, X_m)$, and $X^\nu = X_1^{\nu_1} \cdot \ldots \cdot X_m^{\nu_m}$, and consider power series of the form $\Sigma_{\nu \in \mathbb{N}^m} a_\nu X^\nu$, where $|a_\nu|_p \to 0$ as $|\nu| := \nu_1 + \ldots + \nu_m \to \infty$. We denote by $\mathbb{Z}_p\{X\}$ the ring of all such power series. Each such power series converges on $\mathbb{Z}_p^m$ so defines a function $\mathbb{Z}_p^m \to \mathbb{Z}$. The language L_D^{an} has symbols for all such functions (for all m), together with a binary function symbol D, defined by putting $D(x, y) = x/y$ if $|x|_p \leq |y|_p$ and $y \neq 0$, and $D(x, y) = 0$ otherwise. Let T_{an}^D be the theory of $\mathbb{Z}_p$ in the language L_{an}^D. We refer to the corresponding expansion of $\mathbb{Z}_p$ as $\mathbb{Z}_p^{\mathrm{an}}$. We remark that by [10, Lemma 1.9], if $f : \mathbb{Z}_p^m \to \mathbb{Z}_p$ is an analytic function, then f is definable in the language L_{an}^D. This is an elementary application of the topological compactness of $\mathbb{Z}_p^m$.

Theorem 3.11. *(i) The theory T_{an}^D has quantifier elimination.*
(ii) The theory T_{an}^D is NIP.

Part (ii) above follows from [11] and [15] – it is shown in [11] that $\mathbb{Z}_p^{\mathrm{an}}$ is *P-minimal*, and in [15] that all P-minimal structures are NIP.

For the direction $\Leftarrow$ in Theorem 3.1, our key tool is the following.

Theorem 3.12 (du Sautoy [10])**.** *If G is a p-adic analytic pro-p group, then G is definable in $\mathbb{Z}_p^{\mathrm{an}}$, and its open subgroups are uniformly definable.*

We give some of the basic ideas behind du Sautoy's proof. First, p-adic expoenntiation on G is well-defined: if $g \in G$ and $\lambda \in \mathbb{Z}_p$, define

$$g^\lambda = \lim_{a_n \to \lambda} g^{a_n},$$

where $a_n \in \mathbb{Z}$ (this is well-defined, i.e. independent of the choice of (a_n)). Given topological generators $x_1, \ldots, x_d$ of G with d minimal, each $x \in G$ is uniquely of the form

$$x = x_1^{\lambda_1} \cdot \ldots \cdot x_d^{\lambda_d},$$

with $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}_p$, so G 'lives' on $\mathbb{Z}_p^d$. Furthermore the group operation and inversion are analytic maps ($\mathbb{Z}_p^d \times \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ and $\mathbb{Z}_p^d \to \mathbb{Z}_p^d$ respectively) so are definable in $\mathbb{Z}_p^{\mathrm{an}}$.

Furthermore, every open subgroup has a 'good basis' $(h_1, \ldots, h_d)$, and the set of good bases is definable, so I consists of equivalence classes of good bases. With a little further work to deal with finite extensions, this yields Theorem 3.1$\Leftarrow$.

We now consider the direction $\Rightarrow$, so suppose that $\mathcal{G} = (G, I)$ is a full profinite group with NIP theory.

If G has infinite rank, then by standard results on profinite groups, G has for every k an open normal subgroup N_k and there is H_k with $N_k \leq H_k \leq G$ such that H_k/N_k is a (finite) p-group requiring at least k generators. This group H_k/N_k has a quotient isomorphic to $(C_p)^l$ for some $l \geq k$) (factor out the Frattini subgroup and apply the Burnside Basis Theorem). The C_p^l are uniformly interpretable, contradicting NIP. (Subgroups of index p are uniformly interpretable so by NIP there is t such that any such (finite) intersection is a t-intersection, so has index at most p^t, a contradiction.)

Now by a theorem of C. Read [36], G has closed normal subgroups $N \triangleleft A \triangleleft G$ such that G/A is finite, A/N is abelian, and N is pronilpotent. The group N is a Cartesian product of Sylow subgroups, as is A/N. Use the NIP condition to show that there are finitely many in each case, and then that A/N is finite.

We end with a conjecture, suggestive of a 1-based/fieldlike dichotomy for compact p-adic analytic groups. We view a finite group $G/P_n(G)$ as an L_{prof}-structure $(G/P_n(G), \omega)$, interpreting K_i by the group $K_iP_n(G)/P_n(G)$, so for each n, the K_i are all equal for $n \geq i$).

Conjecture 3.13. *Let $\mathcal{G} = (G, I)$ be a compact p-adic analytic group, full as a profinite group. Then the following are equivalent.*
(i) The ring $\mathbb{Z}_p$ is not interpretable in $\mathcal{G}$.

(ii) For every sentence σ in the language L_{prof}, there is $N \in \omega$ such that either each quotient $(G/P_n(G), I)$ satisfies σ forn $> N$, or each such quotient satisfies $\neg\sigma$.

(iii) The group G is nilpotent-by-finite.

References

[1] J. Ax, 'The elementary theory of finite fields', Ann. Math. 88 (1968), 239–271.

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

[3] R.W. Carter, *Simple groups of Lie type*, Wiley, London, 1972.

[4] Z. Chatzidakis, 'Model theory of profinite groups having the Iwasawa property', Ill. J. Math. 42 (1998), 70–96.

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

[6] Z. Chatzidakis, E. Hrushovski, 'The model theory of difference fields', Trans. Amer. Math. Soc. 351 (1999), 2997–3071.

[7] Z. Chatzidakis, E. Hrushovski, Y. Peterzil, 'Model theory of difference fields II. Periodic ideals and the trichotomy in all characteristics', Proc. London Math. Soc. (3) 85 (2002), 257–311.

[8] J. Denef, L. van den Dries, 'p-adic and real subanalytic sets', Ann. Math. 128 (1988), 79–138.

[9] J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal, *Analytic pro-p groups*, London Math. Soc. Lecture Notes no. 157, Cambridge University Press, Cambridge, 1991.

[10] M.P.F. du Sautoy, 'Finitely generated groups, p-adic analytic groups, and Poincaré series', Ann. Math. 137 (1993), 639–670.

[11] L. van den Dries, D. Haskell, H.D. Macpherson, 'One-dimensional p-adic analytic subsets', J. London Math. Soc. (2) 59 (1999), 1–20.

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

[13] R. Elwes, E. Jaligot, H.D. Macpherson, M.J. Ryten, 'Groups in supersimple and pseudofinite theories', Proc. London Math. Soc. (3) 103 (2011), 1049–1082.

[14] R. Guralnick, 'On the number of generators of a finite group', Arch. Math. 53 (1989), 521–523.

[15] D. Haskell, H.D. Macpherson, 'A version of o-minimality for the p-adics', J. Symb. Logic 62 (1997), 1075–1092.

[16] E. Hrushovski, The elementary theory of the Frobenius automorphisms, arXiv:math/0406514.

[17] K.Krupinski, 'Profinite structures interpretable in fields', Ann. Pure Appl. Logic 142 (2006), 19–54.

[18] I. Kaplan, A. Usvyatsov, A. Onshuus, 'Additivity of the dp rank', Trans. Amer. Math. Soc. 365 (2013), 5783–5804.

[19] B. Klopsch, 'An introduction to compact p-adic Lie groups', in *Lectures on profinite topics in group theory* (Eds. B. Klosch, N. Nikolov, C. Voll), London Math Soc. Student Texts, 77, Cambridge University Press, Cambridge, 2011, pp. 7-61.

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

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

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

[23] M. Larsen, A. Shalev, P. Tiep, The Waring problem for finite simple groups, *Ann. Math.* **174** (2011) 1885–1950.

[24] Lucchini, 'A bound on the number of generators in a finite group', Arch. Math 42 (1989), 313–317.

[25] H.D. Macpherson, C. Steinhorn, One-dimensional asymptotic classes of finite Structures, *Trans. Amer. Math. Soc.* 360 (2008) 411–448.

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

[27] H.D. Macpherson, K. Tent, 'Pseudofinite groups with NIP theory and definability in finite simple groups', in *Groups and model theory*, Contemp. Math. 576, Amer. Math. Soc., Providence, RI, 2012, 255-267.

[28] H.D. Macpherson, K. Tent, 'Profinite groups with NIP theory and p-adic analytic groups', in preparation.

[29] C. Milliet, 'On the definability of radicals in supersimple groups', MODNET preprint server no. 444.

[30] L. Newelski, 'Small profinite structures', Trans. Amer. Math.Soc. 354 (2002), 925–943.

[31] N. Nikolov, L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem, *J. Euro. Math. Soc.* **13** (2011) 1063–1077

[32] A. Nies, K. Tent, 'Describing finite groups by short first-order sentences', arXiv:1409:8390

[33] N. Nikolov, D. Segal, 'On finitely generated profinite groups, I: strong completeness and uniform bounds', Ann. Math. 165 (2007), 171–238.

[34] N. Nikolov, D. Segal, 'On finitely generated profinite groups, II: products in quasisimple groups', Ann. Math. 165 (2007), 239–273.

[35] A. Pillay, T. Scanlon, F. Wagner, Supersimple fields and division rings, *Math. Research Letters* 5 (1998) 473-483.

[36] C.D. Read, *Finiteness properties of profinite groups*, PhD thesis, University of London, 2010.

[37] L. Ribes, P. Zaleskii, *Profinite groups*, Springer, Berlin, 2000.

[38] M.J. Ryten, Model theory of finite difference fields and simple groups, Ph.D. Thesis, University of Leeds (2007).
(http://www1.maths.leeds.ac.uk/Pure/staff/macpherson/ryten1.pdf)

[39] J-P. Serre, *Galois cohomology*, Springer, Berlin, 1997.

[40] A. Shalev, 'Characterisation of p-adic analytic groups in terms of wreath products', J. Algebra 145 (1992), 204–208.

[41] P. Ugurlu, 'Pseudofinite groups as fixed points of simple groups of finite Morley rank', J. Pure Applied Alg. 217 (2013), 892–900.

[42] F. Wagner, *Stable groups*, London Math. Soc. Lecture Notes no. 240, Cambridge University Press, 1997.

[43] J.S. Wilson, *Profinite groups*, Oxford University Press, Oxford, 1998.

[44] J.S. Wilson, 'Finite axiomatisation of finite soluble groups', J. London Math. Soc. 74 (2006), 566–582.

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