Lecture 7

quantifier elimination

topics

- HW: Skolem paradox
- quantifier elimination (QE)
- non-examples (theories of the semiring of natural numbers, of the ring of integers and of the field of rationals)
- simple examples: DLO and RG
- reduction to primitive formulas
- a sufficient model-theoretic condition
- QE for ACF

HW

Skolem paradox:

- Assume that ZFC is satisfiable and argue first precisely that it has in infinite model.
- By the L-S theorem its has then also a countable model.
- How do you reconcile this with the fact that ZFC proves the existence of an uncountable set?

models of ZFC

$$\mathbf{M} \models \; ZFC \;\; \Rightarrow \;\; \mathbf{M} \models \; \exists \text{ an infinite set} \; .$$

But the term infinite is just a name: you can use any other name. By itself it does not imply that $\mathbf{M}$ is infinite.

Need to show that

$$\mathbf{M} \models \; \exists x_1, \ldots, x_k \; \bigwedge_{i \neq j} x_i \neq x_j$$

for all $k \geq 1$.

Use axioms of ZFC to prove that there are sets

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$$

and that they are all different.

HW cont'd

That ZFC proves the existence of an uncountable set just means that

$$\mathbf{M} \models \forall f,\ \neg(f : \mathbf{N} \rightarrow_{onto} A)$$

for some set $A \in M$.

That is, no $f \in M$ maps $\mathbf{N}$ onto A.

But M (and hence A) are countable and thus there is such a map g but

no such map g is in $\mathbf{M}$!

QE via skolemization

In Lecture 6 we reduced all L-formulas to quantifier-free formulas (= open flas) but at the expense that the language was extended by new function symbols. The price we paid was that we had little specific knowledge how the new f.symbols are interpreted.

Ex.: Over **C** look at

$$\exists y \sum_{0 \leq i \leq n} x_i y^i = 0$$

stating that the polynomial with coefficients x_i has a root.
The Skolem function $f(\overline{x})$ is just an abstract function that maps the coefficients to some root: it does not have to have any algebraic form.

The fla above is also equivalent to simple q-free formula:

$$x_n \neq 0 \vee \cdots \vee x_1 \neq 0 \vee (x_n = \cdots = x_1 = x_0 = 0)$$

which the skolemization ignores.

QE - def.

Definition - QE

An L-theory T has quantifier elimination (abbreviated QE) iff every L-formula is provably in T equivalent to a quantifier free (abbreviated q-free) formula.
An L-structure $\mathbf{A}$ has QE iff $Th(\mathbf{A})$ has QE.

NON-examples: theories of

$$\mathbf{N}, \mathbf{Z} \text{ and } \mathbf{Q}$$

in the language $0, 1, +, \cdot, <$.
Definable sets in these structures include many very complex sets and, in particular, sets that are algorithmically undecidable: this cannot happen for sets defined by q-free formulas.

DLO

Theorem

DLO has QE.

Prf.:

DLO is complete so we can concentrate on one its model: $(Q, <)$.

For $\overline{a} \in Q^n$ define its iso-type $itp_{\overline{a}}(x_1, \ldots, x_n)$ to be the set of formulas for all $i < j$:

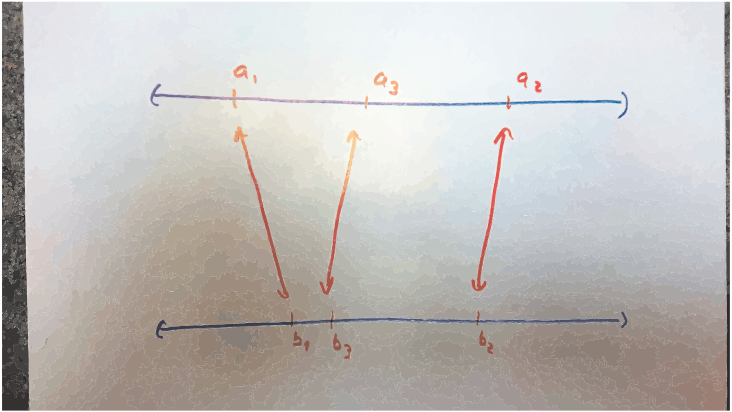
- $x_i = x_j$, if $a_i = a_j$,
- $x_i < x_j$, if $a_i < a_j$,
- $x_j < x_i$, if $a_i > a_j$.

Claim 1: For all $\overline{a}, \overline{b} \in Q^n$, if $itp_{\overline{a}} = itp_{\overline{b}}$ then

$$(Q, \overline{a}, <) \cong (Q, \overline{b}, <) \ .$$

Prf-claim: start the Ehr-Fr. game with pre-defined first n moves as (a_i, b_i), $i \leq n$.

pic



prf cont'd

Claim 1 implies
Claim 2: If $itp_{\overline{a}} = itp_{\overline{b}}$ then for all formulas $\varphi(\overline{x})$:

$$(Q,<) \models \varphi(\overline{a}) \;\Leftrightarrow\; (Q,<) \models \varphi(\overline{b}) \; .$$

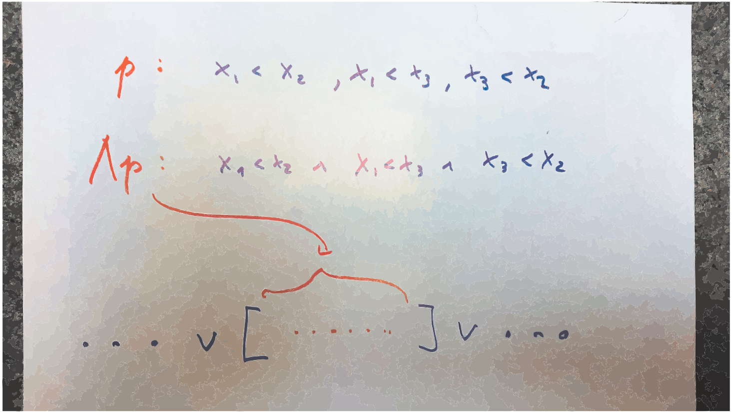
Given any formula $\psi(\overline{x})$ define a set of iso-types:

$$I_\psi\text{: all } itp_{\overline{a}} \text{ for all } \overline{a} \in Q^n \text{ such that } (Q,<) \models \psi(\overline{a}).$$

Claim 3: I_ψ is finite.

Put: $\psi' := \bigvee_{p \in I_\psi} \bigwedge p$
(picture next slide)

pic



prf-end

Claim 4: ψ and ψ' are equivalent in $(Q, <)$ and hence in DLO.
Prf-claim:

$(Q, <) \models \psi(\overline{a}) \;\Rightarrow\; p := itp_{\overline{a}} \in I_\psi \;\Rightarrow$
$\overline{a}$ satisfies $\bigwedge p \;\Rightarrow\; (Q, <) \models \psi'(\overline{a})$.

$(Q, <) \models \psi'(\overline{a}) \;\Rightarrow$
$\overline{a}$ satisfies iso-type of some $\overline{b}$ such that $(Q, <) \models \psi(\overline{b})$
$\Rightarrow$ (Claim 2) $(Q, <) \models \psi(\overline{b})$ too.

$\Box_{thm}$

a remark

An analogous argument works for theory RG as well.

In the theorem we were lucky that the Ehr-Fr game worked so well: it established even countable categoricity.

For incomplete theories (like is ACF without the axiom about characteristic) or for more complex theories as is RCF - the theory of the real closed ordered field we shall discuss in Lect.8 - we shall need a less ad hoc approach.

primitive flas

basic fla: an atomic of the negation of an atomic fla
primitive fla: a fla of the form

$$\exists \overline{y}\ \psi(\overline{x}, \overline{y})$$

where ψ is a conjunction of basic flas.

positive primitive fla: primitive fla without negations

Ex.: if L has no relation symbols then basic flas are equalities and inequalities between terms:

$$t(\overline{x}, \overline{y}) = s(\overline{x}, \overline{y})\ ,\ \ t(\overline{x}, \overline{y}) \neq s(\overline{x}, \overline{y})\ .$$

Hence positive primitive formulas state that a system of equations with parameters $\overline{x}$ is solvable for $\overline{y}$.

a reduction

Lemma

Assume that every primitive formula with one $\exists$ quantifier

$$\exists y \; \psi(\overline{x}, y)$$

is in T equivalent to a q-free formula. Then T has QE.

Prf.:

Any fla can be put into prenex form:

$$Q_1 y_1 \dots Q_k y_k \; \alpha(\overline{x}, \overline{y})$$

with α open. If we could remove one quantifier at a time we remove subsequently Q_k, then Q_{k-1} etc. Because $\forall$ can be replaced by $\neg\exists\neg$ it suffices to show that any fla of the form:

$$\exists y \; \beta(\overline{x}, y)$$

with β q-free is T-equivalent to a q-free fla.

prf cont'd

Write β in DNF:

$$\bigvee_i \bigwedge_j \gamma_{i,j}$$

with $\gamma_{i,j}$ basic flas and note that in logic only:

$$\exists y \bigvee_i \bigwedge_j \gamma_{i,j} \equiv \bigvee_i (\exists y \bigwedge_j \gamma_{i,j}) .$$

The hypothesis states that each fla $\exists y \bigwedge_j \gamma_{i,j}$ is T-equivalent to a q-free fla.
Hence is the whole fla.

$\square$

DLO again

Let us look back at DLO:

Negated atomic flas are DLO equivalent to disjunctions of atomic flas

$$u \neq v \equiv (u < v \vee v < u) \text{ and } \neg u < v \equiv (u = v \vee v < u)$$

and hence any primitive fla is equivalent to a disjunction of positive primitive flas.

Therefore by the lemma it suffices to show that each positive primitive fla with one $\exists$ quantifier

$$\exists y \; \psi(\overline{x}, y)$$

is DLO equivalent to a q-free one.

DLO cont'd

The equivalent q-free fla ψ' can be constructed as follows:

- if $x_i = y$ occurs in ψ, replace everywhere in ψ y by x_i and stop.
- Otherwise for each pair i, j such that both $x_i < y$ and $y < x_j$ occur in ψ add into ψ' fla $x_i < x_j$.
- If neither case occurs put $\psi' := (x_1 = x_1)$.

a model th. condition

Theorem

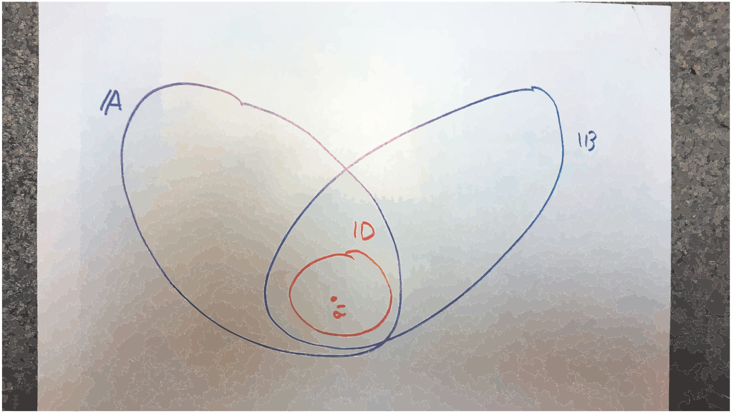
Assume that for any L-formula $\varphi(\overline{x})$ it holds that whenever the following situation occurs:

- $\mathbf{A}, \mathbf{B}$ are models of T,
- $\mathbf{D}$ is a substructure of both $\mathbf{A}$ and $\mathbf{B}$,
- $\overline{a} \in D^n$,
- $\mathbf{A} \models \varphi(\overline{a})$

then also $\mathbf{B} \models \varphi(\overline{a})$.

Then T has QE.

pic



a corollary

Corollary

To establish QE for T is suffices to show that for each primitive fla with one $\exists$ quantifier

$$\exists y\ \psi(\overline{x}, y)$$

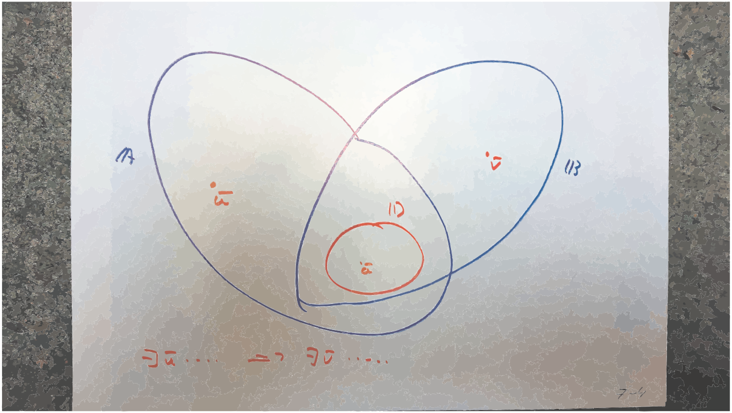
it holds that whenever

- $\mathbf{A}, \mathbf{B}$ are models of T,
- $\mathbf{D}$ is a substructure of both $\mathbf{A}$ and $\mathbf{B}$,
- $\overline{a} \in D^n$,
- $\mathbf{A} \models \psi(\overline{a}, u)$ for some $u \in A$

then there is $v \in B$ such that also

$$\mathbf{B} \models \psi(\overline{v})\ .$$

pic



prf

Prf of the thm: Let $\Gamma(\overline{x})$ be the set of all q-free flas $\alpha(\overline{x})$ such that

$$T \models \varphi(\overline{x}) \rightarrow \alpha(\overline{x}) \; .$$

Claim 1: $T \models \Gamma(\overline{x}) \rightarrow \varphi(\overline{x})$.
Prf - Claim 1:
If not, then there is some $\mathbf{A}$ and $\overline{a} \in A^n$:

$$\mathbf{A} \models T + \Gamma(\overline{a}) + \neg\varphi(\overline{a}) \; .$$

Take $\Sigma(\overline{a})$ the diagram of the substructure $\mathbf{D}$ generated by $\overline{a}$.

Claim 2: $T + \Sigma(\overline{a}) + \varphi(\overline{a})$ is satisfiable.
If not, it would hold that

$$T + \varphi(\overline{a}) \models \bigvee \neg\Sigma(\overline{a})$$

and so $\Sigma(\overline{a}) \cup \Gamma(\overline{a})$ is inconsistent. That is a contradiction - we have $\mathbf{A}$.

prf cont'd

Claim 2 implies that there is some **B** such that

$$\mathbf{B} \models T + \Sigma(\overline{a}) + \varphi(\overline{a})$$

i.e. also $\mathbf{D} \subseteq \mathbf{B}$.
That contradicts the hypothesis of the thm.

$\square_{Claim2}$

By compactness and by Claim 1 there is a finite $\Gamma_0 \subset \Gamma$ such that

$$T \models \Gamma_0(\overline{x}) \rightarrow \varphi(\overline{x})$$

Hence $\varphi(\overline{x})$ is in T equivalent to the disjunction of the q-free formulas in Γ_0.

$\square_{thm}$

QE for ACF

Now we apply the corollary to ACF.

Theorem (Tarski, Chevalley)

ACF has QE.

Prf.:

An atomic formula is an equality between terms $t(\overline{z}) = s(\overline{z})$ and terms compute polynomials over $\mathbf{N}$ (coefficients are generated from $0, 1$ by the operations). Such an equality is thus equivalent to polynomial equation

$$p(\overline{z}) = 0$$

where p is over $\mathbf{Z}$.

Hence a primitive formula with one $\exists$ quantifier asserts that a finite system of polynomial equations and inequalities:

$$\{p_i(\overline{x}, y) = 0\}_i \text{ and } \{q_j(\overline{x}, y) \neq 0\}_j$$

has, for a given tuple $\overline{x}$, a solution for y.

prf cont'd

We need to show that the condition in the corollary is met.
Let **A** and **B** be two ACF and let **D** be a common substructure. Note that we have $0, 1 \in D$ and hence the characteristic of both fields is the same.

The substructure is a ring which is an integral domain. It thus has the quotient field which itself has a unique algebraic closure; we shall call it **K**. It is the smallest ACF containing **D** and hence it is contained in both **A** and **B**.

Now assume $\overline{a} \in D^n \subseteq K^n$. Hence all polynomials $p_i(\overline{a}, y)$ and $q_j(\overline{a}, y)$ are now polynomials in y over **K**. Assume further that $u \in A$ witnesses the solvability of the system for y.

We consider two cases:

prf cont'd

Case 1: The equation part of the substituted system is non-empty, i.e. some equation

$$p_i(\overline{a}, y) = 0$$

is non-trivial. Then u is a root of a polynomial over $\mathbf{K}$ and hence it is in K, as $\mathbf{K}$ is ACF, and thus also in B.

Case 2: Not Case 1. Then either the system is independent of y or contains only some non-trivial satisfiable inequalities $q_j(\overline{a}, y) \neq 0$.

Each such inequality is satisfied by all elements of K except finitely many. Hence the system rules out finitely many possible values for y. But $\mathbf{K}$, being ACF, is infinite. Hence there is $v \in K \subseteq B$ satisfying the system.

$\square_{thm}$

HW problem

A take away problem: Establish QE for $Vect_Q$, the theory of vector spaces over $\mathbf{Q}$.