Programming
Research
Laboratory

FLOLAC '18

Logic

First-order logic

12 July 2018

柯向上

(日本) 国立情報学研究所

hsiang-shang@nii.ac.jp

A richer structure of propositions

When talking about mathematical structures like Peano/Heyting (natural number) arithmetic, we use statements like

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

that involve *quantification* over individuals, which is not present in the language of propositional logic.

(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

In the proposition $\mathtt{suc}\ \mathtt{y} = \mathtt{x}$,

- '$=$' is a *predicate symbol* that accepts two *terms*, and
- '$\mathtt{suc}$' 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 variable symbols.

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:

- $v \in \textsc{Term}_{\mathcal{F}}$ if $v : \mathcal{IV}$;
- for any $f \in \mathcal{F}$ with arity n,
  $f\, t_1 \ldots t_n \in \textsc{Term}_{\mathcal{F}}$ if t_1, …, $t_n \in \textsc{Term}_{\mathcal{F}}$.

Example. For terms in Peano/Heyting arithmetic, we choose $\mathcal{F} := \{\, \mathtt{zero}/0, \mathtt{suc}/1, \mathtt{add}/2, \mathtt{mult}/2 \,\}$ (where '$/n$' indicates the arity of a symbol).

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 defined by the following rules:

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

Example: Signature for Peano/Heyting arithmetic

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

The proposition

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

is written formally as

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

Definition of (capture-avoiding) substitution

Definition. Let $\mathcal{S} = (\mathcal{P}, \mathcal{F})$ be a signature, $t \in \textsc{Term}_{\mathcal{F}}$, and $v \in \mathcal{IV}$. The function $\_[t/v] : \textsc{Form}_{\mathcal{S}} \to \textsc{Form}_{\mathcal{S}}$, which substitutes t for v in a first-order formula, is defined by

$$
\begin{array}{lcll}
\bot\ [t/v] & = & \bot & \\
(p\ t_1 \ldots t_n)\ [t/v] & = & p\ (t_1\ [t/v]) \ldots (t_n\ [t/v]) & \text{for } p/n \in \mathcal{P} \\
(\varphi \wedge \psi)\ [t/v] & = & \varphi\ [t/v]\ \wedge\ \psi\ [t/v] & \\
(\varphi \vee \psi)\ [t/v] & = & \varphi\ [t/v]\ \vee\ \psi\ [t/v] & \\
(\varphi \to \psi)\ [t/v] & = & \varphi\ [t/v]\ \to\ \psi\ [t/v] & \\
(\forall\, u.\ \varphi)\ [t/v] & = & \forall\, u.\ \varphi\ [t/v] & \text{where } u \neq v \text{ and } u \notin FV\ t \\
(\exists\, u.\ \varphi)\ [t/v] & = & \exists\, u.\ \varphi\ [t/v] & \text{where } u \neq v \text{ and } u \notin FV\ t,
\end{array}
$$

where $\_[t/v] : \textsc{Term}_{\mathcal{F}} \to \textsc{Term}_{\mathcal{F}}$ is defined by

$$
\begin{array}{lcll}
u\ [t/v] & = & \textbf{if } u = v \textbf{ then } t \textbf{ else } u & \text{for } u \in \mathcal{IV} \\
(f\ t_1 \ldots t_n)\ [t/v] & = & f\ (t_1\ [t/v]) \ldots (t_n\ [t/v]) & \text{for } f/n \in \mathcal{F}.
\end{array}
$$

The missing definitions

Let $\mathcal{S} = (\mathcal{P}, \mathcal{F})$ be a signature.

Exercise. Define the function *FV* on $\text{FORM}_{\mathcal{S}}$ and $\text{TERM}_{\mathcal{F}}$ mapping a formula or a term to the set of its free variables.

Exercise. Define α-equivalence on $\text{FORM}_{\mathcal{S}}$.

Now consider Peano/Heyting arithmetic.

Exercise. Simplify

$$(\neg(\texttt{Eq x zero}) \to \exists\,\texttt{y}.\ \texttt{Eq}\ (\texttt{suc y})\ \texttt{x})\ [\texttt{add x y}/\texttt{x}]$$

according to the definitions.

Intuitionistic meaning of quantifiers

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

- A proof of $\forall\, v.\ \varphi$ is a method that, for every $d \in \mathcal{D}$, produces a proof of φ about d.
- A proof of $\exists\, v.\ \varphi$ is a value $d \in \mathcal{D}$ (called the *witness*) and a proof of φ about 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 '∀'

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

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

$$FV\,\Gamma \ := \ \bigcup_{\varphi \in \Gamma} FV\,\varphi$$

Exercise. Derive

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

Non-example of ($\forall$I)

Why and how is this derivation wrong?

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\texttt{Eq x zero} \vdash \texttt{Eq x zero}}}{\texttt{Eq x zero} \vdash \forall\,\texttt{x. Eq x zero}}\;(\forall\mathsf{I})}{\vdash \texttt{Eq x zero} \to \forall\,\texttt{x. Eq x zero}}\;(\to\mathsf{I})}{\vdash \forall\,\texttt{x. Eq x zero} \to \forall\,\texttt{x. Eq x zero}}\;(\forall\mathsf{I})}{\vdash \texttt{Eq zero zero} \to \forall\,\texttt{x. Eq x zero}}\;(\forall\mathsf{E})$$

Introducing and eliminating '∃'

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

(∃E) has a side condition that $v \notin FV\,\Gamma \cup FV\,\psi$.

Exercise. Derive

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

Non-example of (∃E)

Why and how is this derivation wrong?

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

Remark on negation and the existential quantifier

We can derive

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

Intuitionistic existential quantification is stronger than its classical counterpart.

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

Similar to the Glivenko's theorem for propositional logic, there are ways to embed classical first-order logic into intuitionistic first-order logic.

Instantiating signatures

Definition. Given a signature $\mathcal{S} = (\mathcal{P}, \mathcal{F})$, an *$\mathcal{S}$-structure* $\mathcal{M}$ consists of

- a nonempty set called the *domain*, which is simply denoted by $\mathcal{M}$,
- a function $[\![p]\!]_{\mathcal{M}} : (\mathcal{M} \rightarrow)^n \mathbf{2}$ for each predicate symbol $p/n \in \mathcal{P}$, and
- a function $[\![f]\!]_{\mathcal{M}} : (\mathcal{M} \rightarrow)^n \mathcal{M}$ for each function symbol $f/n \in \mathcal{F}$.

Definition. Given a structure $\mathcal{M}$, the set of *$\mathcal{M}$-assignments* is defined to be $\mathcal{IV} \rightarrow \mathcal{M}$.

Classical semantics of first-order logic

Definition. Let $\mathcal{S} = (\mathcal{P}, \mathcal{F})$ be a signature, $\mathcal{M}$ an $\mathcal{S}$-structure, and σ an $\mathcal{M}$-assignment. The *truth-value interpretation* $[\![\_]\!]_{\mathcal{M},\sigma} : \textsc{Form}_{\mathcal{S}} \to \mathbf{2}$ of formulas is defined as follows:

$$
\begin{array}{lcll}
[\![\bot]\!]_{\mathcal{M},\sigma} & = & 0 & \\
[\![p\ t_1 \ldots t_n]\!]_{\mathcal{M},\sigma} & = & [\![p]\!]_{\mathcal{M}}\ \ [\![t_1]\!]_{\mathcal{M},\sigma} \ldots [\![t_n]\!]_{\mathcal{M},\sigma} & \text{for } p/n \in \mathcal{P} \\
[\![\varphi \wedge \psi]\!]_{\mathcal{M},\sigma} & = & \mathit{min}\ \ [\![\varphi]\!]_{\mathcal{M},\sigma}\ \ [\![\psi]\!]_{\mathcal{M},\sigma} & \\
[\![\varphi \vee \psi]\!]_{\mathcal{M},\sigma} & = & \mathit{max}\ \ [\![\varphi]\!]_{\mathcal{M},\sigma}\ \ [\![\psi]\!]_{\mathcal{M},\sigma} & \\
[\![\varphi \to \psi]\!]_{\mathcal{M},\sigma} & = & \textbf{if } [\![\varphi]\!]_{\mathcal{M},\sigma} \leqslant [\![\psi]\!]_{\mathcal{M},\sigma} \textbf{ then } 1 \textbf{ else } 0 & \\
[\![\forall\, v.\ \varphi]\!]_{\mathcal{M},\sigma} & = & \textbf{if } [\![\varphi]\!]_{\mathcal{M},\sigma[m/v]} = 1 \text{ for every } m \in \mathcal{M} & \\
 & & \qquad \textbf{then } 1 \textbf{ else } 0 & \\
[\![\exists\, v.\ \varphi]\!]_{\mathcal{M},\sigma} & = & \textbf{if } [\![\varphi]\!]_{\mathcal{M},\sigma[m/v]} = 0 \text{ for every } m \in \mathcal{M} & \\
 & & \qquad \textbf{then } 0 \textbf{ else } 1 &
\end{array}
$$

where $[\![\_]\!]_{\mathcal{M},\sigma} : \textsc{Term}_{\mathcal{F}} \to \mathcal{M}$ is defined as follows:

$$
\begin{array}{lcll}
[\![v]\!]_{\mathcal{M},\sigma} & = & \sigma\, v & \text{for } v \in \mathcal{IV} \\
[\![f\ t_1 \ldots t_n]\!]_{\mathcal{M},\sigma} & = & [\![f]\!]_{\mathcal{M}}\ \ [\![t_1]\!]_{\mathcal{M},\sigma} \ldots [\![t_n]\!]_{\mathcal{M},\sigma} & \text{for } f \in \mathcal{F}.
\end{array}
$$

Semantic definitions

Let $\mathcal{S}$ be a signature, φ, $\psi \in \textsc{Form}_{\mathcal{S}}$, and $\Gamma \subseteq \textsc{Form}_{\mathcal{S}}$.

Definition. An $\mathcal{S}$-structure $\mathcal{M}$ and an $\mathcal{M}$-assignment σ *satisfy* φ exactly when $[\![\varphi]\!]_{\mathcal{M},\sigma} = 1$; they satisfy Γ exactly when they satisfy every formula in Γ.

Definition. φ is a *semantic consequence* of Γ exactly when, for any $\mathcal{S}$-structure $\mathcal{M}$ and $\mathcal{M}$-assignment σ, φ is satisfied by $\mathcal{M}$ and σ if Γ is satisfied by $\mathcal{M}$ and σ. In this case we write $\Gamma \models \varphi$.

Definition. φ is *valid* exactly when $\emptyset \models \varphi$. In this case we also call φ a *tautology* and simply write $\models \varphi$.

Exercise. Prove

$$\models (\forall\, v.\ \neg\varphi) \to \neg(\exists\, v.\ \varphi)$$

Exercise. State and prove the soundness theorem of first-order NJ with respect to the classical semantics.

Heyting arithmetic

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

We write $t_1 \equiv t_2$ for $\texttt{Eq}\ t_1\ t_2$, $t_1 + t_2$ for $\texttt{add}\ t_1\ t_2$, and $t_1 \times t_2$ for $\texttt{mult}\ t_1\ t_2$.

Properties about these constants are postulated by the *Peano axioms*.

Peano axioms: ‘Eq’ is an equivalence relation

The first three axioms make ‘Eq’ an equivalence relation.

$$
\begin{aligned}
\textit{reflexivity} &:= \forall\, \mathtt{x}.\ \mathtt{x} \equiv \mathtt{x} \\
\textit{transitivity} &:= \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \forall\, \mathtt{z}.\ \mathtt{x} \equiv \mathtt{y} \land \mathtt{y} \equiv \mathtt{z} \to \mathtt{x} \equiv \mathtt{z} \\
\textit{symmetry} &:= \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{y} \to \mathtt{y} \equiv \mathtt{x}
\end{aligned}
$$

Peano axioms: constructors

The next three axioms are about `zero` and '`suc`'.

$$\begin{aligned}
\textit{disjointness} &:= \forall\, \mathtt{x}.\ \neg(\mathtt{suc\ x} \equiv \mathtt{zero}) \\
\textit{injectivity} &:= \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \mathtt{suc\ x} \equiv \mathtt{suc\ y} \to \mathtt{x} \equiv \mathtt{y} \\
\textit{congruence} &:= \forall\, \mathtt{x}.\ \forall\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{y} \to \mathtt{suc\ x} \equiv \mathtt{suc\ y}
\end{aligned}$$

Peano axioms: addition and multiplication

The following four axioms characterise '`plus`' and '`mult`'.

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

Peano axioms: induction

Finally there is an *axiom scheme* that generates instances of the induction principle on natural numbers: for every formula φ 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

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

Example: $1 + 1 = 2$

Let $\mathbf{HA}$ be the Peano axioms. We show that
$\mathbf{HA} \vdash_{\mathrm{NJ}} \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc}\ (\mathtt{suc\ zero})$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathbf{HA} \vdash \textit{transitivity}}}{\mathbf{HA} \vdash \forall y.\ \forall z.\ \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv y \land y \equiv z \to \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv z}\,(\forall E)}{\mathbf{HA} \vdash \forall z.\ \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \land \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \equiv z \to \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv z}\,(\forall E)}{\mathbf{HA} \vdash \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \land \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \equiv \mathtt{suc}\ (\mathtt{suc\ zero}) \to \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc}\ (\mathtt{suc\ zero})}\,(\forall E) \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\mathbf{HA} \vdash \textit{additionS}}}{\mathbf{HA} \vdash \forall y.\ \mathtt{suc\ zero} + y \equiv \mathtt{suc}\ (\mathtt{zero} + y)}\,(\forall E)}{\mathbf{HA} \vdash \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero})}\,(\forall E) \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\mathbf{HA} \vdash \textit{congruence}}}{\mathbf{HA} \vdash \forall y.\ \mathtt{zero} + \mathtt{suc\ zero} \equiv y \to \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \equiv \mathtt{suc}\ y}\,(\forall E)}{\mathbf{HA} \vdash \mathtt{zero} + \mathtt{suc\ zero} \equiv \mathtt{suc\ zero} \to \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \equiv \mathtt{suc}\ (\mathtt{suc\ zero})}\,(\forall E) \quad \dfrac{\dfrac{}{\mathbf{HA} \vdash \textit{additionZ}}}{\mathbf{HA} \vdash \mathtt{zero} + \mathtt{suc\ zero} \equiv \mathtt{suc\ zero}}\,(\forall E)}{\mathbf{HA} \vdash \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \equiv \mathtt{suc}\ (\mathtt{suc\ zero})}\,(\to E)}{\mathbf{HA} \vdash \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \land \mathtt{suc}\ (\mathtt{zero} + \mathtt{suc\ zero}) \equiv \mathtt{suc}\ (\mathtt{suc\ zero})}\,(\land I)}{\mathbf{HA} \vdash \mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc}\ (\mathtt{suc\ zero})}\,(\to E)$$

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: $\mathbf{HA} \vdash_{\mathrm{NJ}} \forall\, \mathtt{x}.\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y}$

This requires induction to analyse $\mathtt{x}$.

$$
\dfrac{
\dfrac{}{\mathbf{HA} \vdash \textit{induction}_{\mathtt{x} \equiv \mathtt{zero} \vee \exists \mathtt{y}.\, \mathtt{x} \equiv \mathtt{suc}\, \mathtt{y},\ \mathtt{x}}}
\qquad
\dfrac{
\dfrac{\dfrac{\dfrac{}{\mathbf{HA} \vdash \textit{reflexivity}}}{\mathbf{HA} \vdash \mathtt{zero} \equiv \mathtt{zero}}\,(\forall \mathrm{E})}{\mathbf{HA} \vdash \mathtt{zero} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{zero} \equiv \mathtt{suc}\ \mathtt{y}}\,(\vee \mathrm{IL})
\quad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathbf{HA}, \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y} \vdash \textit{reflexivity}}}{\mathbf{HA}, \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y} \vdash \mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{x}}\,(\forall \mathrm{E})}{\mathbf{HA}, \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y} \vdash \exists\, \mathtt{y}.\ \mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y}}\,(\exists \mathrm{I})}{\mathbf{HA}, \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y} \vdash \mathtt{suc}\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y}}\,(\vee \mathrm{IR})}{\mathbf{HA} \vdash \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y} \to \mathtt{suc}\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y}}\,(\to \mathrm{I})}{\mathbf{HA} \vdash \forall \mathtt{x}.\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y} \to \mathtt{suc}\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y}}\,(\forall \mathrm{I})
}{\mathbf{HA} \vdash (\mathtt{zero} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{zero} \equiv \mathtt{suc}\ \mathtt{y}) \wedge (\forall \mathtt{x}.\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y} \to \mathtt{suc}\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y})}\,(\wedge \mathrm{I})
}{\mathbf{HA} \vdash \forall \mathtt{x}.\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y}}\,(\to \mathrm{E})
$$

Informally:

- We invoke the induction principle on the formula $\varphi := \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y}$ and variable $\mathtt{x}$.
- The first proof obligation $\varphi\,[\mathtt{zero}/\mathtt{x}]$ is discharged by choosing the left-hand side $\mathtt{zero} \equiv \mathtt{zero}$ of ‘$\vee$’ and instantiating *reflexivity*.
- For the second proof obligation $\forall\, \mathtt{x}.\ \varphi \to (\varphi\,[\mathtt{suc}\ \mathtt{x}/\mathtt{x}])$, we choose the right-hand side $\exists\, \mathtt{y}.\ \mathtt{suc}\ \mathtt{x} \equiv \mathtt{suc}\ \mathtt{y}$, supply $\mathtt{x}$ as the witness, and invoke *reflexivity* again.

Theories

Definition. A formula φ is called a *sentence* if *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. $\mathbf{HA}$ is a theory;
$\mathtt{suc\ zero} + \mathtt{suc\ zero} \equiv \mathtt{suc\ (suc\ zero)}$ and
$\forall\, \mathtt{x}.\ \mathtt{x} \equiv \mathtt{zero} \vee \exists\, \mathtt{y}.\ \mathtt{x} \equiv \mathtt{suc\ y}$ are theorems of $\mathbf{HA}$.

(Syntactic) consistency and completeness of theories

Definition. A theory $\mathcal{T}$ is *inconsistent* exactly when $\mathcal{T} \vdash_{\mathrm{NJ}} \bot$; otherwise it is *consistent*.

Theorem. Let $\mathcal{T}$ be a theory. The following statements are equivalent:

- $\mathcal{T}$ is inconsistent;
- there is a sentence φ such that $\mathcal{T} \vdash_{\mathrm{NJ}} \varphi$ and $\mathcal{T} \vdash_{\mathrm{NJ}} \neg\varphi$;
- $\mathcal{T} \vdash_{\mathrm{NJ}} \varphi$ for every sentence φ.

Definition. A theory $\mathcal{T}$ is *complete* exactly when, for every sentence φ, either $\mathcal{T} \vdash_{\mathrm{NJ}} \varphi$ or $\mathcal{T} \vdash_{\mathrm{NJ}} \neg\varphi$.