Model theory, algebraic dynamics and local fields

Thomas Scanlon

University of California, Berkeley

8 June 2010

Compactness theorem

Theorem

Let T be a set of sentences in some first-order language $\mathscr{L}(\tau)$ and suppose that for each finite subset $T_0 \subseteq T$ that there is some model $\mathfrak{M}_0 \models T_0$, then there is a model $\mathfrak{M} \models T$.

There are several proofs of the compactness theorem; the original being a corollary of Gödel's Completeness Theorem (not the more famous Incompleteness Theorems) while the best known version to non-logicians is obtained as a corollary of Łoś's Theorem on ultraproducts.

Łoś's Theorem on Ultraproduct

Given a collection of $\mathscr{L}(\tau)$ structures $\langle \mathfrak{M}_i \rangle_{i \in I}$ indexed by some nonempty set I, there is a natural product $\prod_{i \in I} \mathfrak{M}_i$ whose underlying universe is the product in the category of sets.

Given a finitely additive $\{0,1\}$-valued measure $\mu : \mathscr{P}(I) \to \{0,1\}$ (or, equivalently, an ultrafilter: $\mathscr{U} := \mu^{-1}\{1\}$), one may define an equivalence relation on the product by

$$(a_i) \sim_{\mathscr{U}} (b_i) \Longleftrightarrow \mu(\{i \in I : a_i = b_i\}) = 1$$

and the quotient of the product by this equivalence relation is naturally an $\mathscr{L}(\tau)$-structure called the ultraproduct $\prod_{/\mathscr{U}} \mathfrak{M}_i$

Theorem (Łoś)

If ϕ is any $\mathscr{L}(\sigma)$-sentence, then

$$\prod_{/\mathscr{U}} \mathfrak{M}_i \models \phi \Longleftrightarrow \{i \in I : \mathfrak{M}_i \models \phi\} \in \mathscr{U}$$

Proof of compactness from Łoś's theorem

- Let I be the set of all finite subset of T.
- For each $T_0 \in I$, let $\mathfrak{M}_{T_0} \models T_0$ be some model of that finite set.
- By a standard Zorn's Lemma argument, one shows that there is a finitely additive $\{0,1\}$-valued measure μ on I such that for each $T_0 \in I$ we have $\mu(\{S \in I : T_0 \subset S\}) = 1$.
- Set $\mathfrak{M} := \prod_\mu \mathfrak{M}_{T_0}$.
- Then if $\phi \in T$, since $\{S \in I : \mathfrak{M}_S \models \phi\} \supseteq \{S \in I : \{\phi\} \subseteq S\}$, we have that $\mu(\{S \in I : \mathfrak{M}_S \models \phi\}) = 1$.
- Hence, by Łoś's Theorem, $\mathfrak{M} \models T$.

Corollary of compactness: Undefinability of finiteness

Theorem

Let $\mathscr{L}(\tau)$ be any first-order language, $\phi(x,y)$ an $\mathscr{L}(\tau)$ formula with free variables x and y and T an $\mathscr{L}(\tau)$ theory. Then either there is a number $N = N(\phi)$ such that for any model $\mathfrak{M} \models T$ and parameter b from M if $\phi(\mathfrak{M}, b)$ is finite, then it has cardinality at most N or $\{b \in M : \phi(\mathfrak{M}, b)$ is finite $\}$ is not definable relative to T.

Proof.

- If such a bound N exists, then the set of parameters b for which $\phi(\mathfrak{N}, b)$ is finite is defined by the formula $(\forall x_1) \cdots (\forall x_{N+1})(\bigvee_{i=1}^{N+1} \neg\phi(x_i, y) \vee \bigvee_{i<j} x_i = x_j)$

□

Proof, continued

Theorem

Let $\mathscr{L}(\tau)$ be any first-order language, $\phi(x, y)$ an $\mathscr{L}(\tau)$ formula with free variables x and y and T an $\mathscr{L}(\tau)$ theory. Then either there is a number $N = N(\phi)$ such that for any model $\mathfrak{M} \models T$ and parameter b from M if $\phi(\mathfrak{M}, b)$ is finite, then it has cardinality at most N or $\{b \in M : \phi(\mathfrak{M}, b) \text{ is finite }\}$ is not definable relative to T.

Proof.

- Suppose no such bound exists but that the formula $\vartheta(y)$ defines the set of parameters for which $\phi(\mathfrak{M}, y)$ is finite as $\mathfrak{M}$ ranges through the models of T.
- The following set of sentences in $\mathscr{L}(\tau')$ where τ' is obtained from τ by adding one new constant symbol c would be finitely satisfiable $T \cup \{\vartheta(c)\} \cup \{(\exists x_1) \cdots (\exists x_n) \bigwedge_{i=1}^{n} \phi(x_i, c) \& \bigwedge_{i<j} x_i \neq x_j$
- By compactness, there is a model $(\mathfrak{M}, c)$ of this set of sentences and we have $\mathfrak{M} \models T$, $\phi(\mathfrak{M}, c)$ is infinite, but $\mathfrak{M} \models \vartheta(c)$.

Soft proofs of boundedness

From the principle that finite definable sets have bounded cardinality, we can sometimes prove the existence of bounds at the cost of proving finiteness in every model.

- The fact that if $f : X \to Y$ is a map of varieties over an algebraically closed field K then there is a number N so that for any point $y \in Y(K)$ either $|f^{-1}\{y\}| \leq N$ or $f^{-1}\{y\}$ is infinite is a reflection of this principle.
- It does not follow from Faltings theorem (as a simple application of compactness) that there is a bound depending just on the genus $g > 1$ for the number of rational points on a curve of genus g. It would follow if one could show that for a nonstandard model of the theory of the rationals that every high genus curve has only finitely many rational points.

Theorem (Ax)

If $f : X \to X$ is a regular self-map on a complex algebraic variety which is injective on $\mathbb{C}$-points, then f is surjective.

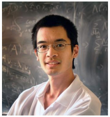
Proof.

- The result is true with $\mathbb{F}_p^{alg}$ in place of $\mathbb{C}$ as $f : X(\mathbb{F}_p^{alg}) \to X(\mathbb{F}_p^{alg})$ may be expressed as a direct limit of injective (and, therefore, surjective) self-maps on finite sets.
- The statement of the theorem is not a first-order sentence in the language of rings, but by restricting the complexity of the defining equations for X and f it may be expressed as a set of sentences.
- It follows by compactness that the theorem is true for some algebraically closed field of characteristic zero and then by completeness of the theory of algebraically closed fields of a fixed characteristic, for all algebraically closed fields.

□

Secret ingredient?

From what I can see of the paper so far, the proofs of the combinatorial statements in Hrushovski's paper proceed by a "correspondence principle" or "compactness and contradiction" method, in which one assumes that the combinatorial statement fails, and extracts from this (via compactness) some infinitary limit structure which is supposed to ultimately lead to some sort of contradiction. Fair enough I've seen many arguments of this sort before, such as in Gromov's proof of his theorem on groups of polynomial growth, or Furstenberg's proof of Szemerédi's theorem. My question though is what is the secret ingredient in the infinitary world that makes this correspondence powerful, and which is then difficult to replicate in the finitary world?



T. Tao, 19 October 2009

Here is a kind of response to Terence Tao's question about the power of the model theoretic methods. As with the other examples he mentions (theory of topological groups, measurable dynamics,...) there is a powerful and nontrivial theory around, namely stability theory, or rather neo-stability theory. This is a specialised area of model theory, which many people in the subject may not be exposed to. Stability theory (developed originally by Shelah) includes notions of forking, stationarity, orthogonality, ... and was originally developed just in the context of stable (first order) theories, for reasons I will not go into here.

...

So my basic point is that there is a theory here, going considerably beyond compactness, which one is plugging into.

A. Pillay, 20 October 2009

Theorem (S., following Hrushovski, Pillay)

Let X be an algebraic variety over a field K and $\Xi \subseteq X(K)$ a set of K-rational points. We say that a subvariety $Y \subseteq X^n$ is ***Ξ-special*** *if $Y = \overline{Y(K) \cap \Xi^n}$. Suppose that the class of Ξ-special varieties is closed under intersection. Then for any algebraic family $Y \subseteq X \times B$ of subvarieties of X there is an associated constructible family $Z \subseteq X \times C$ so that for any $b \in B(K)$ there is some $c \in C(K)$ with $\overline{Y_b(K) \cap \Xi} = Z_c$.*

- In particular, this implies that there is a bound depending just on the family for the cardinality of $Y_b(K) \cap \Xi$ when finite.
- The hypotheses apply directly to the Manin-Mumford and André-Oort conjectures yielding bounds for the complexity of the exceptional groups and Hecke correspondences appearing in the conclusions.
- One may weaken the hypotheses asking only that if $Y, Z \subseteq X^n$ are Ξ special and C is a component of $X \cap Y$ with $C(K) \cap \Xi^n \neq \varnothing$, then C is Ξ special and thereby include the Mordell-Lang conjecture and its dynamical variants.

Ingredients in proof of automatic uniformity

The proof of automatic uniformity is soft, using compactness, but also a large dose of (elementary) stability theory.

The principle in question here goes under the name of Lagrange interpolation in algebraic geometry but more generally is (uniform) definability of types:

Theorem (Shelah)

Suppose that T is a stable theory, $\mathfrak{M} \models T$ is a model of T, and $A \subseteq M^n$ is a subset of some cartesian power of the universe of $\mathfrak{M}$ and $X \subseteq M^n$ is an M-definable set, then there is an A-definable set $Y \subseteq M^n$ for which $X(\mathfrak{M}) \cap A = Y(\mathfrak{M}) \cap A$. Moreover, if X varies in a definable family, then Y may be chosen from a fixed definable family.

The "moreover" clause, namely, the assertion of uniformity, follows from the first part of the theorem via a nontrivial compactness argument.

What is stability theory?

Stability theory arose from Morley's proof of Łoś's Categoricity conjecture (if T is a countable theory having the property that for some uncountable cardinal κ there is exactly one model of T of size κ up to isomorphism, then for every uncountable cardinal λ there is exactly one model of T of size λ).

The central objects of study are types. Indeed, combinatorially, the most natural definition of stability is in terms of numbers of types: a theory T is stable just in case for some cardinal $\kappa \geq |T|$ for any model $\mathfrak{M} \models T$ of cardinality at most κ, there are no more than κ many 1-types over M.

What is a type?

Definition

If $\mathfrak{M}$ is an $\mathscr{L}(\tau)$-structure, $A \subseteq M$ is a subset of the universe of $\mathfrak{M}$, and $b \in M^n$ is a tuple from $\mathfrak{M}$, then the type of b over A is

$$\mathrm{tp}(b/A) := \{\phi(x_1, \ldots, x_n) : \mathfrak{M} \models \phi(b),$$

$$\phi \text{ an } \mathscr{L}(\tau)\text{-formula with parameters from } A\}$$

More generally, an n-type over A is a complete consistent extension of the theory of $\mathfrak{M}$ with parameters from A in the language $\mathscr{L}(\tau)$ augmented by n new constant symbols $x_1, \ldots, x_n$.

By the compactness theorem, if $p(x)$ is a type over A, then there is a model $\mathfrak{N} \succeq \mathfrak{M}$ and a tuple b from N with $p = \mathrm{tp}(b/A)$.

We write $S_n(A)$ for the space of n-types over A. This set carries a natural topology with respect to which it is compact, Hausdorff, and totally disconnected, but the topology may be safely ignored for now.

Given an algebraically closed field K and a subring $k \subseteq K$, there is a natural map

$$\rho : S_n(k) \to \mathbb{A}^n_k = \operatorname{Spec} k[x_1, \ldots, x_n]$$

given by

$$p \mapsto \{Q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] : Q(x) = 0 \in p\}$$

It follows from elementary algebra that ρ is surjective. It follows from Tarski's quantifier elimination theorem that ρ is injective. Moreover, ρ is continuous, but it is not a homeomorphism.

Types relative to the theory of real closed fields

Given a subring $k \subseteq \mathbb{R}$ of the real numbers, again we have a natural map $\rho : S_n(k) \to \mathbb{A}^n_k$ but it is neither injective nor surjective.

For example, if $k = \mathbb{Q}$, then $\mathrm{tp}(\pi/k) \neq \mathrm{tp}(e/k)$ as $(\exists y) x = y^2 + 3 \in \mathrm{tp}(\pi/k) \smallsetminus \mathrm{tp}(e/k)$ but both these types map to the generic point of $\mathbb{A}1_{\mathbb{Q}}$.

Likewise, the point $(x^2 + 1)$ is not in the image of ρ.

A correct spectral description of the type space for real fields requires the notion of the real spectrum.

Definability of types

At one level it does not make sense to speak of types as being definable since they are infinitary objects, but they might reasonably be pro-definable.

Definition

We say that a type $p(x) \in S_n(A)$ (where $A \subseteq M$, $\mathfrak{M}$ is an $\mathscr{L}(\tau)$-structure) is definable if for each formula $\phi(x; y) = \phi(x_1, \ldots, x_n; y_1, \ldots, y_m)$ there is another formula $\psi(y)$, possibly defined with parameters, such that $\{a \in A^m : \phi(x; a) \in p\} = \{a \in A^m : \mathfrak{M} \models \psi(a)\}$

If $p(x) = \mathrm{tp}(b/A)$ then it is easy to get a definition of p using b as a parameter: set $\psi(y) := \phi(b; y)$. This notion is useful only when we can find the definition of the type over a set of parameters which is somehow independent from the realization.

Equivalence of definability of types and stable embeddedness

Proposition

The following are equivalent for a theory T.

- *If $\mathfrak{M} \models T$, $A \subseteq M$ and $p(x) \in S_n(A)$ is a type over A, then p is definable over A.*
- *If $\mathfrak{M} \models T$, $A \subseteq M$, $X \subseteq M^n$ is M-definable, then there is $Y \subseteq M^n$ which is A-definable and satisfies $X(\mathfrak{M}) \cap A = Y(\mathfrak{M}) \cap A$.*

We prove $\Longrightarrow$:

Proof.

- Write $X(\mathfrak{M}) = \phi(b; \mathfrak{M})$ for some tuple b from M.
- As $\mathrm{tp}(b/A)$ is A-definable, there is some $\psi(y)$ defined with parameters from A so that for $a \in A$ we have $\phi(x; a) \in \mathrm{tp}(b/A) \Longleftrightarrow \mathfrak{M} \models \psi(a)$.
- That is, letting ψ define Y, we have $X(\mathfrak{M}) \cap A = Y(\mathfrak{M}) \cap A$.

□

Looking ahead: canonical bases and moduli

The trick of interchanging the rôles of parameter and object variables and more generally of regarding types themselves as definable objects will recur throughout these lectures.

Suppressing some hypotheses, we will associate to a type $p(x)$ its canonical base, $\mathrm{Cb}(p)$, which may be identified with the set of ϕ-definitions of p (as ϕ ranges through the language). The canonical base acts as a generalized moduli point, or more accurately since definable sets are naturally subobjects, as a kind of point in a Hilbert scheme or Douady space.

Our three highlights of the theory of canonical bases are the Chatzidakis/Hrushovski approach to descent in algebraic dynamics, the Pillay/Ziegler jet space theory for difference and differential varieties, and the Hrushovski/Loeser treatment of Berkovich spaces.