Logic in Computer Science

For a given language $\mathcal{F}, \mathcal{P}$, a *first-order theory* is a set T of sentences (closed formulae) in this given language. The elements of T are also called *axioms* of T.

A model of T is a model $\mathcal{M}$ of the given language such that $\mathcal{M} \models \psi$ for all sentences ψ in T.

$T \vdash \varphi$ means that we can find $\psi_1, \ldots, \psi_n$ in T such that $\psi_1, \ldots, \psi_n \vdash \varphi$.
$T \models \varphi$ means that $\mathcal{M} \models \varphi$ for all models $\mathcal{M}$ of T.

The generalized form of *soundness* is that $T \vdash \varphi$ implies $T \models \varphi$ and *completness* is that $T \models \varphi$ implies $T \vdash \varphi$.

If T is a finite set $\psi_1, \ldots, \psi_n$ this follows from the usual statement of soundness ($\vdash \delta$ implies $\models \delta$) and completness ($\models \delta$ implies $\vdash \delta$). Indeed, in this case, we have $T \vdash \varphi$ iff $\vdash (\psi_1 \wedge \cdots \wedge \psi_n) \to \varphi$ and $T \models \varphi$ iff $\models (\psi_1 \wedge \cdots \wedge \psi_n) \to \varphi$.

Theory of equivalence relations

The language is $\mathcal{P} = \{E\}$, binary relation, and $\mathcal{F} = \emptyset$. The axioms are

$$\forall x.\ E(x,x) \qquad \forall x\ y\ z.\ (E(x,z) \wedge E(y,z)) \to E(x,y)$$

We can then show $T \vdash \forall x\ y. E(x,y) \to E(y,x)$ and $T \vdash \forall x\ y\ z.\ (E(x,y) \wedge E(y,z)) \to E(x,z)$.

Theory about orders

The theory of *strict order*. The language is $\mathcal{P} = \{R\}$, binary relation, and $\mathcal{F} = \emptyset$. The axioms are

$$\forall x. \neg R(x,x) \qquad \forall x\ y\ z.\ (R(x,y) \wedge R(y,z)) \to R(x,z)$$

We can add equality and get the theory T_{lin} of *linear* orders

$$\forall x\ y.\ (x \neq y) \to (R(x,y) \vee R(y,x))$$

Models are given by the usual order on $\mathbb{N}, \mathbb{Q}, \mathbb{R}$. The model of rationals $(\mathbb{Q}, <)$ also satisfies

$$\psi_1 = \forall x. \exists y.\ R(x,y) \qquad \psi_2 = \forall x. \exists y.\ R(y,x) \qquad \psi_3 = \forall x\ y.\ R(x,y) \to \exists z.\ R(x,z) \wedge R(z,y)$$

It can be shown that we have $(\mathbb{Q}, <) \models \varphi$ iff $(\mathbb{R}, <) \models \varphi$ iff $T_{lin}, \psi_1, \psi_2, \psi_3 \vdash \varphi$ and furthermore, there is an algorithm to decide whether $(\mathbb{Q}, <) \models \varphi$ holds or not.

Theory about arithmetic

The language is $\mathcal{F} = \{\mathsf{zero}, \mathrm{S}\}$ and $\mathcal{P} = \emptyset$, but we have equality.

The first theory T_0 is

$$\forall x. \mathsf{zero} \neq \mathrm{S}(x) \qquad \forall x\ y. \mathrm{S}(x) = \mathrm{S}(y) \to x = y$$

A model of this theory is a set A with a constant $a \in A$ and a function $f \in A \to A$ such that f is injective and a is not in the image of f.

A particular model $\mathbb{N}$ is given by the set of natural numbers and $0 \in \mathbb{N}$ and the successor function s on $\mathbb{N}$.

The formulae $\delta_1 = \forall x.x \neq \mathrm{S}(x)$, $\delta_2 = \forall x.x \neq \mathrm{S}(\mathrm{S}(x)), \ldots$ are not provable in T_0 but are valid in the model $(\mathbb{N}, 0, \mathrm{s})$. The formula $\psi = \forall x.x = 0 \vee \exists y.(x = \mathrm{S}(y))$ is not provable in $T_0, \delta_1, \delta_2, \ldots$ but is also valid in the model $(\mathbb{N}, 0, \mathrm{s})$.

It can be shown that we have $(\mathbb{N}, 0, \mathrm{s}) \models \varphi$ iff $T_0, \delta_1, \delta_2, \ldots, \psi \vdash \varphi$ and furthermore, there is an algorithm to decide $(\mathbb{N}, 0, \mathrm{s}) \models \varphi$.

Presburger arithmetic

We add the binary function symbol $(+)$ and add to T_0 the axioms

$$\forall x.\ x + \mathsf{zero} = x \qquad\qquad \forall x\ y.\ x + \mathrm{S}(y) = \mathrm{S}(x + y)$$

and the induction schema

$$\forall y_1 \ldots y_m.\varphi(y_1, \ldots, y_m, \mathsf{zero}) \wedge \forall x.(\varphi(y_1, \ldots, y_m, x) \rightarrow (y_1, \ldots, y_m, \mathrm{S}(x))) \rightarrow \forall z.\varphi(y_1, \ldots, y_m, z)$$

The resulting theory PrA is called *Presburger arithmetic*. It can be shown that $(\mathbb{N}, 0, \mathrm{s}, +) \models \varphi$ iff $PrA \vdash \varphi$ and there is an algorithm to decide $(\mathbb{N}, 0, \mathrm{s}, +) \models \varphi$.

Presburger arithmetic

We add the binary function symbol $(\cdot)$ and add to PrA the axioms for multiplication

$$\forall x.\ x \cdot \mathsf{zero} = \mathsf{zero} \qquad\qquad \forall x\ y.\ x \cdot \mathrm{S}(y) = x \cdot y + x$$

with the induction schema, where the formula $\varphi(y_1, \ldots, y_m, x)$ can also used multiplication. The resulting theory PA is called *Peano arithmetic*. It has been shown by Gödel that PA is *incomplete*: there is a formula φ such that $(\mathbb{N}, 0, \mathrm{s}, +, \cdot) \models \varphi$ but we don't have $PA \vdash \varphi$.

Furthermore $(\mathbb{N}, 0, \mathrm{s}, +, \cdot) \models \varphi$ is undecidable (there is no algorithm to decide $\mathbb{N} \models \varphi$) and there is *no* effective way to enumerate all sentences φ valid in the model $(\mathbb{N}, 0, \mathrm{s}, +, \cdot)$.

The decision problem

The *decision problem* (Hilbert-Ackermann 1928) is the problem of deciding if a sentence in a given language is provable or not.

More generally the problem is to decide if we have $\psi_1, \ldots, \psi_n \vdash \varphi$ or not.

There are special cases where this problem has a positive answer.

A general method is to apply the following remark: we have $\psi_1, \ldots, \psi_n \vdash \varphi$ iff the following theory $\psi_1, \ldots, \psi_n, \neg\varphi$ has *no* models. This follows from soundness and completeness.

Bernays-Schönfinkel decidable case

This is the particular case where $\mathcal{F}$ has only *constant* symbols and all formulae $\psi_1, \ldots, \psi_n, \varphi$ are of the form $\forall y_1 \ldots y_m.\delta$ or $\exists y_1 \ldots y_m.\delta$ where δ is quantifier-free.

In this case the following algorithm, that I illustrate on some examples, gives a way to decide whether $\psi_1, \ldots, \psi_n, \neg\varphi$ has a model or not. (If it has a model, it always has a *finite* model.) In this way, we decide whether $\psi_1, \ldots, \psi_n \vdash \varphi$ holds or not.

We take the example

$$T_1 = \exists x.(P(x) \wedge \neg M(x)), \exists y.(M(y) \wedge \neg S(y)), \forall z.(\neg P(z) \vee S(z))$$

The first step is to eliminate the existential quantifiers by introducing constants

$$T_2 = P(a) \wedge \neg M(a),\ M(b) \wedge \neg S(b), \forall z.(\neg P(z) \vee S(z))$$

It should be clear that T_1 has a model iff T_2 has a model.

The second step is to eliminate the universal quantifiers by instantiating on all constants

$$T_3 = P(a) \wedge \neg M(a),\ M(b) \wedge \neg S(b),\ \neg P(a) \vee S(a),\ \neg P(b) \vee S(b)$$

In this way we find a model with two elements $P(a), \neg M(a), S(a), M(b), \neg S(b), \neg P(b)$.

This implies that $\exists x.(P(x) \wedge \neg M(x)), \exists y.(M(y) \wedge \neg S(y)) \vdash \exists z.(P(z) \wedge \neg S(z))$ is *not* valid.

Other examples

$\forall x.\neg R(x,x) \vdash \forall x\ y.(R(x,y) \rightarrow \neg R(y,x)$ is not valid since we find a model of

$$T_1 = \forall x.\neg R(x,x),\ \exists x\ y.\ R(x,y) \wedge R(y,x)$$

by eliminating existentials

$$T_2 = \forall x.\neg R(x,x),\ R(a,b) \wedge R(b,a)$$

and then universals

$$T_3 = \neg R(a,a),\ \neg R(b,b),\ R(a,b) \wedge R(b,a)$$

and we get a counter-model with two elements.

On the other hand $\forall x\ y.(R(x,y) \rightarrow \neg R(y,x) \vdash \neg R(x,x)$ is valid, since if we try to find a model of

$$T_1 = \forall x\ y.(R(x,y) \rightarrow \neg R(y,x)),\ \exists x.R(x,x)$$

by eliminating existentials

$$T_2 = \forall x\ y.(R(x,y) \rightarrow \neg R(y,x)),\ R(a,a)$$

and then universals

$$T_3 = R(a,a) \rightarrow \neg R(a,a),\ R(a,a)$$

we should have $R(a,a)$ and $\neg R(a,a)$ and we cannot find a counter-model.

Theory of cyclic order

(Not covered in the lecture, but a nice example of a theory and of the use of the Bernays-Schönfinkel algorithm.)

A *cyclic order* is a way to arrange a set of objects in a circle (examples: seven days in a week, twelve notes in the chromatic scale, ...). The language is $\mathcal{P} = \{S\}$ which is a *ternary* predicate symbol and the first 3 axioms are

$$\psi_1 = \forall x\ y\ z.S(x,y,z) \to S(y,z,x) \qquad \psi_2 = \forall x\ y\ z.S(x,y,z) \to \neg S(x,z,y)$$

$$\psi_3 = \forall x\ y\ z\ t.(S(x,y,z) \wedge S(x,z,t)) \to S(x,y,t)$$

One can then use the Bernays-Schönfinkel algorithm to show automatically that these axioms are *independent*: we don't have $\psi_1, \psi_2 \vdash \psi_3$ or $\psi_2, \psi_3 \vdash \psi_1$ or $\psi_3, \psi_1 \vdash \psi_2$.

The last axiom of the theory of cyclic order uses equality

$$\psi_4 = \forall x\ y\ z.(x \neq y \wedge y \neq z \wedge z \neq x) \to S(x,y,z) \vee S(x,z,y)$$

The extension of the Bernays-Schönfinkel algorithm to equality is possible by axiomatising the equality relation. (This was first done by Ramsey, 1928, by another method.)