The logic of large finite structures

Ehud Hrushovski

UCLA, April 23, 2011

The pseudo-finite world

Theorem (C. Jordan)

Let G be a finite subgroup of $GL_n(\mathbb{C})$. Then $|G|$ has an Abelian subgroup of bounded index (depending only on n.)

"Il importe ... de bien préciser le sens que nous attachons aux mot limité et illimité. Ils ne sont pas synonymes de *fini* et *infini* ..."

- use of char. 0: no non-identity unipotent element.
- In *Équations diférentielles linéaires à intégrale algébrique*, Crelle 1878, pp. 89-215:
- Differential Galois theory (Picard-Vessiot), 2pp. Above pseudo-finite theorem: 13pp. Determination of the (finitely many) finite subgroups of GL_2 and $GL_3(\mathbb{C})$, 111pp.
- Glimpses by: finite group theory, algebraic geometry, additive combinatorics, dynamical systems, model theory.

Unbounded finite world is as rich as infinite world

... if one considers the syntax of formal statements *about* infinite objects (Gödel, 1930)

... or if one filters the quantifiers (in Paris-Harrington, 1977).

Consider finite structures A with sub-universes $A_\alpha \subset A_\beta \subset \cdots A$ ($\alpha, \beta, \cdots \in I$, I a linearly ordered set.)

$(\forall x)(\exists y)(...)$ interpreted as: $(\forall x \in A_\alpha)(\exists y \in A_\beta)(....)$ - *any* $\alpha < \beta \in I$.

This is coherent, if I is sufficiently Ramsey.

Skolem's paradox crosses the finite/infinite boundary: any sentence with an infinite model has a finite quasi-model (and vice versa).

However, Ramsey tends to force: $|A_\alpha| <<< |A_\beta| <<< |A|$.

View from the classification of finite simple groups,

A large finite simple group is:
Alt_n,
or an object of algebraic geometry
e.g. $SL_4(F_q)$,
or of high-dimensional linear algebra
$SL_n(F_2)$
or a combination of the two parameters $SL_n(F_q)$

Follows from classification of *all* finite simple groups, concentrating on sporadics; no pseudo-finite proof known. (Compare Jordan.)
Gorenstein's reason: difficulty of using simplicity (or for group actions, *primitivity:* no invariant equivalence relation).
Properties of *all* structures equivalent to classification of primitive ones?

In these talks, I would like to describe a model-theoretic viewpoint, born in the study of uncountably categorical structures, that has proved useful in several pseudo-finite regimes: bounded rank, bounded orbit spaces, and now of approximate subgroups in the sense of Tao.

I will describe some developments that have taken place in parallel in model theory and additive combinatorics (unbeknownst to either); and some that have not yet found their parallels.

In model theory, the basic language is based on *dimension theories* and notions of *genericity* or randomness. The most classic example: dimension of an algebraic variety, generic points.

Background: approximate orbits

Let G be a group.
Assume $G = < g_1, \ldots, g_n >$, and G acts on a set Ω.
$Y \subset \Omega$, $|g_i Y - Y| < \epsilon |Y|$.
How close is Y to being a G-orbit?
Expanders, amenability, property τ, ... are defined in these terms.
Representation theory version:

$$|g_i v - v| < \epsilon$$

(consider the characteristic function v of Y.)

Example

$[-n, n] \subset \mathbb{Z}$. Almost invariant under ± 1.
But no such approximately fixed sets for $+1, \cdot 2$, or for Cayley graphs of two-generated free group, or $SL_3(\mathbb{Z})$.

Approximate substructures for binary operations

Example

$[-n, n]$ is 99%-closed under ± 1, but only 50%- closed under addition.

Proposition (99 % theory)

Let $X \subseteq G$. Suppose $xy \in X$ for 99.9% of all pairs $(x, y) \in X^2$. Then there exists $H \leq G$ such that almost all $x \in X$ are in H, and vice versa.

Weil, algebraic geometry setting: "99 %" means: away from a lower-dimensional subvariety. Actually Weil assumes no ambient group (local group / group chunk seting.)

Proof.

Let $X' = \{b \in X : bX =_{99\%} X\}$. Then $|X'| \geq .9|X|$.
Gap: if $aX =_{80\%} X$ then $aX =_{98\%} X$: Take $b \in X' \cap a^{-1}X'$. So $a, ab \in X'$. Then $aX =_{99\%} a(bX) = (ab)X =_{99\%} X$.
Let $H = \{a \in G : aX =_{90\%} X\} = \{a \in G : aX =_{80\%} X\}$ $\square$

Best bounds by Ben-or, Coppersmith, Luby, Rubinfeld.

1 % theory

A cube $X = \Pi_i [0, m_i] \subset \mathbb{Z}^n$ satisfies: $|X + X| \le 2^n |X|$. So does any homomorphic image of X, or of a translate.

Theorem (Freiman 1959)

Let $X \subset \mathbb{Z}$ and suppose $|X + X| \le k|X|$. Then X forms k'% of a generalized arithmetic progression.

Similar examples in *nilpotent groups*; classification by Green-Rusza, Fisher, Breuillard, Tao.
Compare: simplicity.

Groups of polynomial growth

Theorem (Gromov 81)

Let G be a group generated by a finite subset $X = X^{-1}$. Assume $|X^n| \leq Cn^k$. Then G is nilpotent-by-finite.

Note e.g. if $|X^n| = Cn^k$, then X^{2^n} is a 2^k- approximate subgroup.

Gromov's proof:

- "Looking at G from afar", Gromov sees a locally compact space. Montgomery-Zippin is used, in the main case, to find a homomorphism to a linear group, essentialy to the automorphism group of this space. This is the heart of the proof.
- The image of G in a *linear* group must be solvable-by-finite (Tits' alternative.)
- The solvable case, conjectured by Bass-Serre, was proved by Milnor-Wolf.
- Gromov thus finds a homomorphism of a finite index subgroup to $\mathbb{Z}$; shows the kernel has polynomial growth of lower order. Induction shows G is virtually solvable.

Sum-product phenomenon

Theorem (Erdös - Szemerédi 1983)

Let X be a finite subset of $\mathbb{R}$. Then $|X + XX| \geq C|X|^{1+\epsilon}$.

Conjecture: $|X|^{2-\epsilon}$.

Theorem (Edgar-Miller 2003)

Let R be a Borel subring of $\mathbb{R}$. Then R has Hausdorff dimension 0 or $R = \mathbb{R}$.

Theorem (Bourgain-Katz-Tao 2004)

$|X + XX| \geq C|X|^{1+\epsilon}$ *for finite fields. ($|X|$ not too large.)*

This can be viewed as giving the structure of approximate subgroups of $G_m \ltimes G_a$ (upper triangular part of $SL_2(\mathbb{C})$.)
Applications to expanders, sieves, concentrators, ... Bourgain, Gamburd, Sarnak, ...: see talks by Avi Wigderson, Ben Green.

Approximate subgroups of non-commutative groups

G a group. X denotes a subset, with $1 \in X = X^{-1}$.
Two subsets X, Y of G are *(k)-commensurable* if each is contained in the union of finitely many (k-) left cosets of the other.
X is a k- *approximate subgroup* if $1 \in X = X^{-1}X$, and XX is k-commensurable with X.
Tao: If $|XX| \leq k_1|X|$, then X is contained in a finite union of cosets of a k_2- approximate group X', with $|X'/X| \leq k_3$; k_2, k_3 are polynomially bounded in terms of k.

Problem (Bourgain, Tao, E. Lindenstrauss, Breuillard)

Describe the structure of approximate subgroups. Modulo nilpotent groups, are they close to actual subgroups?

Analogs

Theorem (Zilber)

T a theory with finite Morley dimension. G a group. X a definable subset, such that $\dim(XX) = \dim(X)$ and multiplicity $= 1$. Then there exists a definable subgroup H, such that $\dim(X \triangle Ha) < \dim(X) = \dim(H)$.

Pseudo-finite interpretation: $|X \triangle Ha|/|X| \to 0$.

Theorem

Finite S1 dimension. G a group. X a definable subset, such that $\dim(XX) = \dim(X)$. Then there exists a definable subgroup H, $a \in G$, $\dim(X \cap Ha) = \dim(H) = \dim(C)$.

Pseudo-finite interpretation: $|X \cap C| \geq c|X|$, $c > 0$.
Similar results for rings.

Aside: Strong approximation

Corollary (Matthews, Vaserstein, Weisfeiler 1984; Nori 1987,Gabber 1988)

Let Γ be a finite subgroup of $GL_n(\mathbb{F}_p)$, generated by unipotents. Then Γ is k- commensurable with $G(\mathbb{F}_p)$, G an algebraic group; k a constant independent of p.

Idea of proof: pass to pseudo-finite fields; S1 dimension theory; take a product $X = X_1 ... X_l$ of copies of $(\mathbb{F}_p, +)$ in $GL_n(\mathbb{F}_p)$, so that $\dim(XX) = \dim(X)$; obtain H.
For simple G, one unipotent in Γ suffices; and is provided by Jordan's theorem.
The case of $GL_n(\mathbb{F}_{p^m})$: Larsen-Pink.

Linear groups

Let $\underline{G}$ be a simple algebraic group, e.g. $\underline{G} = SL_n$.

Theorem

Let F be a finite field and let $G = \underline{G}(F)$. Suppose that $X \subseteq G$ is a k-approximate subgroup that generates G. Then X is bounded, or $|G|/|X|$ is bounded.

Theorem (Breuillard-Green-Tao 2010)

Moreover the bound has the form k^C, with C independent of F, X.

Similar results by Pyber-Szabo. Earlier: Helfgott , SL_2, SL_3.

Corollary

Let $k \in \mathbb{N}$, and let L be a linear group, or a connected Lie group. If X is a k-approximate subgroup of L, then there exist a solvable subgroup S of L such that X is contained in $\leq k' = k'(k, L)$ cosets of S.

Approximate subgroups of solvable groups were further reduced to nilpotent gruops in case G is *strongly torsion-free* (Tao) or solvable groups or linear over $\mathbb{C}$ (Breuillard-Green).

Groups with large approximate subgroups

Theorem

Let G_0 be a finitely generated group, $k \in \mathbb{N}$. Assume G_0 has a cofinal family of k-approximate subgroups (i.e. any finite $F_0 \subset G_0$ is contained in one.) Then G_0 is nilpotent-by-finite.

The strategy of proof is closely patterned after Gromov's. But: (i) a different connection to Lie groups; using measure theory and not a metric. (ii) induction on Lie dimension, in place of the order of polynomial growth. Main point: a canonical connection between approximateness and Lie groups, visible in the model-theoretic boundary.

A (rough and partial) dictionary

structure A	sequence A_n of finite structures
definable subset / subgroup	subset / subgroup
finite	bounded
nonforking	positive measure
dimension α	size $\sim n^{\alpha}$
stability	99% world
independent amalgamation	triangle removal
dimension theorem	
	relative triangle removal
stabilizer	Balog-Szemerédi-Tao-Sanders$\cdots$
$\bigwedge$-definable subgroup with	approximate subgroup
locally compact quotient	*
compact Lascar group	compact groups in Furstenberg analysis
boundedly closed base	relative weak mixing
domination	
internality, liaison groups	
modularity	
trichotomy	

Model theoretic topology

Let $\mathcal{A}$ be the class of all (G, X, μ, δ) with: G a group, X a finite, k-approximate subgroup, $\mu(Y) = |Y|/|X|$,
$\delta(Y) = |\log(Y)|/|\log(X)|$
A *basic open set* is the collection of all pairs (G, X) described by some condition (sentence) formulated using starting from the basic data $G, X, \cdot$, using Boolean operators $\wedge, \neg$, and quantifiers. Along with $(\exists x)$, we allow cardinality comparison quantifiers.

Example

- G is (not) 2-nilpotent",
- "for at least 90% of all elements $a \in G$, the centralizer $T = C_G(a)$ satisfies $|N(T)/T| \leq 2$
- $|T^4| \geq |G|$
- XX is contained in $\leq k$ cosets of X.

Model theoretic compactification

Let $\bar{\mathcal{A}}$ be the closure of $\mathcal{A}$ in the class of all structures (G, X, μ, δ). These are structures $(G, X, \cdot, \mu, \delta)$ with $(G, \cdot)$ a group, X a subset, in fact a k-approximate subgroup.
μ extends to a countably additive measure with $0 < \mu(X) < \infty$. X is no longer finite, but $\mu(XXX) \leq k'\mu(X)$. We will say that X is a *near-subgroup*. δ a real-valued *dimension*; to be discussed later.
$\bar{\mathcal{A}}$ is *compact* in the topology described above.
The elements of $\bar{\mathcal{A}}$ can be taken to be *ultraproducts* of elements of $\mathcal{A}$ along an ultrafilter u. One can (maximall) take a *definable subset* of $\Pi_{i \to u} A_i^n$ to be one of the form $\Pi_{i \to u} S_i$, $S_i \subset A_i^n$.

Approximateness subgroups and Lie groups.

Example

L be a connected (non-compact) Lie group, X a compact neighborhood of 1. Then the Haar measure μ measures $G =< X >$, but X is not commensurable to a subgroup.

Theorem

Let $(G, X, \mu, \delta) \in \bar{\mathcal{A}}$*.*

1. *There exists a homomorphism* h *from a subgroup of* G *to* L *a connected, finite-dimensional Lie group* L*.*
2. *If* $K \subset U \subset L$*,* K *compact,* U *open, then there exists a definable* D*, commensurable with* X*, with* $h^{-1}(K) \subset D \subset h^{-1}(U)$*.*
3. *We can take* L *to have no compact normal subgroups; in this case* L *is uniquely determined;* $\dim(L)$ *is called the Lie dimension of* X*.*

Example

If the Lie dimension is 0, L compact, then taking $K = U = L$ we find a definable subgroup of G, commensurable with X.

Construction of a locally compact group H:

Lemma (Stabilizer / Balog-Szemeredi-Tao-Sanders)

$X[n]$ can be defined for $n \in \mathbb{Z}$, so that $X(0) = X^{-1}X$ and $X[n]X[n] \subseteq X[n+1]$, and $0 < \mu(X[n]) < \infty$.

Construction

of quotient. $H = \lim_{n\to\infty} \lim_{-\infty\leftarrow m} X[n]/X[m]$

Where:

$$\varprojlim X/X[m] = \{(a_1, a_2, \dots) : a_m a_{m'}^{-1} \in X[-(m+2)],\ m = 1, 2, \dots\}/\sim$$

$a \sim b$ iff for all m, $a_m b_m^{-1} \in X[-m]$.

By Yamabe (1953), any locally compact group H has an open subgroup H' and a normal compact subgroup C such that H'/C is a Lie group.

Quasi-finite dimension: properties of δ

$\delta(Y) \in \mathbb{R}^{\geq 0}_{\infty}$ for nonempty definable Y. If $\Gamma = \cap Y_n$, $Y_1 \supset Y_2 \supset \ldots$, let $\delta(\Gamma) = \inf \delta(Y_n)$.

- $\delta(\{y\}) = 0$.
- $\delta(Y \cup Y') = \max(\delta(Y), \delta(Y'))$
- $\delta(Y \times Y') = \delta(Y) + \delta(Y')$
- More generally, if f is a definable function on Y,

  $$\delta(Y) = \inf\{\alpha + \beta : \alpha \in \mathbb{R}_{\infty}, \beta = \dim\{z : \delta(f^{-1}(z)) \geq \alpha\}$$

  This holds for $Y \to Y/E$ even for an $\bigwedge$-definable equivalence relation T.
- Write $Y_a = f^{-1}(a)$. Then for any $\alpha < \beta \in \mathbb{R}$, $\{a : \delta(Y_a) \leq \alpha\} \subset D \subset \{a : \delta(Y_a) < \beta\}$ for some definable a.

The Larsen-Pink inequality

Proposition

Assume Γ *is a Zariski dense subgroup of* G*,* G *a simple algebraic group. Let* V *be a subvariety of* G*.* $\delta(V \cap \Gamma) \leq \frac{\dim(V)}{\dim(G)}\delta(\Gamma)$*.*

Proof.

(sketch for $\dim(V) = 1$, $\dim(G) = 2$.) We may assume V is irreducible. Define $f : (V \cap \Gamma)^2 \to G$, $f(y_1, h_2) = y_1 y_2^{-1}$. For $c \notin Stab(V)$, $f^{-1}(c)$ is finite. Hence
$\delta(\Gamma) \geq \delta(f(\Gamma \cap Y)^2) \geq 2\delta(Y)$. $\square$

Corollary

Let $a \in \Gamma$*,* $H = C_G(a)$*. Then* $\delta(\Gamma \cap H) = \frac{\dim(Y)}{\dim(G)}\delta(\Gamma)$*.*

This is obtained using the map $ad_a(x) = x^{-1}ax$; we have
$\delta(a^G) = \delta(G) - \delta(H)$.

Proof of BGT

- $X[0] = X, X[n+1] = XX[n]$ $(n \in \mathbb{N}.)$
- to show: for any $0 < \epsilon < \epsilon'$, for some m, for all $X \subseteq G$ generating G, $|X[m]| \geq |X|^{1+\epsilon}$ (unless $|X|^{1+\epsilon'} > |G|$.)
- Suppose not. Then by compactness, can find $X_n (n \in \mathbb{Z})$ with $X_n X_n \subset X_{n+1}$ and $1 \leq \delta(X_n) \leq 1 + \epsilon < 1 + \epsilon' \leq \delta(G)$ for all n; and X_n contained in no definable subgroup of G.
- Let $\Gamma = \cap_n X_n$. This is a Zariski dense subgroup of G, $0 < \delta(\Gamma) < \infty$. Renormalize so that $\delta(\Gamma) = \dim(G)$.
- Let R be the set of regular semisimple elements of G. Note: $\dim(G \setminus R) < \dim(G)$, so $\delta(\Gamma \setminus R) < \delta(\Gamma)$.
- Let $\Upsilon = \{C_G(a) : a \in R \cap \Gamma\}$. Clearly, Υ is Γ-conjugation invariant. We will show Υ is definable, i.e. $\{b : C_G(b) \in \Upsilon\}$ is definable, using a dimension gap:

Proof of BGT

- Let $T = C_G(b)$, $b \in R$.
- $T = C_G(a), a \in R \cap \Gamma$, then $\delta(\Gamma \cap T) \geq \dim(T)$ by Larsen-Pink.
- If $\delta(T \cap X) > \dim(T) - 1$, then as $\delta((T \cap X)/(T \cap \Gamma)) \leq \delta(X/\Gamma) \leq \delta(X) - \delta(\Gamma) = 0$ we have:
- $\delta(T \cap \Gamma) > \dim(T) - 1 \geq \dim(T \setminus R)$ so $T \cap \Gamma \cap R \neq \emptyset$.
- Thus $T \in \Upsilon$ iff $\delta(T \cap X) > \dim(T) - 1$ iff $\delta(T \cap X) \geq \dim(T)$; so Υ is definable.
- Hence the normalizer $N(\Upsilon)$ is a definable group, and it contains Γ. By assumption, $N(\Upsilon) = G$.
- Fix $T \in \Upsilon$. $G/N(T)$ embeds into Υ; so $\delta(G/N(T)) \leq \delta(\Upsilon) = \delta(\Gamma) - \delta(N(T) \cap \Gamma)$. It follows that $\delta(G) = \delta(\Gamma) = \delta(X)$; contradicting the assumption on X.

Quasi-finite structures

L a finite language (e.g. graphs).

Theorem (Zilber, CHL; envelopes)

Let M be an infinite structure with $|M^k|/Aut(M) = f(k) < \infty$. Assume $\dim(Def(M)) \to \mathbb{N}$ (or Ord) is defined, with Morley dimension properties. Then it is possible to interpret in M a finite number of infinite dimensional projective geometries over finite fields, $V_1, \ldots, V_l$. M is a approximated by a family of finite structures $M(d) = M(d_, \ldots, d_l)$, with $\dim V_i(M(d)) = d_i$. For any sentence θ true in M and any $K \in \mathbb{N}$, for large enough d, $M(d) \models \theta$ and $M(d) \in C(L, f|K)$.

Example

$(\mathbb{Z}/4\mathbb{Z})^\infty$.

Quasi-finite structures

$C(L, f)$ = class of finite L-structures A such that $|A^k/Aut(A)| \leq f(k)$. $\bar{C}(L, f)$=first order closure.

Example

Classical geometries over finite fields: vector spaces with unitary/orthogonal/symplectic forms;

Definition

$a \downarrow_C b$ if $\delta(ab/C) = d(a/C) + \delta(b/C)$.

(Agrees with nonforking definition.)

Proposition (CSFG)

Let $M \in \bar{C}(L, f)$.

- *3-amalgamation holds over algebraically closed sets.*
- *Modularity holds: $A \downarrow_{A \cap B} B$ for algebraically closed A, B.*
- *Auxiliary properties: no random bipartite graph; (3 others.)*

Theorem (Cherlin-H.)

- *Assume (1-3) hold. Then M is coordinatized by classical geometries over finite fields.*
- *Theory of envelopes extends to this setting.*
- *Let $f : [1, 4] \to \mathbb{N}$. There exist finitely many $M_1, \ldots, M_\nu \in \bar{C}(L, f)$ with $|M^k|/Aut(M) = f(k)$ ($k \leq 4$) and $|M^k|/Aut(M) < \infty$ in general, whose finite envelopes coincide with $C(L, f)$.*

Corollary

Within $C(L, f)$, isomorphism can be decided in polynomial time. If M is not primitive, an invariant equivalence relation can be found in polynomial time.