Lecture 10:
Applications of model theory in combinatorics

Gabriel Conant
University of Cambridge

December 3, 2020
An Excursion into Model Theory and Its Applications
LMS Online Lecture Series

Outline

1. Graph Regularity

2. Approximate subgroups

Part I

Graph Regularity

Pseudofinite Methods

Applications of model theory via ultraproduct constructions:

Asymptotic statements about finite structures $\longleftrightarrow$ Uniform statement about an infinite structure

10.1 Ramsey's Theorem

For any $n \geq 1$ there is $R(n) \geq 1$ such that any finite graph of size at least $R(n)$ contains a complete or independent subset of size n.

Proof. Suppose this fails for some $n \geq 1$. Then for any $R \geq 1$ there is a graph G_R of size at least R with no complete or independent set of size n. Now $(\prod_R G_R)/\mathcal{U}$ (with $\mathcal{U}$ non-principal) is an infinite graph with no complete or independent set of size n.

Claim. Any infinite graph contains an infinite complete or independent subset.

Graph regularity

Let (V, E) be a finite graph and fix $\epsilon > 0$.

Given $X, Y \subseteq V$, call (X, Y) ϵ-regular if there is some $\delta \in [0, 1]$ such that for any $A \subseteq X$ and $B \subseteq Y$, we have

$$\big||E \cap (A \times B)| - \delta|A \times B|\big| < \epsilon|X \times Y|$$

Idea: (X, Y) is "ϵ-close" to a random bipartite graph of uniform edge density δ.

10.2 Szemerédi's Regularity Lemma (weak version)

For any $\epsilon > 0$ there is some $m \geq 1$ such that, if (V, E) is a finite graph then there is a partition $V = X_1 \cup \ldots \cup X_n$ such that $n \leq m$ and, if S is the set of (i, j) for which (X_i, X_j) is not ϵ-regular then $\sum_{(i,j)\in S} |X_i \times X_j| < \epsilon|V|^2$.

This result has many applications, e.g., in additive combinatorics (finding arithmetic progressions in dense sets of integers) and extremal graph theory (counting the number of graphs satisfying certain properties).

The pseudofinite counting measure

Let L be a language, and let $(M_i)_{i \in I}$ be a collection of finite L-structures.
Let $M = (\prod_{i \in I} M_i)/\mathcal{U}$, where $\mathcal{U}$ is an ultrafilter on I.
Any definable set $X \subseteq M^n$ is of the form $(\prod_{i \in I} X_i)/\mathcal{U}$, where $X_i \subseteq M_i^n$.
The normalized pseudofinite counting measure of X is $\mu(X) = \lim_{\mathcal{U}} |X_i|/|M_i^n|$.[1]

10.3 Adding the measure to the language

Let $\mathcal{R} = (\mathbb{R}, +, <, 0)$ and $\mathcal{R}^* = \mathcal{R}^I/\mathcal{U}$. Call $x \in \mathcal{R}^*$ finite if $|x| \leq r$ for some real $r > 0$, and infinitesimal if $|x| \leq r$ for all real $r > 0$.

Exercise: For any finite $x \in \mathcal{R}^*$ there is a unique $r \in \mathcal{R}$ such that $x - r$ is infinitesimal. This r is called the standard part of x, denoted $\mathrm{st}(x)$.

Let $\boldsymbol{M}_i$ be the *two-sorted* structure $(M_i, \mathcal{R})$ with additional functions:
For every L-formula $\phi(x_1, \ldots, x_n; y_1, \ldots, y_k)$, add a k-ary function symbol f_ϕ from the M_i sort to the $\mathcal{R}$ sort. Interpret $f_\phi^{\boldsymbol{M}_i}(\bar{b}) = |\phi(M_i^n, \bar{b})|/|M_i^n|$.

Let $\boldsymbol{M} = (\prod_{i \in I} \boldsymbol{M}_i)/\mathcal{U} = (M, \mathcal{R}^*)$.

Exercise: If $X \subseteq M^n$ is defined by $\phi(\bar{x}; \bar{b})$, then $\mu(X) = \mathrm{st}(f_\phi^{\boldsymbol{M}}(\bar{b}))$.

[1] Definition. $\lim_{\mathcal{U}} r_i = s$ if and only if for all $\epsilon > 0$, $\{i \in I : |r_i - s| < \epsilon\} \in \mathcal{U}$.

Pseudofinite graph regularity

Now assume L contains (at least) a binary relation symbol E.

Let $(M_i)_{i \in I}$ be a collection of finite L-structures where E^{M_i} is a graph relation.

Let $M = (\prod_{i \in I} M_i)/\mathcal{U}$, where $\mathcal{U}$ is an ultrafilter on I.

Given definable $X, Y \subseteq M$, call (X, Y) ϵ-regular if there is $\delta \in [0, 1]$ such that, for any definable $A \subseteq X$ and $B \subseteq Y$ we have

$$\left|\mu(E \cap (A \times B)) - \delta\mu(A \times B)\right| < \epsilon\mu(X \times Y).$$

10.4 Szemerédi's Regularity Lemma (pseudofinite version)

For any $\epsilon > 0$, there is a partition $M = X_1 \cup \ldots \cup X_n$ such that each X_i is definable and, if S is the set of (i, j) for which (X_i, X_j) is not ϵ-regular, then $\sum_{(i,j) \in S} \mu(X_i \times X_j) < \epsilon$.

Exercise: Use this to prove the regularity lemma for finite graphs.

Proof of pseudofinite Szemerédi

$M = (M; E, \ldots)$ is a pseudofinite L-structure expanding a graph.

The pseudofinite counting measure μ is a finitely additive probability measure on definable subsets of M.

Fact 10.5: μ determines a unique regular Borel probability measure on $S_n(M)$ such that, if $X \subseteq M^n$ is definable, then the clopen set $[X]$ has measure $\mu(X)$.

Let $\mathbf{1}_E \colon S_2(M) \to [0,1]$ be the characteristic function of $[E]$.

Let $\mathcal{B}$ be the σ-algebra on $S_2(M)$ generated by all clopen sets $[A \times B]$ for all definable $A, B \subseteq M$.

10.6 Radon-Nikodym Theorem (special case)

There is a $\mathcal{B}$-measurable function $f \colon S_2(M) \to [0,1]$ such that for any $W \in \mathcal{B}$,

$$\int_W f \, d\mu = \int_W \mathbf{1}_E \, d\mu = \mu([E] \cap W).$$

In particular, for definable $A, B \subseteq M$, we have $\int_{[A \times B]} f \, d\mu = \mu(E \cap (A \times B))$.

Proof of pseudofinite Szemerédi, continued

Claim 1: For any $\epsilon > 0$, there is a partition $M = X_1 \cup \ldots \cup X_n$, with X_i definable, and some $\delta_{ij} \in [0,1]$ such that if $g = \sum_{ij} \delta_{ij} \mathbf{1}_{[X_i \times X_j]}$ then $\int |f - g| d\mu < \epsilon$.

Proof: First approximate f by a $\mathcal{B}$-simple function h such that $\|f - h\|_\infty < \epsilon/2$. Then use regularity of μ to find the desired g with $\int |h - g| d\mu < \epsilon/2$.

Now fix $\epsilon > 0$ and choose g as in Claim 1, but with $\int |f - g| d\mu < \epsilon^2$.
Define $S = \left\{(i,j) : \int_{[X_i \times X_j]} |f - \delta_{ij}| d\mu \geq \epsilon \mu(X_i \times X_j)\right\}$.

Claim 2: $\sum_{(i,j) \in S} \mu(X_i \times X_j) < \epsilon$.

Proof: If not, then one directly computes $\int |f - g| d\mu \geq \epsilon^2$.

Claim 3: If $(i,j) \notin S$ then (X_i, X_j) is ϵ-regular with density δ_{ij}.

Proof: Fix definable $A \subseteq X_i$ and $B \subseteq X_j$. Then

$$\begin{aligned} \left|\mu(E \cap (A \times B)) - \delta_{ij}\mu(A \times B)\right| &= \left|\int_{[A \times B]} f \, d\mu - \int_{[A \times B]} \delta_{ij} \, d\mu\right| \\ &\leq \int_{[A \times B]} |f - \delta_{ij}| d\mu < \epsilon \mu(X_i \times X_j). \end{aligned}$$

Stable Graph Regularity

A binary relation E on a set V is k-stable if there do not exist $v_1, \ldots, v_k, w_1, \ldots, w_k \in V$ such that $E(v_i, w_j)$ if and only if $i \leq j$.

Folklore (Lovász, Seymour, Trotter / Alon, Duke, Leffman, Rödl, Yuster): Unstable graphs witness the need for irregular pairs in Szemerédi's regularity lemma.

10.7 Theorem (Malliaris-Shelah 2011)

For any $\epsilon > 0$ and $k \geq 1$, there is some m such that any finite k-stable graph (V, E) can be partitioned $V = X_1 \cup \ldots \cup X_n$, with $n \leq m$, so that every pair (X_i, X_j) is ϵ-regular with density in $[0, \epsilon) \cup (1 - \epsilon, 1]$.

A short pseudofinite proof was given by Malliaris and Pillay (2015). Their proof gives no information about m in terms of ϵ and k. The original proof by Malliaris and Shelah yields $m = O_k(\epsilon^{-O_k(1)})$.

NIP Graph Regularity

A binary relation E on a set V is **k-NIP** if there do not exist $v_1, \ldots, v_k \in V$ and $w_s \in V$ for all $s \subseteq \{1, \ldots, k\}$ such that $E(v_i, w_s)$ holds if and only if $i \in s$.

10.8 Theorem

Suppose (V, E) is a finite k-NIP graph. Then for any $\epsilon > 0$ there is a partition $V = X_1 \cup \ldots \cup X_n$, with $n \leq O_k(\epsilon^{-O_k(1)})$, and a set $S \subseteq \{1, \ldots, n\}^2$ such that:

- $\sum_{(i,j) \in S} |X_i \times X_j| < \epsilon |V|^2$ and
- if $(i, j) \notin S$ then (X_i, X_j) is ϵ-regular with density in $[0, \epsilon) \cup (1 - \epsilon, 1]$.

History: In combinatorics, NIP is better known as VC-dimension.

- Alon, Fisher, Newman (2007) and Lovász-Szegedy (2010)
- Chernikov and Starchenko (2016): generalization to "generically stable" measures on definable NIP hypergraphs in arbitrary structures
- Fox, Pach, Suk (2017): sharp bounds for (finite) hypergraphs

Arithmetic Regularity

Arithmetic regularity was invented by Green (2005) as a group-theoretic analogue of graph regularity for subsets of finite abelian groups.

Terry and Wolf (2017) investigated arithmetic regularity for "stable" subsets of finite abelian groups.

10.9 Theorem (Conant, Pillay, Terry 2017)

Suppose G is a finite group and $A \subseteq G$ is such that "$xy \in A$" is k-stable. Then for any $\epsilon > 0$, there is a normal subgroup $H \leq G$ of index $O_{k,\epsilon}(1)$ and a set $Y \subseteq G$, which is a union of cosets of H, such that $|A \triangle Y| < \epsilon |H|$.

Related results for NIP (finite VC-dimension):

- Alon, Fox, Zhao (2018): finite abelian groups of bounded exponent
- Sisask (2018): finite abelian groups
- Conant, Pillay, Terry (2018): arbitrary finite groups

Lecture 10 Exercises (Part 1)

10.E1 Fill in the details of the pseudofinite proof of Ramsey's Theorem outlined on slide 1.

10.E2 Let I be a nonempty set and $\mathcal{U}$ an ultrafilter on I. Let (X, d) be a compact metric space. Prove that for any sequence $(r_i)_{i \in I}$ from X, there is a unique $s \in X$ such that for all $\epsilon > 0$, $\{i \in I : d(r_i, s) < \epsilon\} \in \mathcal{U}$ (s is called the ultralimit of $(r_i)_{i \in I}$ along $\mathcal{U}$, and denoted $\lim_{\mathcal{U}} r_i$).

10.E3 Prove the exercises in "10.3 Adding the measure to the language".

10.E4 Prove Szemerédi's Regularity Lemma (10.2) from the pseudofinite version (10.4). Hints will be posted to Piazza.

Part II

Approximate subgroups

Approximate subgroups

Definition. A subset A of a group G is a *k-approximate subgroup* if $1 \in A$, $A = A^{-1}$, and $A^2 := \{xy : x, y \in A\}$ is covered by k left translates of A.

10.10 Theorem (Freiman 1975)

If A is a finite k-approximate subgroup of $\mathbb{Z}$, then there is a generalized arithmetic progression $P \subseteq \mathbb{Z}$ of rank $O_k(1)$ such that $A \subseteq P$ and $|P| \leq O_k(|A|)$.

A (symmetric) generalized arithmetic progression of rank n in an abelian group G is a subset of the form $\{r_1 g_1 + \ldots + r_n g_n : r_1, \ldots, r_n \in \mathbb{Z},\ |r_i| \leq K_i\}$ for some fixed $g_1, \ldots, g_n \in G$ and $K_1, \ldots, K_n \in \mathbb{N}$.

10.11 Theorem (Green-Ruzsa 2005)

If G is an abelian group, and A is a finite k-approximate subgroup, then there is a generalized arithmetic progression $P \subseteq G$ of rank $O_k(1)$, and a finite subgroup $H \leq G$, such that $A \subseteq P + H$ and $|P + H| \leq O_k(|A|)$.

Approximate subgroups of nonabelian groups

- (2008) Helfgott $\mathrm{SL}_2(\mathbb{F}_p)$
- (2010) Dinai) $\mathrm{SL}_2(\mathbb{F}_{p^k})$
- (2010) Tao solvable groups with bounded solvability length
- (2010) Bourgain, Gamburd, & Sarnak $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ for m square-free
- (2010) Gill & Helfgott solvable algebraic groups over $\mathbb{F}_p$
- (2010, 2011) Pyber & Szabó; Breuillard, Green, & Tao simple algebraic groups over finite fields
- (2011) Helfgott $\mathrm{SL}_3(\mathbb{F}_p)$
- (2011, 2012) Breuillard & Green torsion-free nilpotent groups, solvable linear groups, compact Lie groups
- (2012) Varjú $\mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$ for m square-free
- (2012) Bourgain & Varjú $\mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$ for any m
- (2012) Salehi & Varjú $\boldsymbol{G}(\mathbb{Z}/m\mathbb{Z})$ for m square-free and $\boldsymbol{G}$ perfect

Common theme: Approximate subgroups exhibit “nilpotent structure”.

Approximate subgroups of arbitrary groups

Notation in groups: $X \subseteq_d Y$ means X can be covered by d left translates of Y.

10.12 Theorem (Hrushovski 2012)

Suppose G is a group and A is a finite k-approximate subgroup. Then, for any $f : \mathbb{N} \to \mathbb{N}$, there is some $d \leq O_{k,f}(1)$ and a chain $X_N \subseteq \ldots \subseteq X_1 \subseteq A^4$, with $N \geq f(d)$, such that the following properties hold.

(*i*) $A \subseteq_d X_1$, and $X_i \subseteq_d X_{i+1}$ for all i.

(*ii*) For all i, $X_i = X_i^{-1}$ and $X_{i+1}^2 \subseteq X_i$.

(*iii*) If $r < i + j$ then $[X_i, X_j] \subseteq X_r$.

Idea: A^4 contains arbitrary approximations to a virtually nilpotent subgroup.

10.13 Theorem (Breuillard, Green, Tao 2012)

If G is a group and A is a finite k-approximate subgroup, then there is a "nilprogression" $P \subseteq G$ of rank and step $O_k(1)$, and a finite subgroup $H \leq G$, such that $PH \subseteq A^4$ and $A \subseteq_{O_k(1)} PH$.

The pseudofinite setting

Let L be a language containing the language of groups and a unary relation A.

Let $(G_i)_{i \in I}$ be a collection of L-structures such that the group language is interpreted as a group and $A_i := A^{G_i}$ is finite and nonempty.

Let $G = (\prod_{i \in I} G_i)/\mathcal{U}$, where $\mathcal{U}$ is an ultrafilter on I.

Then $A = A^G$ is a *pseudofinite* definable subset of G.

Remark. A is a k-approximate subgroup of G if and only if the set of $i \in I$, for which A_i is a k-approximate subgroup of G_i, is in $\mathcal{U}$.

Without loss of generality, replace G with a κ-saturated and strongly κ-homogeneous elementary extension, where κ is large (e.g., inaccessible). Throughout: "bounded" means "strictly less than κ".

Definition. A subset X of G is type-definable if it is an intersection of a bounded number of definable sets.

Hrushovski's Stabilizer Theorem

Let $\langle A \rangle$ denote the subgroup of G generated by A.

10.14 Theorem

Assume A is an approximate subgroup. Then there is a type-definable bounded-index subgroup H of $\langle A \rangle$ such that $H \subseteq A^4$.

Timeline:

- Hrushovski: Previous result after expanding the language, plus further properties of H.
- Breuillard, Green, & Tao: Combinatorial proof based on work of Sanders.
- Massicot-Wagner: Modification of BGT's proof in order to avoid expanding the language.

Both proof strategies exploit the existence of a measure on definable sets.

Measures

Recall $G \succeq (\prod_{i \in I} G_i)/\mathcal{U}$.

Any definable set $X \subseteq (\prod_{i \in I} G_i)/\mathcal{U}$ is of the form $(\prod_{i \in I} X_i)/\mathcal{U}$, where $X_i \subseteq G_i$. The $|A|$-normalized pseudofinite counting measure of X is

$$\mu(X) = \lim_{\mathcal{U}} |X_i|/|A_i|.$$

So μ is a finitely additive measure on definable sets, which takes values in the extended real line $[0, \infty]$, and $\mu(A) = 1$.

We add μ to the language and bring it with us to G: $\mu(\phi(x, b)) = \mathrm{st}(f_\phi^G(b))$.

Exercise. Suppose $X \subseteq \langle A \rangle$ is definable. Then $X \subseteq (A \cup A^{-1})^n$ for some n. Therefore, if A is an approximate subgroup, then X is covered by finitely many left translates of A. In particular, $\mu(X) < \infty$.

Local Stability

Assume A is a k-approximate subgroup.

Hrushovski works in an expansion of L similar to what is used for adding μ.

Fix $M \prec G$ with $|M| < \kappa$. Then μ is M-invariant: if $\phi(x, \bar{y})$ is an L-formula, and $\bar{b}, \bar{c} \in G^{\bar{y}}$ are such that $\mathrm{tp}(\bar{b}/M) = \mathrm{tp}(\bar{c}/M)$, then $\mu(\phi(x, \bar{b})) = \mu(\phi(x, \bar{c}))$.

Claim. There is $p \in S_1(M)$ such that $A \in p$ and $\mu(\phi(x)) > 0$ for any $\phi(x) \in p$.

Let $X = p(G) := \{a \in G : a \models p\}$. Then X is a type-definable set contained in A, and any definable set containing X has positive measure.

Let $H = (X^{-1}X)^2$. So $H \subseteq A^4$.

Main Result. H is a type-definable bounded-index subgroup of $\langle A \rangle$.

Key Tool: Given formulas $\phi(x, \bar{y})$ and $\psi(x, \bar{z})$, define a relation R on $G^{\bar{y}} \times G^{\bar{z}}$ such that $R(\bar{b}, \bar{c})$ holds if and only if $\mu(\phi(x, \bar{b}) \wedge \psi(x, \bar{c})) = 0$. Then R is stable.

Approximating by a chain

Setting: G is a saturated group, and $A \subseteq G$ is definable and pseudofinite.

Assume A is an approximate subgroup. Then we have a type-definable bounded-index subgroup H of $\langle A \rangle$ such that $H \subseteq A^4$.

10.15 Corollary

If A is an approximate subgroup, then there is a chain

$$A^4 \supseteq X_1 \supseteq X_2 \supseteq X_3 \supseteq \dots$$

of definable subsets of G satisfying the following properties:

(*i*) $A \subseteq_{<\omega} X_1$, and $X_i \subseteq_{<\omega} X_{i+1}$ for all $i \geq 1$.

(*ii*) For all $i \geq 1$, $X_i = X_i^{-1}$ and $X_{i+1}^2 \subseteq X_i$.

Missing: (*iii*) If $r < i + j$ then $[X_i, X_j] \subseteq X_r$.

Nilpotence

Without loss of generality: H is a normal subgroup of $\langle A \rangle$.

Set $\Gamma = \langle A \rangle / H$, and let $\pi : \langle A \rangle \to \Gamma$ be the canonical map.

Fact 10.16. Γ is a locally compact Hausdorff group under the topology where $C \subseteq \Gamma$ is closed if $\pi^{-1}(C) \cap X$ is type-definable for any definable $X \subseteq \langle A \rangle$.

Gleason-Yamabe (1953) *locally compact groups are modeled by Lie groups*
For any open identity nbhd $U \subseteq \Gamma$, there is an open subgroup $V \leq \Gamma$ and a compact normal subgroup $K \leq V$ such that $K \subseteq U$ and V/K is a Lie group.

Hrushovski/BGT use a version for "local groups" due to Goldbring (2009).

Breuillard, Green, & Tao (requires pseudofiniteness of A).
The Lie groups V/K above have nilpotent connected components.

This is a sophisticated variation on Jordan's Theorem (1878): Any finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ contains an abelian subgroup of index $O_n(1)$.

Future Directions

The original results for abelian groups by Freiman (10.10) and Green-Ruzsa (10.11) provide explicit bounds. For nonabelian groups, quantitative versions of Hrushovksi/BGT (10.12 & 10.13) are known for various classes of groups, but there is no known proof of the general result that avoids ultraproducts and produces effective bounds.

Given a sufficiently saturated group G and a definable approximate subgroup A, one can obtain the locally compact quotient $\langle A \rangle / H$ whenever there is a left-invariant finitely additive real-valued measure on definable subsets of $\langle A \rangle$. More generally, what can be said about approximate subgroups which do not admit such a measure?

See: E. Hrushovski, *Beyond the Lascar group*, arXiv 24 Nov 2020

Lecture 10 Exercises (Part 2)

Let G be a sufficiently saturated expansion of a group, and suppose $A \subseteq G$ is $\emptyset$-definable and pseudofinite. Let μ be the $|A|$-normalized pseudofinite counting measure on definable subsets of G (described on slide 17).

10.E5 Suppose $X \subseteq \langle A \rangle$ is definable. Show that $X \subseteq (A \cup A^{-1})^n$ for some n. Using this, show that if A is an approximate subgroup, then X is covered by finitely many left translates of A and $\mu(X) < \infty$.

10.E6 Suppose $M \prec G$ and $|M|$ is bounded. Show that there is a type $p \in S_1(M)$ such that $A \in p$ and $\mu(\phi(x)) > 0$ for any $\phi(x) \in p$.

10.E7 Prove Corollary 10.15 from Theorem 10.14.

10.E8 Suppose H is a type-definable bounded index subgroup of $\langle A \rangle$. Let $N = \bigcap_{a \in \langle A \rangle} aHa^{-1}$. Prove that N is a type-definable bounded-index subgroup of $\langle A \rangle$.

10.E9 Prove Fact 10.16. (This may require some effort.)

Lecture 10 Exercises (Part 2)

10.E10 Prove that for that for any $k, n \geq 1$ there is some $m \geq 1$ such that, if G is a group and $A \subseteq G$ is a k-approximate subgroup, then there is a set $X \subseteq G$ such that $X = X^{-1}$, $X^n \subseteq A$, and $A \subseteq_m X$.

Discussion: This statement follows very easily from Theorem 10.12. Thus, for practice with ultraproduct constructions, one should solve the previous exercise using only Theorem 10.14.