FINITE MODEL THEORY (MATH 285D, UCLA, WINTER 2017) LECTURE NOTES IN PROGRESS

ARTEM CHERNIKOV

1. Intro

- Motivated by connections with computational complexity (mostly a part of computer scientice today).
- First-order logic is both too weak and too strong (see below), so expansions of first-order logic are often considered.
- Aim - to study definability on finite structures and connections to infinitary model theory.
- Points of contact exist, e.g: [Cherlin, Harrington, Lachlan], [Hrushovski] Let T be a countable complete totally categorical theory (i.e. T has a unique model of any infinite cardinality, up to isomorphism). Then T is axiomatized by a single sentence + the axiom schema of infinity. In particular, T is pseudofinite (i.e. every sentence in T has a finite model).

2. First-order logic on finite structures

- By default, all structures will be in a finite language. Often - finite relational language.
- We write $\mathcal{M} \equiv \mathcal{N}$ to denote that $\mathcal{M}$ is elementarily equivalent to $\mathcal{N}$.
- For $n \in \mathbb{N}$, $\mathcal{M} \equiv^n \mathcal{N}$ means that $\mathcal{M}$ and $\mathcal{N}$ satisfy the same sentences ϕ of quantifier rank at most n.
- Given a set of $\mathcal{L}$-sentences Φ, we let $\mathrm{Mod}(\Phi) := \{\mathcal{M} : \mathcal{M} \text{ is an } \mathcal{L}\text{-structure and } \mathcal{M} \models \Phi\}$
- and $\mathrm{Mod}_{<\omega}(\Phi)$ the set of all finite models of Φ.
- A property of $\mathcal{L}$-structures is FO-expressible (FO-expressible on finite structures) if the set of $\mathcal{L}$-structures satisfying it is of the form $\mathrm{Mod}(\phi)$ for a sentence ϕ.

Proposition 2.1. *For every finite $\mathcal{A}$ there is a first-order sentence $\theta_{\mathcal{A}}$ so that $\mathcal{B} \models \theta_{\mathcal{A}} \iff \mathcal{B} \cong \mathcal{A}$.*

Proof. Let $\mathcal{A} = \{a_1, \ldots, a_n\}$. Let $\psi(x_1, \ldots, x_n)$ be the conjunction of all:

- $\phi(x_1, \ldots, x_n)$, where ϕ is atomic and $\mathcal{A} \models \phi(a_1, \ldots, a_n)$,
- $\neg\phi(x_1, \ldots, x_n)$, where ϕ is atomic and $\mathcal{A} \not\models \phi(a_1, \ldots, a_n)$,
- $\forall x (x = x_1 \vee \ldots \vee x = x_n)$.

Let $\theta_{\mathcal{A}}$ be the sentence $\exists x_1 \ldots \exists x_n \psi(x_1, \ldots, x_n)$. Clearly $\mathcal{A} \models \theta_{\mathcal{A}}$. If $\mathcal{B} \models \theta_{\mathcal{A}}$, and $\mathcal{B} \models \psi(b_1, \ldots, b_n)$, then $b_i \mapsto a_i$ is an isomorphism $\mathcal{B} \cong \mathcal{A}$. ☐

- Notice that $\theta_{\mathcal{A}}$ is at least as long as the size of the domain of $\mathcal{A}$. What is the shortest possible length of such a sentence?

Exercise 2.2. Show that for general structures, up to a constant this is the best possible (e.g. one can use a Kolmogorov comlexity argument).

- For certain classes of structures, one can do much better:
- [Nies, Tent] Simple groups are $O(\log|\mathcal{A}|)$-describable, and arbitrary groups are $O\left(\log^3|\mathcal{A}|\right)$-describable ($\log = \log_2$).
- [Felgner] The class of finite non-abelian simple groups is defined by a single sentence.
- [Aschenbrenner, Khélif, Naziazeno, and Scanlon] assume that an $\mathcal{L}$-structure $\mathcal{A}$ is bi-interpretable with $(\mathbb{N}, +, \times)$. Then thre is some $\mathcal{L}$-sentence σ such that $\mathcal{A} \models \sigma$ and every finitely generated $\mathcal{L}$-structure satisfying σ is isomorphic to $\mathcal{A}$. Then it follows that every finitely generated commutative ring satisfies this as well.
- Pop's conjecture (open): let $\mathcal{K}$ and $\mathcal{L}$ be finitely generated fields with $\mathcal{K} \equiv \mathcal{L}$. Then $\mathcal{K} \cong \mathcal{L}$. (every field finitely generated as a ring is finite)
- Hence, questions of definability in first-order logic are much more meaningful when one talks about classes of finite structures rather that an individual finite structure.

3. Failure of metatheorems of first-order logic "in the finite"

Example 3.1. Compactness fails. Consider $\{\phi_n : n \in \omega\}$, where $\phi_n = \exists x_1 \ldots \exists x_n (x_1 \neq \ldots \neq x_n)$. Then every finite subset has a finite model, but not the whole set.

- Almost all "preservation" theorems fail in the finite.
- [Los, Tarski] A first-order sentence ϕ defines a class that is closed under substructures $\iff$ ϕ is equivalent to a universal sentence. Equivalently, ϕ defines a class that is closed under extensions $\iff$ ϕ is equivalent to an existential sentence

Example 3.2. [Tait, example by Gurevich] There is a sentence ϕ such that $\mathrm{Mod}_{<\omega}(\phi)$ is closed under extensions and ϕ is not equivalent over finite structures to any existential sentence.

Let ϕ be $\alpha \to \beta$ where

- α is a universal sentence saying:
  - $<$ is a linear order,
  - min is the minimal element, max is the maximal element,
  - $S(x, y) \to y$ is the successor of x
- β says:
  $\forall x < \max \exists y (S(x, y))$.

ϕ is preserved by extensions: suppose $\mathcal{A}$ is a substructure of $\mathcal{B}$, $\mathcal{A} \models \phi$ and $\mathcal{B} \models \alpha$. Then $A = B$.

As α is universal, $\mathcal{A} \models \alpha$. Hence $\mathcal{A} \models \beta$. It suffices to prove that if b is the successor of $a \in A$ with respect to $<$ on B, then $b \in A$. Since $\mathcal{A} \models \beta$, there exists $c \in A$ such that $\mathcal{A} \models S(a, c)$. Then $\mathcal{B} \models S(a, c)$. Since $\mathcal{B} \models \alpha$, $b = c \in \mathcal{A}$.

By contradiction, suppose ϕ is equivalent to an existential sentence $\psi = \exists x_1 \ldots \exists x_k \Psi(x_1, \ldots, x_k)$, where Ψ is quantifier-free. The interval $[1, k+3]$ of integers with the successor relation gives a model $\mathcal{A}$ for ϕ. Fix witnesses $a_1, \ldots, a_k$ realizing Ψ, let b be a non-initial non-final element different from all a_i and discard the edge $(b, b+1)$ of $\mathcal{A}$. The resulting structure satisfies ψ but fails to satisfy ϕ.

- Recall Ehrefeucht-Fraïssé games:

Fact 3.3. $\mathcal{A} \equiv_n \mathcal{B} \iff$ *Duplicator has a winning strategy in* $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$.

Exercise 3.4. Let $\mathcal{A}, \mathcal{B}$ be finite linear orders. Then $|A|, |B| \geq 2^n \implies \mathcal{A} \equiv_n \mathcal{B}$ for all $n \in \mathbb{N}$.

Corollary 3.5. *The class of all linear orders of finite size is not definable by a first-order sentence.*

Proof. Assume definable by a sentence of quantifier rank at most n. Let $\mathcal{A}_n$ be of size 2^n and let $\mathcal{B}_n$ be of size $2^n + 1$. Then $\mathcal{A}_n \equiv_n \mathcal{B}_n$, a contradiction. □

Example 3.6. Failure of Beth definability theorem [Hajek].

Claim 1. Let $\mathcal{L} = \{<\}$. There is no $\mathcal{L}$-formula $\theta(x)$ so that for every finite linear order $\mathcal{A}$ we have $\mathcal{A} \models \theta(a) \iff a$ is an even element.

Indeed, otherwise $\exists x (\theta(x) \land \forall y (y = x \lor y < x))$ would contradict the corollary.

Claim 2. *There is an $\mathcal{L}$-sentence ϕ which defines a unary predicate P implicitly but not explicitly.*

Consider ϕ the conjunction of

- "$<$ is a linear order",
- $\exists x (P(x) \land \forall y (y = x \lor x < y))$,
- $\forall x \forall y ($"y a successor of x"$\rightarrow (P(y) \leftrightarrow \neg P(x)))$.

Every finite linear order has a unique P satisfying ϕ. However, if $\phi \vdash P(x) \leftrightarrow \theta(x)$ with $\theta(x)$ is an $\{<\}$-sentence, then $\theta(x)$ contradicts Claim 1.

Example 3.7. Craig interpolation theorem fails.

Let $\mathcal{L} = \{<, c\}$. There are an $\mathcal{L} \cup \{P\}$-sentence ϕ_1 and an $\mathcal{L} \cup \{Q\}$-sentence ϕ_2 so that $\phi_1 \vdash \phi_2$ but no $\mathcal{L}$-sentence θ satisfies both $\phi_1 \vdash \theta$ and $\theta \vdash \phi_2$.

Indeed, let ϕ be as in the previous example. Let ϕ' be obtained from ϕ by replacing P by Q.

Let ϕ_1 be $\phi \land P(c)$ and let ϕ_2 be $\phi' \rightarrow Q(c)$. Now $\phi_1 \vdash \phi_2$.

Suppose $\phi_1 \vdash \theta$ and $\theta \vdash \phi_2$, where θ is an $\mathcal{L}$-sentence. Then $\phi \vdash P(x) \leftrightarrow \theta$, hence ϕ defines P explicitly — contrary to the previous example.

- Remarkably (with a rather involved combinatorial argument as opposed to the use of compactness in the classical case):

Theorem 3.8. *[Rossman] A first-order sentence is preserved under homomorphisms on all finite structures if and only if it is equivalent on finite structures to an existential-positive sentence (i.e. a sentence built up from atomic formulas by disjunction, conjunction and $\exists$).*

4. First-order spectra

- Which properties are first-order definable or non-definable?

Definition 4.1. For a sentence ϕ, we let $\mathrm{Spec}(\phi) := \{n \in \mathbb{N} : \exists \mathcal{A} \models \phi, |A| = n\}$.

A set $S \subseteq \mathbb{N}$ is a spectrum if $S = \mathrm{Spec}(\phi)$ for some sentence ϕ in some language.

Problem 4.2. (Scholz) Which sets of natural numbers are spectra? (Asser) Is the complement of a spectrum a spectrum?

Example 4.3.

1. Powers of 2 form a spectrum.
   They are the cardinalities of finite Boolean algebras, being a Boolean algebra is definable by a single sentence (Exercise).
2. Powers of primes form a spectrum
   They are the cardinalities of finite fields.

(3) (Exercise) Show that the set of primes is a spectrum. (we will see later that there is no formula $\psi(y)$ in the ring language which defines in each finite field $\mathbb{F}_{p^2}$ the subfield $\mathbb{F}_p$)
(4) (Exercise) For any $a, b \in \mathbb{N}$, show that $a + b\mathbb{N}$ is a spectrum (use one unary function symbol).
(5) (Exercise) Let S_1, S_2 be spectra. Then $S_1 \cup S_2, S_1 \cap S_2, S_1 + S_2 = \{m + n : m \in S_1, n \in S_2\}$, $S_1 \cdot S_2 = \{m \cdot n : m \in S_1, n \in S_2\}$ are also spectra.

- We will see that Scholz and Asser's problems translate into open problems in computational complexity.

4.1. **Trakhtenbrot's theorem.**

Theorem 4.4. *[Trakhtenbrot, 1950] The set of first-order sentences valid on all finite structures is not recursively enumerable.*

- A Turing machine M consists of a *tape*, a finite set of *states* and a finite set of *instructions*.
- The tape consists of numbered *cells* $1, 2, 3, \ldots$.
- Each cell contains 0 or 1.
- States are denoted by $q_1, \ldots, q_n$ (q_1 is the *initial state*).
- Instructions are quadruples of one of the following kinds:
  - $q\alpha\beta q'$, meaning: if in state q reading α, then write β and go to state q'.
  - $q\alpha R q'$, meaning: if in state q reading α, then move right and go to state q'.
  - $q\alpha L q'$, meaning: if in state q reading α, then move left and go to state q'.
- A *configuration* is a sequence $\alpha_1\alpha_2 \ldots \alpha_{i-1} q \alpha_i \ldots \alpha_n$, meaning that the machine is in state q reading α_i in cell i.
- The sequence $q_1\alpha_1\alpha_2 \ldots \alpha_n$ is called the *initial configuration* with *input* $\alpha_1 \ldots \alpha_n$.
- A *computation* is a sequence $I_1, \ldots, I_n$ of configurations so that I_1 is an initial configuration and I_{i+1} is obtained from I_i by the application of an instruction.
- Computation *halts* if no instruction applies to the last configuration.
- M is *deterministic* if for all q and α there is at most one instruction starting with $q\alpha$.
- Otherwise M is *non-deterministic*.

Proof. We reduce the *Halting Problem* to the problem of deciding whether a FO-sentence has a finite model.

Let $\mathcal{L}_0 := \{B_0, B_1, C, S, 1, N, \prec\}$.

We think of $\mathcal{L}_0$-structures in the following terms:

- universe of the model is "time",
- $S^{(i)}(1)$ means q_i,
- $B_\alpha(x, t)$ means that cell x contains symbol α at time t,
- $C(t, q, x)$ means that at time t the machine is in the state q reading cell x.

Suppose a machine M is given. We can construct an $\mathcal{L}_0$-sentence ϕ_M so that M halts $\iff$ ϕ_M has a finite model (see e.g. [1, p.12-14]).

Now let $\mathrm{Val} := \{\#(\phi) : \phi \text{ is true on all finite } \mathcal{L}_0\text{-structures}\}$ and $\mathrm{Sat} := \{\#(\phi) : \phi \text{ has a finite model}\}$, where $\#(\phi)$ is the Gödel number of ϕ. We have proved that M halts $\iff$ $\#(\phi_M) \in \mathrm{Sat}$. Since the Halting Problem is undecidable, so is Sat. Since Sat is trivially recursively enumerable, its complement Val cannot be recursively enumerable. □

Corollary 4.5.

(1) *There is no effective axiomatic system S so that ϕ valid on finite structures $\iff$ ϕ provable in S. This means the total failure of the completeness theorem.*
(2) *There is no recursive function f so that if a FO-sentence ϕ has a finite model, then it has a model of size $\leq f(\phi)$ (failure of finitary downward Löwenheim-Skolem).*

References

[1] Jouko Väänänen. A short course on finite model theory. *http://mathstat.helsinki.fi/logic/people/jouko.vaananen/shortcourse.pdf*, *volume=1994, year=1993.*