Math 225A – Model Theory

Speirs, Martin

Autumn 2013

General Information

These notes are based on a course in *Metamathematics* taught by Professor Thomas Scanlon at UC Berkeley in the Autumn of 2013. The course will focus on Model Theory and the course book is Hodges' *a shorter model theory*.

As with any such notes, these may contain errors and typos. I take full responsibility for such occurences. If you find any errors or typos (no matter how trivial!) please let me know at mps@berkeley.edu.

Lecture 12

Quantifier elimination for $\mathrm{Th}(\mathbb{Z})$ as ordered group

Let $\tau = \{+, -, 0, 1, <\}$ where $+$ and $-$ are binary function symbols, 0 and 1 are constants and $<$ is a binary relation. We will consider the theory of the integers as a discretely ordered group. We claim the the theory, T, need to describe this will be the theory of discretely ordered abelian groups G having $G/nG \cong \mathbb{Z}/n\mathbb{Z}$ for each $n \in \mathbb{Z}$. More precisely we let T be the theory with axioms

- ordered abelian groups axioms as usual
- discretely orderede: $\forall x \neg(0 < x < 1)$
- $0 < 1$
- for each $n \in \mathbb{Z}$
$$\forall x \bigvee_{j=0}^{n-1} \exists y (x = j + ny)$$
where j is short for $1 + 1 + \cdots + 1$ (j times) and ny is short for $y + y + \cdots + y$ (n times).

The last axioms schema does show that $G/nG \cong \mathbb{Z}/n\mathbb{Z}$ for all n whenever $G \models T$, since then G is *discretely* ordered and so G/nG is generated by 1.

Definition. We define the **complexity**, $c(t)$ of a τ-term t to by essentially the number of additions in t. More precisely let

- $c(0) = c(1) = 1$
- $c(x_i) = 1$
- $c(-t) = c(t)$
- $c(t + s) = c(t) + c(s)$.

Now we define the elimination set.

Definition. Let $\Xi_{n,k}$ be the set of formulae in n variables $x_0, \ldots, x_{n-1}$ of the form

- $t(\bar{x}) > 0$ where $c(t) \leq k$
- $s(\bar{x}) \equiv j \pmod{k!}$ where $c(s) \leq k$.

Theorem 1 (Presburger). *T is equal to* $\mathrm{Th}(\mathbb{Z}, +, -, 0, 1, <)$ *and* $\Xi = \bigcup \Xi_{n,k}$ *is an elimination set.*

In particular T is a *complete* theory. The proof of the theorem will actually yield an effective procedure to convert a general formula to an equivalent formula in Ξ, i.e. we will get decidability for the theory.

Remark. In fact the decidability result for T follows (by Göde's Completeness theorem) from the first statement $T = \mathrm{Th}(\mathbb{Z}, +, -, 0, 1, <)$ since $\mathrm{Th}(\mathbb{Z}, +, -, 0, 1, <)$ is complete.

The general approach of the proof will be the following: Show that equivalence relative to Ξ can be used to set up a back-and-forth system. This we know is enough to determine elementary equivalence, which gives the first statement. We also know that every formula is equivalent to a disjunction of formulas from the set $\Theta = \bigcup \Theta_{n,k}$ (constructed in Lecture 10), so if we can show that the "equivalence relation gotten from Ξ" is *finer* than that gotten from Θ then every element of Θ can be expressed as a disjunction of elements of Ξ. Since Θ was enough for an elimination set we see that Ξ will be enough for an elimination set.

Let us first define the "equivalence relation gotten from Ξ".

Definition. For $\mathfrak{A}$ and $\mathfrak{B}$ models of T and for $\bar{a} \in A^n$ and $\bar{b} \in B^n$, we say that

$$(\mathfrak{A}, \bar{a}) \sim_k^{\Xi} (\mathfrak{B}, \bar{b})$$

iff for all $\xi \in \Xi_{n,k}$ we have $\mathfrak{A} \models \xi(\bar{a}) \iff \mathfrak{B} \models \xi(\bar{b})$.

Now our goal is to show that there is a sequence of numbers $(k_i)_{i=0}^{\infty}$ such that $k_0 < k_1 < \cdots$ and such that we can carry out the back-and-forth construction if we know that we have the $\sim_k^{\Xi}$ for all k. More precisely we want

- if $(\mathfrak{A}, \bar{a}) \sim_0^{\Xi} (\mathfrak{B}, \bar{b})$ then $(\mathfrak{A}, \bar{a}) \approx_0 (\mathfrak{B}, \bar{b})$, and
- if $(\mathfrak{A}, \bar{a}) \sim_{k_{i+1}}^{\Xi} (\mathfrak{B}, \bar{b})$ and if $c \in A$ then there exists $d \in B$ such that $(\mathfrak{A}, \bar{a}, c) \sim_{k_i}^{\Xi} (\mathfrak{B}, \bar{b}, d)$. Vice verse: if $d \in B$ then there exists $c \in A$ such that $(\mathfrak{A}, \bar{a}, c) \sim_{k_i}^{\Xi} (\mathfrak{B}, \bar{b}, d)$.

The existence of such a sequence (k_i) will then imply that $\sim_k^{\Xi}$ is finer than $\approx_i$ which is what we want.

We need two technical lemmas. The first will show that k_0 may be chosen to be 3.

Lemma. *If* $(\mathfrak{A}, \bar{a}) \sim_3^{\Xi} (\mathfrak{B}, \bar{b})$ *then* $(\mathfrak{A}, \bar{a}) \approx_0 (\mathfrak{B}, \bar{b})$.

Proof. We must check that all unnested atomic formulae: $x_j < x_i$, $x_k = x_i + x_j$, $x_i = 0$, $x_j = 1$ and $x_i = x_j$. As an example we check $\mathfrak{A} \models a_k = a_i + a_j \iff \mathfrak{B} \models b_k = b_i + b_j$. Using the axioms of ordered abelian groups

$$a_k{=}a_i{+}a_j \iff a_k{-}(a_i{+}a_j){=}0 \iff \neg(a_k{-}(a_i{+}a_j){>}0) \wedge \neg((a_i{+}a_j){-}a_k){>}0).$$

Let $t(\bar{x}) := x_k + -(x_i + x_j)$ and $u(\bar{x}) := -t(\bar{x})$ be terms. Both have complexity 3. By hypothesis $\neg(t(\bar{x}) > 0)$ and so by definition of $\sim_3^{\Xi}$ we have $(\mathfrak{B}, \bar{b}) \models \neg(t(\bar{x}) > 0)$, and likewise $(\mathfrak{B}, \bar{b}) \models \neg(u(\bar{x}) > 0)$ so $t(\bar{b}) = 0$ i.e. $b_k = b_i + b_j$.

A similar argument works for the four other unnested atomic formulae and so $(\mathfrak{A}, \bar{a}) \approx_0 (\mathfrak{B}, \bar{b})$. $\square$

So $k_0 = 3$. Now to go up a step is a bit more complicated. We shall let $k_m = m^{2m}$. This suffices by the following lemma.

Lemma. *If* $(\mathfrak{A}, \bar{b}) \sim_{m^{2m}}^{\Xi} (\mathfrak{B}, \bar{b})$ *($m \geq 3$) and* $c \in A$ *then there exists* $d \in B$ *such that* $(\mathfrak{A}, \bar{a}, c) \sim_m^{\Xi} (\mathfrak{B}, \bar{b}, d)$. *Similarly if* $d \in B$ *then there exists* $c \in A$ *such that* $(\mathfrak{A}, \bar{a}, c) \sim_m^{\Xi} (\mathfrak{B}, \bar{b}, d)$.

Proof. We will deal with congruence issues and then with the order issues.

Let $c \in A$. We want to understand the congruence relations that c might have relative to terms when we plug in $\bar{a}$. We only consider terms of complexity $m - 1$. Consider the set

$$\begin{aligned} \Gamma := \quad & \{t(\bar{x}) + ix_n \equiv j \pmod{m!} \mid \\ & c(t) \leq m-1,\ i \leq m,\ 0 \leq j \leq m! \text{ and } \mathfrak{A} \models t(\bar{a}) + ic \equiv j \pmod{m!}\} \end{aligned}$$

As $(\mathfrak{A}, \bar{a}) \sim_{m^{2m}}^{\Xi} (\mathfrak{B}, \bar{b})$, for each t of complexity $\leq m - 1$ we have $t(\bar{a}) \equiv t(\bar{b}) \pmod{m!}$. This statement makes sense since $\mathfrak{A}/ \pmod{m!}\mathfrak{A} \cong \mathbb{Z}/m!\mathbb{Z}$ and $\mathbb{Z}/m!\mathbb{Z} \cong \mathfrak{B}/m!\mathfrak{B}$ so we can identify elements of $\mathfrak{A}$ and $\mathfrak{B}$ with their image under the isomorphisms. Let $\alpha : \mathfrak{A}/m!\mathfrak{A} \longrightarrow \mathbb{Z}/m!\mathbb{Z}$ and $\beta : \mathfrak{B}/m!\mathfrak{B} \longrightarrow \mathbb{Z}/m!\mathbb{Z}$ be the isomorphisms. Now since $\alpha(c)$ satisfies all formulae of Γ we have that $e := \beta^{-1}(\alpha(c)) \in \mathfrak{B}$ also satisfies all formulae in Γ. So we have found e which looks like c up to congruence $\pmod{m!}$. Without loss of generality we can assume $0 \leq e < m!$.

Our final goal is to modify e, while preserving its congruence mod $m!$ so that it also looks like c in relation to the ordering. I.e. we must find $f \in \mathfrak{B}$ such that $d = e + f(m!)$ works.

We must deal with assertions of the form

$$t(\bar{a}) + ic > 0$$

where the complexity of t is $\leq m-1$ and $0 < i \leq m$. By multiplying through by $\frac{m!}{i}$ we reduce to assertions of the form

$$\frac{m!}{i} t(\bar{a}) + m!c > 0.$$

Setting $u(\bar{a}) := \frac{m!}{i} t(\bar{a}) + m!c$ we have that the complexity of u is $\leq (m-1)m! < m^{2m}$. Consider the set

$$\{t(\bar{a}) \mid c(t) \leq (m-1)m!\}.$$

This is a finite set. Let $t(\bar{a})$ chosen from this set so that $t(\bar{a}) < m!c$ maximally so (i.e. there is no other term $t'(\bar{a})$ such that $t(\bar{a}) < t'(\bar{a}) < m!c$). Similarly let $u(\bar{a})$ be chosen so that $u(\bar{a}) \geq m!c$ minimally so. If one of t or u doesn't exist, then we just ignore the corresponding part of the following argument. Now we have

$$t(\bar{a}) < m!c \leq u(\bar{a}).$$

Since $(\mathfrak{A}, \bar{a}) \sim^{\Xi}_{m^{2m}} (\mathfrak{B}, \bar{b})$ we have that

$$t(\bar{a}) \equiv t(\bar{b}) \pmod{(m!)^2}$$
$$u(\bar{a}) \equiv u(\bar{b}) \pmod{(m!)^2}.$$

and

$$m!c \equiv m!e \pmod{(m!)^2}$$

since $c \equiv e \pmod{(m!)}$. Thus there exists $g \in \mathfrak{B}$ such that

$$g \equiv m!e \equiv m!c \pmod{(m!)^2}.$$

Now letting $d = \frac{g}{m!}$ gives the desired element of $\mathfrak{B}$, so that $(\mathfrak{A}, \bar{a}, c) \sim^{\Xi}_{m} (\mathfrak{B}, \bar{b}, d)$. This completes the proof. □

The theorem now follows from the lemmas and the remarks above.

Automorphisms

We move on to discuss the relationship between reducts (and expansions), and automorphisms.

We will need a topology on our automorphism groups.

Definition. Given a set X let $\mathrm{Sym}(X) := \{\sigma : \sigma : X \to X \text{ is a bijection }\}$ by the group of permutations of X.

Remark. $\mathrm{Sym}(X)$ may be regarded as the automorphism group of the structure $\mathfrak{X}$ in the empty signature, with $\mathrm{dom}(\mathfrak{X}) = X$.

Sym(X) has a topology on it.

Notation. For $\sigma \in \mathrm{Sym}(X)$ and $\bar{a} \in X^n$ we write $\sigma\bar{a}$ for $(\sigma(a_0), \ldots, \sigma(a_{n-1}))$.

Definition. The **basic open set** $U_{\bar{a},\bar{b}}$ in Sym(X) have the form

$$U_{\bar{a},\bar{b}} := \{\sigma \in \mathrm{Sym}(X) : \sigma\bar{a} = \bar{b}\}$$

for $\bar{a}, \bar{b} \in X^n$. The open sets of the topology are unions of the basic open sets.

Remark. $U_{\bar{a},\bar{b}}$ are actually closed since

$$\mathrm{Sym}(X) \setminus U_{\bar{a},\bar{b}} = \bigcup_{\bar{c} \neq \bar{b}} U_{\bar{a},\bar{c}}.$$

So the sets $U_{\bar{a},\bar{b}}$ are *clopen.*

Remark. $U_{\bar{a},\bar{b}}$ is a coset of the stabilizer subgroup $\mathrm{Sym}(X)_{\bar{a}}$ (and also a coset of $\mathrm{Sym}(X)_{\bar{b}}$).

Remark. The point sets are closed. I.e. for any $\sigma \in \mathrm{Sym}(X)$

$$\{\sigma\} = \bigcap_{a \in X} U_{a,\sigma(a)}$$

is closed.

Remark. The topology we have given makes the action

$$\mu : \mathrm{Sym}(X) \times X \longrightarrow X$$

continuous when X is given the discrete topology. In fact it is the coarsest such topology. To see this let $V \subseteq X$ be a basic open set, i.e. $V = \{x\}$ for some $x \in X$. Then

$$\mu^{-1}(V) := \{(\sigma, y) \mid \sigma(y) = x\} = \bigcup_{y \in X} U_{y,x} \times \{y\}$$

which is open in the product topology $\mathrm{Sym}(X) \times X$.

If $\mathfrak{A}$ is a τ-structure then $\mathrm{Aut}(\mathfrak{A})$ is a subgroup of $\mathrm{Sym}(A)$. More generally if $\mathfrak{A}'$ is a τ'-structure and $\tau \subseteq \tau'$ then $\mathrm{Aut}(\mathfrak{A}')$ is a subgroup of $\mathrm{Aut}(\mathfrak{A}'|_\tau)$.

Theorem 2. $\mathrm{Aut}(\mathfrak{A})$ *is a closed subgroup of* $\mathrm{Sym}(A)$.

Proof. Let $\sigma \in \overline{\mathrm{Aut}(\mathfrak{A})}$. We want to show that $\sigma \in \mathrm{Aut}(\mathfrak{A})$. Let $\varphi(\bar{x})$ be any $\mathscr{L}(\tau)$-formula. We must show that for any $\bar{a}$ from $\mathfrak{A}$

$$\mathfrak{A} \models \varphi(\bar{a}) \iff \mathfrak{A} \models \varphi(\sigma\bar{a}).$$

Suppose $\mathfrak{A} \models \varphi(\bar{a})$. Let $\bar{b} := \sigma\bar{a}$. Since $\sigma \in \overline{\mathrm{Aut}(\mathfrak{A})}$ we have that $U_{\bar{a},\bar{b}} \cap \mathrm{Aut}(\mathfrak{A}) \neq \emptyset$ so there is some $\delta \in \mathrm{Aut}(\mathfrak{A})$ such that $\delta \in U_{\bar{a},\bar{b}}$ i.e. $\delta(\bar{a}) = \bar{b} = \sigma(\bar{a})$. So

$$\mathfrak{A} \models \varphi(\bar{a}) \iff \mathfrak{A} \models \varphi(\delta(\bar{a})) \iff \mathfrak{A} \models \varphi(\sigma(\bar{a})).$$

Thus $\sigma \in \mathrm{Aut}(\mathfrak{A})$. $\square$