Soundness of the Lean typing system

Sander Suverkropp Thijs van Loenhout

Radboud University Nijmegen

December 10, 2021

Today's goal

Soundness

There is no proof of $\bot$ that is verified by the Lean kernel.

- Werner: ZFC_ω and CIC_ω equiconsistent
  - $\mathrm{ZFC}_n \vdash \mathrm{Con}(\mathrm{CIC}_{n+1})$
  - $\mathrm{CIC}_{n+2} \vdash \mathrm{Con}(\mathrm{ZFC}_n)$
- Using Werner's construction: $\mathrm{Lean}_{n+2} \vdash \mathrm{Con}(\mathrm{ZFC}_n)$
- Left to do (today): $\mathrm{ZFC}_{n+1} \vdash \mathrm{Con}(\mathrm{Lean}_{n+1})$

Outline

1. Translate language to a ‘proof splitting language’
2. Define a semantics on the proof splitting language
3. Prove soundness using this semantics
4. A remark on type injectivity

Proof splitting

- In $\mathbb{P}$ there is proof irrelevance

$$\frac{\Gamma \vdash p : \mathbb{P} \quad \Gamma \vdash h : p \quad \Gamma \vdash h' : p}{\Gamma \vdash h \equiv h'}$$

Proof splitting

- In $\mathbb{P}$ there is proof irrelevance

$$\frac{\Gamma \vdash p : \mathbb{P} \quad \Gamma \vdash h : p \quad \Gamma \vdash h' : p}{\Gamma \vdash h \equiv h'}$$

- So we split $\mathbb{P}$ from U_n for $n \geq 1$

$$\forall x : e.\ e \quad \lambda x : e.\ e \quad e\ e$$

Proof splitting

- In $\mathbb{P}$ there is proof irrelevance

$$\frac{\Gamma \vdash p : \mathbb{P} \quad \Gamma \vdash h : p \quad \Gamma \vdash h' : p}{\Gamma \vdash h \equiv h'}$$

- So we split $\mathbb{P}$ from U_n for $n \geq 1$

$$\begin{array}{llll} \forall x : e.\ e & \lambda x : e.\ e & e\ e & \text{for } \mathbb{P} \\ \Pi x : e.\ e & \Lambda x : e.\ e & e \cdot e & \text{for } \mathsf{U}_n, n \geq 1 \end{array}$$

New rules

$$e ::= \cdots \mid \forall x : e.\ e \mid \Pi x : e.\ e \mid \lambda x : e.\ e \mid \Lambda x : e.\ e \mid e\ e \mid e \cdot e$$

$$\frac{\Gamma \vdash e_1 : \Pi x : \alpha.\ \beta \quad \Gamma \vdash e_2 : \alpha}{\Gamma \vdash e_1 \cdot e_2 : \beta[e_2/x]}$$

$$\frac{\Gamma \vdash e_1 : \forall x : \alpha.\ \beta \quad \Gamma \vdash e_2 : \alpha}{\Gamma \vdash e_1\ e_2 : \beta[e_2/x]}$$

$$\frac{\Gamma, x : \alpha \vdash e : \beta : \mathsf{U}_n \quad 1 \leq n}{\Gamma \vdash \Lambda x : \alpha.\ e : \Pi x : \alpha.\ \beta}$$

$$\frac{\Gamma, x : \alpha \vdash e : \beta : \mathbb{P}}{\Gamma \vdash \lambda x : \alpha.\ e : \forall x : \alpha.\ \beta}$$

$$\frac{\Gamma \vdash \alpha : \mathsf{U}_{n_1} \quad \Gamma, x : \alpha \vdash \beta : \mathsf{U}_{n_2} \quad 1 \leq n_2}{\Gamma \vdash \Pi x : \alpha.\ \beta : \mathsf{U}_{\max(n_1, n_2)}}$$

$$\frac{\Gamma \vdash \alpha : \mathsf{U}_n \quad \Gamma, x : \alpha \vdash \beta : \mathbb{P}}{\Gamma \vdash \forall x : \alpha.\ \beta : \mathbb{P}}$$

$$\frac{\Gamma, x : \alpha \vdash e : \beta : \mathsf{U}_n \quad 1 \leq n \quad \Gamma \vdash e' : \alpha}{\Gamma \vdash (\Lambda x : \alpha.\ e) \cdot e' \equiv e[e'/x]}$$

$$\frac{\Gamma, x : \alpha \vdash e : \beta : \mathbb{P} \quad \Gamma \vdash e' : \alpha}{\Gamma \vdash (\lambda x : \alpha.\ e)\ e' \equiv e[e'/x]}$$

$$\frac{\Gamma \vdash e : \Pi y : \alpha.\ \beta}{\Gamma \vdash \Lambda x : \alpha.\ e \cdot x \equiv e}$$

Level expressions

- Universes are indexed by level expressions

$$\ell ::= u \mid 0 \mid S\ell \mid \max(\ell, \ell) \mid \mathrm{imax}(\ell, \ell)$$

- But for the translation we need to know the exact level

Level expressions

- Universes are indexed by level expressions

$$\ell ::= u \mid 0 \mid S\ell \mid \max(\ell, \ell) \mid \mathrm{imax}(\ell, \ell)$$

- But for the translation we need to know the exact level
- So we fix a universe valuation v

$$\begin{aligned}
[\![u]\!]_v &= v(u) \\
[\![0]\!]_v &= 0 \\
[\![S\ell]\!]_v &= [\![\ell]\!]_v + 1 \\
[\![\max(\ell, \ell')]\!]_v &= \max([\![\ell]\!]_v, [\![\ell']\!]_v) \\
[\![\mathrm{imax}(\ell, \ell')]\!]_v &= \begin{cases} 0 & \text{if } [\![\ell']\!]_v = 0 \\ \max([\![\ell]\!]_v, [\![\ell']\!]_v) & \text{if } [\![\ell']\!]_v \neq 0 \end{cases}
\end{aligned}$$

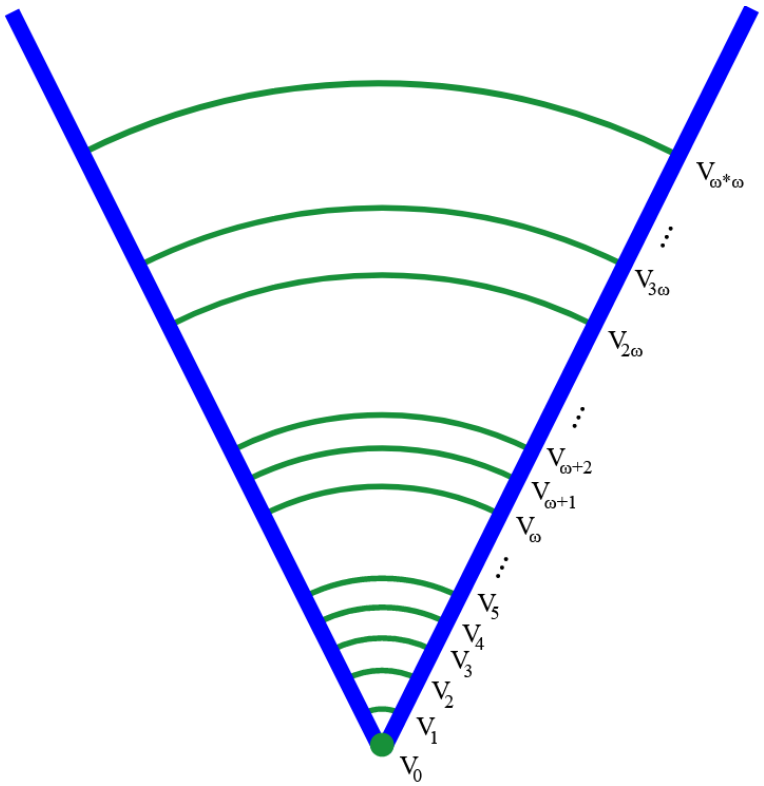
Helper functions

- We can define two functions lvl and sort
- $\mathsf{lvl}_v(\Gamma \vdash \alpha)$, such that $\Gamma \vdash \alpha : \mathsf{U}_\ell$ implies $[\![\ell]\!]_v = \mathsf{lvl}_v(\Gamma \vdash \alpha)$
- $\mathsf{sort}_v(\Gamma \vdash e)$, such that if $\Gamma \vdash e : \alpha$, then $\mathsf{sort}(\Gamma \vdash e) = \mathsf{lvl}(\Gamma \vdash \alpha)$

Translation

- $\langle x \rangle_\Gamma = x$
- $\langle \mathsf{U}_\ell \rangle_\Gamma = \mathsf{U}_{[\![\ell]\!]}$
- $\langle e_1\ e_2 \rangle_\Gamma = \begin{cases} \langle e_1 \rangle_\Gamma\ \langle e_2 \rangle_\Gamma & \text{if } \mathsf{sort}(\Gamma \vdash e_1) = 0 \\ \langle e_1 \rangle_\Gamma \cdot \langle e_2 \rangle_\Gamma & \text{if } \mathsf{sort}(\Gamma \vdash e_1) \geq 1 \end{cases}$
- $\langle \lambda x : \alpha.\ e \rangle_\Gamma = \begin{cases} \lambda x : \langle \alpha \rangle_\Gamma.\ \langle e \rangle_{\Gamma, x:\alpha} & \text{if } \mathsf{sort}(\Gamma \vdash e) = 0 \\ \Lambda x : \langle \alpha \rangle_\Gamma.\ \langle e \rangle_{\Gamma, x:\alpha} & \text{if } \mathsf{sort}(\Gamma \vdash e) \geq 1 \end{cases}$
- $\langle \forall x : \alpha.\ \beta \rangle_\Gamma = \begin{cases} \forall x : \langle \alpha \rangle_\Gamma.\ \langle \beta \rangle_{\Gamma, x:\alpha} & \text{if } \mathsf{lvl}(\Gamma \vdash \beta) = 0 \\ \Pi x : \langle \alpha \rangle_\Gamma.\ \langle e \rangle_{\Gamma, x:\alpha} & \text{if } \mathsf{lvl}(\Gamma \vdash \beta) \geq 1 \end{cases}$
- Other terms are translated simply by translating their parts.

Intermezzo: Inaccessible cardinals



Inaccessible Cardinals

If κ an inaccessible cardinal, then V_κ a model for ZFC.

Gödel: ZFC cannot prove the existence of inaccessible cardinals!

From types to sets

- Fix a sequence $(\kappa_n)_{n\in\mathbb{N}}$ of strong limit cardinals. It is n-correct if κ_i is inaccessible for all $i < n$.
- Define $U_0 = \{\varnothing, \{\bullet\}\}$, $U_{n+1} = V_{\kappa_n}$
- $[\![\Gamma]\!]$: a set of lists of types
- $[\![\Gamma \vdash e]\!]$: a total function on $[\![\Gamma]\!]$

Examples

- $[\![\Gamma \vdash x]\!]_\gamma = \pi_i(\gamma)$, where x is the ith variable in the context.
- $[\![\cdot]\!] = \{()\}$
- $[\![\Gamma, x : \alpha]\!] = \sum_{\gamma \in [\![\Gamma]\!]} [\![\Gamma \vdash \alpha]\!]_\gamma$
- $[\![\Gamma \vdash \mathsf{U}_n]\!]_\gamma = U_n$
- $[\![\Gamma \vdash e_1\ e_2]\!]_\gamma = \bullet$
- $[\![\Gamma \vdash \lambda x : \alpha.\ e]\!]_\gamma = \bullet$
- $[\![\Gamma \vdash \bot]\!]_\gamma = \emptyset$

Examples

- $[\![\Gamma \vdash e_1 \cdot e_2]\!]_\gamma = [\![\Gamma \vdash e_1]\!]_\gamma([\![\Gamma \vdash e_2]\!]_\gamma)$
- $[\![\Gamma \vdash \Lambda x : \alpha.\ e]\!]_\gamma = (x \in [\![\Gamma \vdash \alpha]\!]_\gamma \mapsto [\![\Gamma, x : \alpha \vdash e]\!]_{(\gamma,x)})$
- Denote with $[p]$ the set $\{x \in \{\bullet\} \mid p\}$. Then:

$$[\![\Gamma \vdash \forall x : \alpha.\ \beta]\!]_\gamma = \{\bullet\} \cap \bigcap_{x \in [\![\Gamma \vdash \alpha]\!]_\gamma} [\![\Gamma, x : \alpha \vdash \beta]\!]_{(\gamma,x)}$$
$$= [\forall x \in [\![\Gamma \vdash \alpha]\!]_\gamma, \bullet \in [\![\Gamma, x : \alpha \vdash \beta]\!]_{(\gamma,x)}]$$

- $[\![\Gamma \vdash \Pi x : \alpha.\ \beta]\!]_\gamma = \prod_{x \in [\![\Gamma \vdash \alpha]\!]_\gamma} [\![\Gamma, x : \alpha \vdash \beta]\!]_{(\gamma,x)}$

W-types in ZFC

Recall: W-types

$$\mathsf{W}a : A.B := \mu w : \mathsf{U}_l.(\mathsf{sup} \ : \forall a : A.(B \to w) \to w)$$

W-types in ZFC

Recall: W-types

$$\mathsf{W}a : A.B := \mu w : \mathsf{U}_l.(\mathsf{sup} \ : \forall a : A.(B \to w) \to w)$$

In ZFC: if A is a set, B a set indexed by $a \in A$, then:

$$\mathsf{W}_{a \in A} B(a) := \text{“the smallest set } W \text{ such that } (a, f) \in W \text{ whenever } a \in A \text{ and } f : B(a) \to W\text{”}$$

$$[\![\Gamma \vdash Wa : A.B]\!]_\gamma = \mathsf{W}_{a \in [\![\Gamma \vdash A]\!]_\gamma} [\![\Gamma, a : A \vdash B]\!]_{(\gamma, x)}$$

W-types in ZFC

Recall: W-types

$$\mathsf{W}a : A.B := \mu w : \mathsf{U}_l.(\mathsf{sup} \ : \forall a : A.(B \to w) \to w)$$

In ZFC: if A is a set, B a set indexed by $a \in A$, then:

$$\mathsf{W}_{a \in A} B(a) := \text{“the smallest set } W \text{ such that } (a, f) \in W \text{ whenever } a \in A \text{ and } f : B(a) \to W\text{”}$$

$$[\![\Gamma \vdash Wa : A.B]\!]_\gamma = \mathsf{W}_{a \in [\![\Gamma \vdash A]\!]_\gamma} [\![\Gamma, a : A \vdash B]\!]_{(\gamma, x)}$$

Claim

U_{n+1} is closed under W-types if the κ sequence is $(n+1)$-correct

Proof

Lemma

- (Weakening) If $\Gamma \vdash e : \alpha$ and $\vdash \Gamma, \Delta$ ok, and $(\gamma, \delta) \in [\![\Gamma, \Delta]\!]$, then $[\![\Gamma, \Delta \vdash e]\!]_{\gamma,\delta} = [\![\Gamma \vdash e]\!]_{\gamma}$.
- (Substitution) If $\Gamma, x : \alpha \vdash e_1 : \beta$, $\Gamma \vdash e_2 : \alpha$, $\gamma \in [\![\Gamma]\!]$, and $z := [\![\Gamma \vdash e_2]\!]_{\gamma} \in [\![\Gamma \vdash \alpha]\!]_{\gamma}$, then $[\![\Gamma \vdash e_1[e_2/x]]\!]_{\gamma} = [\![\Gamma, x : \alpha \vdash e_1]\!]_{(\gamma,z)}$.

Proof

Theorem

- *If* $\Gamma \vdash \alpha : \mathbb{P}$, *then* $[\![\Gamma \vdash \alpha]\!]_\gamma \subseteq \{\bullet\}$.
- *If* $\Gamma \vdash e : \alpha$ *and* $\mathsf{lvl}(\Gamma \vdash \alpha) = 0$, *then* $[\![\Gamma \vdash e]\!]_\gamma = \bullet$.
- *If* $\Gamma \vdash e : \alpha$, *then there exists a* n *such that if the* κ *sequence is* n*-correct, then for all* $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash e]\!]_\gamma \in [\![\Gamma \vdash \alpha]\!]_\gamma$.
- *If* $\Gamma \vdash e \equiv e'$, *then there exists a* n *such that if the* κ *sequence is* n*-correct, then for all* $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash e]\!]_\gamma = [\![\Gamma \vdash e']\!]_\gamma$.

Proof

Theorem

- *If* $\Gamma \vdash \alpha : \mathbb{P}$, *then* $[\![\Gamma \vdash \alpha]\!]_\gamma \subseteq \{\bullet\}$.
- *If* $\Gamma \vdash e : \alpha$ *and* $\mathsf{lvl}(\Gamma \vdash \alpha) = 0$, *then* $[\![\Gamma \vdash e]\!]_\gamma = \bullet$.
- *If* $\Gamma \vdash e : \alpha$, *then for all* $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash e]\!]_\gamma \in [\![\Gamma \vdash \alpha]\!]_\gamma$.
- *If* $\Gamma \vdash e \equiv e'$, *then for all* $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash e]\!]_\gamma = [\![\Gamma \vdash e']\!]_\gamma$.

$$\frac{\Gamma \vdash \alpha : \mathsf{U}_n \quad \Gamma \vdash e : \beta}{\Gamma, x : \alpha \vdash e : \beta} \qquad \frac{\Gamma \vdash \alpha : \mathsf{U}_n}{\Gamma, x : \alpha \vdash x : \alpha}$$

$$\frac{}{\vdash \mathsf{U}_n : \mathsf{U}_{n+1}} \qquad \frac{\Gamma \vdash e : \alpha \quad \Gamma \vdash \alpha \equiv \beta}{\Gamma \vdash e : \beta}$$

Proof

Theorem

- *If* $\Gamma \vdash \alpha : \mathbb{P}$, *then* $[\![\Gamma \vdash \alpha]\!]_\gamma \subseteq \{\bullet\}$.
- *If* $\Gamma \vdash e : \alpha$ *and* $\mathsf{lvl}(\Gamma \vdash \alpha) = 0$, *then* $[\![\Gamma \vdash e]\!]_\gamma = \bullet$.
- *If* $\Gamma \vdash e : \alpha$, *then for all* $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash e]\!]_\gamma \in [\![\Gamma \vdash \alpha]\!]_\gamma$.
- *If* $\Gamma \vdash e \equiv e'$, *then for all* $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash e]\!]_\gamma = [\![\Gamma \vdash e']\!]_\gamma$.

$$\frac{\Gamma \vdash e_1 : \forall x : \alpha.\ \beta \quad \Gamma \vdash e_2 : \alpha}{\Gamma \vdash e_1\ e_2 : \beta[e_2/x]}$$

$$\frac{\Gamma \vdash \alpha : \mathsf{U}_\ell \quad \Gamma, x : \alpha \vdash \beta : \mathsf{U}_{\ell'}}{\Gamma \vdash \mathsf{W}x : \alpha.\ \beta : \mathsf{U}_{\mathsf{max}(\ell,\ell',1)}}$$

Proof

Corollary

If $\mathrm{ZFC} + \{$*there are* n *inaccessible cardinals* $\mid n \in \omega\}$ *is consistent, then so is Lean. That is, there is no proof of* $\bot$ *that is verified by the Lean kernel.*

Proof.

- Suppose $\Vdash e : \bot$
- Then $\vdash e : \bot$
- Let v be the universe valuation that sets every variable to 0
- Let $(\kappa_i)_{i \in \omega}$ be a cardinal sequence which is n-correct
- Then $\vdash \langle e \rangle_{v,.} : \bot$
- Then $[\![\vdash \langle e \rangle]\!]_{()} \in [\![\vdash \bot]\!]_{()} = \emptyset$ □

Type Injectivity

- Accidental collapse of types into the same set
- Solution: set of ‘tagged types’

Obligatory Cat Picture