FLOLAC 2026

Logic

II. First-order logic and Peano–Heyting arithmetic

柯向上

中央研究院資訊科學研究所

https://josh-hs-ko.github.io

A richer structure of propositions

When talking about mathematical structures such as Peano–Heyting (natural number) arithmetic, we use statements such as

for every x, if $x \neq 0$ then **there exists** y such that $\mathit{suc}\ y = x$

that involve *first-order quantification* over individual values in a *domain*.

(The function *suc* is the *successor* function on natural numbers.)

This motivates us to extend propositional logic with first-order quantification, and the result is called *first-order logic*.

Going from propositional logic to first-order logic requires more than enriching the language with quantification though.

Substitution

Variables are to be *substituted* for. For example, from

for every x, if $x \neq 0$ then there exists y such that *suc* $y = x$

we should be able to deduce

if $1 \neq 0$ then there exists y such that *suc* $y = 1$

by substituting 1 for the variable x.

The structure of (previously) atomic propositions must be refined so the variable x can be substituted.

Sub-atomic structure

Syntactically, the proposition $suc\ y = x$ may be analysed as follows:

- '$=$' is a *predicate symbol* that accepts two *terms*, and
- '*suc*' is a *function symbol* that can be used to construct more complex terms, which can contain variables.

Each symbol has an associated natural number called its *arity*, which specifies the number of sub-terms the symbol expects.

Terms

Let $\mathcal{IV} := \{ \mathtt{x}, \mathtt{y}, \mathtt{z}, \ldots \}$ be an infinite set of individual variables.

Definition. Given a set $\mathcal{F}$ of symbols with arities, the set $\textsc{Term}_{\mathcal{F}}$ of *terms* is inductively defined by the following rules:

- $v : \textsc{Term}_{\mathcal{F}}$ for all $v : \mathcal{IV}$;
- $f\, t_1 \ldots t_n : \textsc{Term}_{\mathcal{F}}$ for all $f/n : \mathcal{F}$ (function symbol f with arity n) and t_1, …, $t_n : \textsc{Term}_{\mathcal{F}}$.

Example. For terms in Peano–Heyting arithmetic, we choose $\mathcal{F} := \{ \mathtt{zero}/0, \mathtt{suc}/1, \mathtt{add}/2, \mathtt{mul}/2 \}$.

Question. Why does $\mathcal{IV}$ need to be infinite?

First-order formulas

Definition. A *signature* $\mathcal{S}$ is a pair of sets $(\mathcal{P}, \mathcal{F})$ of symbols with arities, where elements of $\mathcal{P}$ are called *predicate symbols* and elements of $\mathcal{F}$ are called *function symbols*.

Definition. Given a signature $\mathcal{S} = (\mathcal{P}, \mathcal{F})$, the set $\textsc{Form}_{\mathcal{S}}$ of *first-order formulas* is inductively defined by the following rules:

- $\bot : \textsc{Form}_{\mathcal{S}}$;
- $p\ t_1 \ldots t_n : \textsc{Form}_{\mathcal{S}}$ for all $p/n : \mathcal{P}$ and t_1, …, $t_n : \textsc{Term}_{\mathcal{F}}$;
- $\varphi \wedge \psi : \textsc{Form}_{\mathcal{S}}$ for all φ, $\psi : \textsc{Form}_{\mathcal{S}}$;
- $\varphi \vee \psi : \textsc{Form}_{\mathcal{S}}$ for all φ, $\psi : \textsc{Form}_{\mathcal{S}}$;
- $\varphi \to \psi : \textsc{Form}_{\mathcal{S}}$ for all φ, $\psi : \textsc{Form}_{\mathcal{S}}$;
- $\forall\, v.\ \varphi : \textsc{Form}_{\mathcal{S}}$ for all $v : \mathcal{IV}$ and $\varphi : \textsc{Form}_{\mathcal{S}}$;
- $\exists\, v.\ \varphi : \textsc{Form}_{\mathcal{S}}$ for all $v : \mathcal{IV}$ and $\varphi : \textsc{Form}_{\mathcal{S}}$.

Instantiations of first-order logic

Example. The signature for Peano–Heyting arithmetic consists of $\mathcal{P} := \{\, \mathtt{Eq}/2 \,\}$ and $\mathcal{F} := \{\, \mathtt{zero}/0,\ \mathtt{suc}/1,\ \mathtt{add}/2,\ \mathtt{mul}/2 \,\}$.

The proposition

> **for every** x, if $x \neq 0$ then **there exists** y such that *suc* $y = x$

is written formally as

$$\forall\, \mathtt{x}.\ ((\neg\, \mathtt{Eq}\ \mathtt{x}\ \mathtt{zero}) \to \exists\, \mathtt{y}.\ \mathtt{Eq}\ (\mathtt{suc}\ \mathtt{y})\ \mathtt{x})$$

Question. Why these particular parentheses? Why not more? Why not less?

Instantiations of first-order logic (continued)

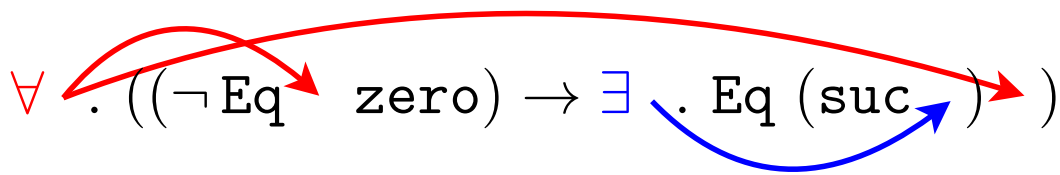
Example. For Tarski's axioms for Euclidean geometry, individuals are points, and the signature consists of $\mathcal{P} := \{\, \mathtt{Eq}/2, \mathtt{B}/3, \mathtt{Ed}/4 \,\}$ and $\mathcal{F} := \{\}$, where $\mathtt{Eq}$ is equality of points, $\mathtt{B}\ x\ y\ z$ means y is between x and z, and $\mathtt{Ed}\ x\ y\ z\ w$ means the distances from x to y and from z to w are equal.

Exercise. Formalise the 'axiom of segment construction': given any segment $\overline{ab}$, any segment $\overline{xy}$ can be extended to a segment $\overline{xz}$ such that the segment $\overline{yz}$ is as long as $\overline{ab}$.

Representations of binding (intuitively)

The choice of variable in *binders* $\forall\, v$ and $\exists\, v$ is not important and can be changed by *α-conversion*; what is important is the *binding* structure, that is, when a binder is instantiated, which variable occurrences are to be substituted for.

'Ideally' we would want to represent binding graphically, for example writing/drawing



which can be represented textually as

$$\forall \mathtt{x}.\ ((\neg\, \mathtt{Eq\ x\ zero}) \rightarrow \exists\, \mathtt{y}.\ \mathtt{Eq\ (suc\ y)\ x})$$
$$\forall \mathtt{z}.\ ((\neg\, \mathtt{Eq\ z\ zero}) \rightarrow \exists\, \mathtt{y}.\ \mathtt{Eq\ (suc\ y)\ z})$$

and so on (these are called *α-equivalent* formulas), but not as

$$\forall \mathtt{x}.\ ((\neg\, \mathtt{Eq\ x\ zero}) \rightarrow \exists\, \mathtt{x}.\ \mathtt{Eq\ (suc\ x)\ x})$$

which represents a different binding structure.

Substitution and variable capture (informally)

A variable occurrence under a binder of the same variable is *bound*; otherwise it is *free*.

Write $\varphi\,[t/v]$ for the result of substituting the term t for the free occurrences of the variable v in the formula φ.

Naive substitution can result in *variable capture*, which creates unintended variable binding. For example:

$$\begin{aligned}&((\neg\,\texttt{Eq x zero}) \to \exists\,\texttt{y}.\ \texttt{Eq (suc y) x})\,[\texttt{add z y/x}]\\ \neq\ &(\neg\,\texttt{Eq (add z y) zero}) \to \exists\,\texttt{y}.\ \texttt{Eq (suc y) (add z y)}\end{aligned}$$

Textual substitution

Substitution $\varphi\,[t/v]$ can be performed directly by replacing every occurrence of v in φ with t if a side condition is satisfied:

> *all the binder variables in φ are different from v and the (free) variables in t.*

And the side condition can always be satisfied by α-converting φ suitably.

Exercise. Let $\varphi := (\exists\, \mathtt{z}.\ \mathtt{Eq\ x\ (add\ z\ y)}) \wedge \exists\, \mathtt{y}.\ \mathtt{Eq\ x\ (add\ y\ y)}$.

- Which variable occurrences are free in φ?
- Compute $\varphi\,[\mathtt{zero}/\mathtt{y}]$.
- Compute $\varphi\,[\mathtt{suc\ z}/\mathtt{x}]$.

Question. Why is the side condition sufficient?

Formal definitions of free variables

Definition. Let $\mathcal{F}$ be a set of function symbols with arities. The set of (free) variables in a term is defined by

$$\begin{array}{lcll} FV : \textsc{Term}_{\mathcal{F}} \to \wp\, \mathcal{IV} & & & \\ FV\, v & = & \{v\} & \text{for } v : \mathcal{IV} \\ FV\, (f\, t_1 \ldots t_n) & = & FV\, t_1 \cup \cdots \cup FV\, t_n & \text{for } f/n : \mathcal{F} \end{array}$$

Definition. Let $\mathcal{S} = (\mathcal{P}, \mathcal{F})$ be a signature. The set of free variables in a first-order formula is defined by

$$\begin{array}{lcll} FV : \textsc{Form}_{\mathcal{S}} \to \wp\, \mathcal{IV} & & & \\ FV\, \bot & = & \{\} & \\ FV\, (p\, t_1 \ldots t_n) & = & FV\, t_1 \cup \cdots \cup FV\, t_n & \text{for } p/n : \mathcal{P} \\ FV\, (\varphi \bullet \psi) & = & FV\, \varphi \cup FV\, \psi & \text{where } \bullet = \wedge, \vee, \to \\ FV\, (\forall\, v.\, \varphi) & = & FV\, \varphi \setminus \{v\} & \\ FV\, (\exists\, v.\, \varphi) & = & FV\, \varphi \setminus \{v\} & \end{array}$$

Exercise. Define α-conversion, substitution, etc formally.

Intuitionistic meaning of quantifiers

We assume a set $\mathcal{D}$, called the *domain (of discourse)*, over which we quantify.

A formula φ with free variable v describes a property of an element in $\mathcal{D}$ referred to as v.

- A proof of $\forall\, v.\ \varphi$ is a method that, for every element $d : \mathcal{D}$, produces a proof of φ for d.
- A proof of $\exists\, v.\ \varphi$ is an element $d : \mathcal{D}$ —called the *witness*— and a proof of φ for d.

To obtain a deduction system for intuitionistic first-order logic, we extend NJ with introduction and elimination rules for '$\forall$' and '$\exists$'.

Introducing and eliminating '∀'

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall\, v.\ \varphi}\ (\forall\mathsf{I}) \qquad \frac{\Gamma \vdash \forall\, v.\ \varphi}{\Gamma \vdash \varphi\,[t/v]}\ (\forall\mathsf{E})$$

($\forall$I) has a side condition that $v \notin FV\,\Gamma$, where

$$FV\,\Gamma \;:=\; \bigcup_{\psi \in \Gamma} FV\,\psi$$

That is, to generalise φ to $\forall v.\ \varphi$, there should be no assumptions about v.

Exercise. Derive

$$\vdash (\forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \mathtt{P}\ \mathtt{x}\ \mathtt{y}) \to \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \mathtt{P}\ \mathtt{y}\ \mathtt{x}$$

Exercise. Try to derive

$$\vdash \forall \mathtt{x}.\ (\mathtt{Eq}\ \mathtt{x}\ \mathtt{zero} \to \forall\, \mathtt{x}.\ \mathtt{Eq}\ \mathtt{x}\ \mathtt{zero})$$

Introducing and eliminating '∃'

$$\frac{\Gamma \vdash \varphi\,[t/v]}{\Gamma \vdash \exists\, v.\ \varphi}\ (\exists\mathsf{I}) \qquad \frac{\Gamma \vdash \exists\, v.\ \varphi \qquad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \psi}\ (\exists\mathsf{E})$$

($\exists$E) has a side condition that $v \notin FV\,\Gamma \cup FV\,\psi$.
That is, v should be a name chosen freshly for the witness.

Exercise. Derive

$$\vdash (\exists\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \mathtt{P\ x\ y}) \to \forall\, \mathtt{y}.\ \exists\, \mathtt{x}.\ \mathtt{P\ x\ y}$$

Exercise. Try to finish deriving

$$\dfrac{\dfrac{\exists\, \mathtt{x}.\ \mathtt{P\ x} \vdash \mathtt{P\ x}}{\exists\, \mathtt{x}.\ \mathtt{P\ x} \vdash \forall\, \mathtt{x}.\ \mathtt{P\ x}}\ (\forall\mathsf{I})}{\vdash (\exists\, \mathtt{x}.\ \mathtt{P\ x}) \to \forall\, \mathtt{x}.\ \mathtt{P\ x}}\ (\to\mathsf{I})$$

Exercise. Try to derive

$$\vdash \forall\, \mathtt{x}.\ ((\neg\, \mathtt{Eq\ x\ zero}) \to \neg\, \exists\, \mathtt{x}.\ \mathtt{Eq\ x\ zero})$$

Remark on intuitionistic existential quantification

We can derive

$$\vdash (\exists\, v.\ \varphi) \to (\neg \forall\, v.\ \neg\varphi) \quad \text{but not} \quad \vdash (\neg \forall\, v.\ \neg\varphi) \to (\exists\, v.\ \varphi)$$

Intuitionistic existential quantification is stronger than its classical counterpart (which is definable from '$\forall$' and '$\neg$').

Exercise. Derive $\vdash (\neg \forall\, v.\ \neg\varphi) \to (\exists\, v.\ \varphi)$ assuming the law of excluded middle or the principle of indirect proof.

Similar to Glivenko's theorem for propositional logic, there are double-negation translations for embedding classical first-order logic into intuitionistic first-order logic.

Peano–Heyting arithmetic

The signature for Peano–Heyting arithmetic consists of $\mathcal{P} := \{\, \mathtt{Eq}/2 \,\}$ and $\mathcal{F} := \{\, \mathtt{zero}/0,\ \mathtt{suc}/1,\ \mathtt{add}/2,\ \mathtt{mul}/2 \,\}$.

In the following we write $t_1 \equiv t_2$ for $\mathtt{Eq}\ t_1\ t_2$, $t_1 + t_2$ for $\mathtt{add}\ t_1\ t_2$, and $t_1 \times t_2$ for $\mathtt{mul}\ t_1\ t_2$.

Properties about these constants are postulated by the (infinite) list $\mathbf{PA}$ of *Peano axioms*, to be given in the next two slides.

Definition. A formula φ is a *sentence* exactly when $FV\,\varphi = \emptyset$.

Definition. A list of sentences is called a *theory*, whose elements are called *axioms*.

Definition. A sentence derivable from a theory $\mathcal{T}$ is called a *theorem* of $\mathcal{T}$.

Example. $\mathbf{PA}$ is a theory.

Question. Why include only sentences in a theory?

Peano axioms: predicate and function symbols

The first three axioms make $\mathtt{Eq}$ an equivalence relation.

$$
\begin{array}{lcl}
\mathit{reflexivity} & := & \forall\, \mathtt{x}.\ \mathtt{x} \equiv \mathtt{x} \\
\mathit{transitivity} & := & \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \forall\, \mathtt{z}.\ ((\mathtt{x} \equiv \mathtt{y} \wedge \mathtt{y} \equiv \mathtt{z}) \rightarrow \mathtt{x} \equiv \mathtt{z}) \\
\mathit{symmetry} & := & \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ (\mathtt{x} \equiv \mathtt{y} \rightarrow \mathtt{y} \equiv \mathtt{x})
\end{array}
$$

The next three axioms are about $\mathtt{zero}$ and $\mathtt{suc}$.

$$
\begin{array}{lcl}
\mathit{disjointness} & := & \forall\, \mathtt{x}.\ \neg\, (\mathtt{suc}\ \mathtt{x} \equiv \mathtt{zero}) \\
\mathit{injectivity} & := & \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ (\mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y} \rightarrow \mathtt{x} \equiv \mathtt{y}) \\
\mathit{congruence} & := & \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ (\mathtt{x} \equiv \mathtt{y} \rightarrow \mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y})
\end{array}
$$

The following four axioms characterise $\mathtt{add}$ and $\mathtt{mul}$.

$$
\begin{array}{lcl}
\mathit{additionZ} & := & \forall\, \mathtt{y}.\ \mathtt{zero} + \mathtt{y} \equiv \mathtt{y} \\
\mathit{additionS} & := & \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ (\mathtt{suc}\ \mathtt{x}) + \mathtt{y} \equiv \mathtt{suc}\ (\mathtt{x} + \mathtt{y}) \\
\mathit{multiplicationZ} & := & \forall\, \mathtt{y}.\ \mathtt{zero} \times \mathtt{y} \equiv \mathtt{zero} \\
\mathit{multiplicationS} & := & \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ (\mathtt{suc}\ \mathtt{x}) \times \mathtt{y} \equiv \mathtt{y} + (\mathtt{x} \times \mathtt{y})
\end{array}
$$

Peano axioms: induction

Finally there is an *axiom scheme* that generates infinite instances of the induction principle on natural numbers: for every formula φ (called the *motive*) and variable v there is an axiom

$$\begin{aligned} &\mathit{induction}_{\varphi,\,v} \;:= \\ &\quad \mathit{closure}\,((\varphi\,[\mathtt{zero}/v] \wedge \forall\, v.\ (\varphi \to (\varphi\,[\mathtt{suc}\ v/v]))) \to \forall\, v.\ \varphi) \end{aligned}$$

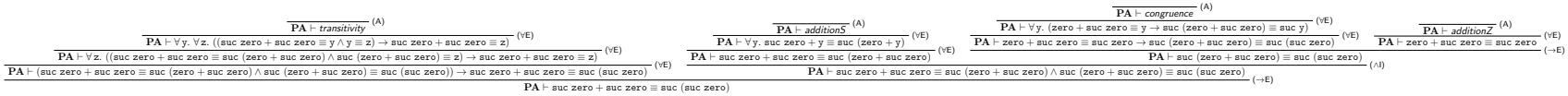
Definition. The *universal closure* of a formula ψ is defined by

$$\mathit{closure}\,\psi \;:=\; \forall\, v_1.\ \ldots \forall\, v_n.\ \psi \quad \text{where} \quad \mathit{FV}\,\psi = \{v_1, \ldots, v_n\}$$

Question. Is it necessary to take the closure? Alternatively, for example, can φ range over formulas with v as its only free variable?

Example: $1 + 1 = 2$

Deriving $\mathbf{PA} \vdash \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc}\ (\mathtt{suc\ zero})$:



Informally:

- The left-hand side $\mathtt{suc\ zero} + \mathtt{suc\ zero}$ of '$\equiv$' is transformed into $\mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero})$ by *additionS*.
- The sub-term $\mathtt{zero} + \mathtt{suc\ zero}$ is just $\mathtt{suc\ zero}$ by *additionZ*, so by *congruence* we can derive that $\mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero})$ is equal to $\mathtt{suc}\ (\mathtt{suc\ zero})$.
- The above two equations are concatenated by *transitivity*.

Example: every natural number is either even or odd

Deriving $\mathbf{PA} \vdash \forall\, \mathtt{x}.\ \exists\, \mathtt{y}.\ (\mathtt{x} \equiv \mathtt{y} + \mathtt{y} \vee \mathtt{x} \equiv \mathtt{suc}\ (\mathtt{y} + \mathtt{y}))$:

This requires an induction on $\mathtt{x}$. Informally:

- Base case: derive $\mathtt{zero} \equiv \mathtt{zero} + \mathtt{zero}$, which follows from *additionZ* and *symmetry*.
- Inductive case: the induction hypothesis can be analysed into two sub-cases $\mathtt{x}' \equiv \mathtt{y}' + \mathtt{y}'$ and $\mathtt{x}' \equiv \mathtt{suc}\ (\mathtt{y}' + \mathtt{y}')$.
  - For the first sub-case, derive $\mathtt{suc}\ \mathtt{x}' \equiv \mathtt{suc}\ (\mathtt{y}' + \mathtt{y}')$ by *congruence*.
  - For the second sub-case, derive $\mathtt{suc}\ \mathtt{x}' \equiv \mathtt{suc}\ \mathtt{y}' + \mathtt{suc}\ \mathtt{y}'$ by *additionS* and the property below (with the help of *symmetry*, *transitivity*, and *congruence*).

Exercise. Derive $\mathbf{PA} \vdash \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \mathtt{suc}\ (\mathtt{x} + \mathtt{y}) \equiv \mathtt{x} + \mathtt{suc}\ \mathtt{y}$.