Interactive Proofs for Matching Logic, using Coq

Péter Bereczky [1] **Dániel Horpácsi** [1] **Jan Tušil** [2, 3]

[1] Eötvös Loránd University, Hungary

[2] Masaryk University, Brno, Czech Republic

[3] RuntimeVerification, Inc

February 9, 2023

Previous work

Previous work[1]:

- Syntax
- Semantics
- Proof system
- Soundness of proof system

Now, let us do matching logic proofs!

[1] Bereczky et al., "Mechanizing Matching Logic in Coq."

Hilbert-style proof system of Matching logic

Proof Rule Names	*Proof Rules*	*Proof Rule Names*	*Proof Rules*
(Proposition 1)	$\varphi_1 \to (\varphi_2 \to \varphi_1)$	(Proposition 2)	$(\varphi_1 \to (\varphi_2 \to \varphi_3)) \to (\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3)$
(Proposition 3)	$((\varphi \to \bot) \to \bot) \to \varphi$	(Modus Ponens)	$\dfrac{\varphi_1 \quad \varphi_1 \to \varphi_2}{\varphi_2}$
(∃-Quantifier)	$\varphi[y/x] \to \exists x \,.\, \varphi$	(∃-Generalization)	$\dfrac{\varphi_1 \to \varphi_2}{(\exists x \,.\, \varphi_1) \to \varphi_2}$ with $x \notin FEV(\varphi_2)$
(Propagation$_\bot$)	$C[\bot] \to \bot$	(Propagation$_\vee$)	$C[\varphi_1 \vee \varphi_2] \to C[\varphi_1] \vee C[\varphi_2]$
(Propagation$_\exists$)	$C[\exists x \,.\, \varphi] \to \exists x \,.\, C[\varphi]$ if $x \notin FEV(C)$		
(Framing)	$\dfrac{\varphi_1 \to \varphi_2}{C[\varphi_1] \to C[\varphi_2]}$		
(Substitution)	$\dfrac{\varphi}{\varphi[\psi/X]}$	(Pre-Fixpoint)	$\varphi[(\mu X \,.\, \varphi)/X] \to \mu X \,.\, \varphi$
(Knaster-Tarski)	$\dfrac{\varphi_1[\varphi_2/X] \to \varphi_2}{(\mu X \,.\, \varphi_1) \to \varphi_2}$		
(Existence)	$\exists x \,.\, x$	(Singleton)	$\neg(C_1[x \wedge \varphi] \wedge C_2[x \wedge \neg\varphi])$

Drawbacks

- Gap between human reasoning and the proof system.
- No ”deduction theorem” (moving a LHS of an implication into the theory)

A simple proof

$$\vdash (a \wedge b) \rightarrow (b \wedge a)$$

A simple proof

$$\vdash (a \land b) \to (b \land a)$$

$$\Uparrow$$

$$\{(a \land b)\} \vdash (b \land a)$$

$$\Uparrow$$

$$\{(a \land b)\} \vdash b \qquad \{(a \land b)\} \vdash a$$

$$\Uparrow$$

$$\{(a \land b)\} \vdash (a \land b)$$

Another variant

$$\vdash (a \land b) \to (b \land a)$$

Another variant

$$\vdash (a \land b) \to (b \land a)$$

$$\Uparrow$$

$$\{(a \land b)\} \vdash (b \land a)$$

$$\Uparrow$$

$$\{a, b\} \vdash (b \land a)$$

$$\Uparrow$$

$$\{a, b\} \vdash b \qquad \{a, b\} \vdash a$$

Question

Can we have a conceptually same proof in matching logic?

- Without existence of general deduction theorem?
- Using the existing proof system?
- in Coq?

Question

Can we have a conceptually same proof in matching logic?

- Without existence of general deduction theorem?
- Using the existing proof system?
- in Coq?

Yes.

A Natural Deduction Sequent Calculus

A *sequent* is a quadruple

$$\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \psi \,,$$

(derivable using rules shown later),
where

- Γ is a (possibly infinite) set of matching logic formulas, called a *(global) theory*;
- Δ is a finite (comma-separated) list of matching logic formulas, called a *basic local context* (or just *local context*);
- ψ is a matching logic formula, called *conclusion*; and
- *c* is a *proof constraint* from the set $\mathcal{C}$.

Have a cake and eat it

Goal: $\vdash_{\mathcal{H}} (a \wedge b) \to (b \wedge a)$

Theorem (Soundness, Hilbert proof generation)

$$\Gamma \blacktriangleright_{\top_{\mathcal{C}}} [] \vdash_{\mathcal{N}} \psi \implies \Gamma \vdash_{\mathcal{H}} \psi\,.$$

$$\frac{\Gamma \blacktriangleright_c \Delta, \varphi \vdash_{\mathcal{N}} \psi}{\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \varphi \to \psi} \to_i \qquad \frac{\Gamma \blacktriangleright_c \Delta_1, \varphi_1, \varphi_2, \Delta_2 \vdash_{\mathcal{N}} \psi}{\Gamma \blacktriangleright_c \Delta_1, \varphi_1 \wedge \varphi_2, \Delta_2 \vdash_{\mathcal{N}} \psi} \wedge_e$$

$$\frac{\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \varphi_1 \qquad \Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \varphi_2}{\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \varphi_1 \wedge \varphi_2} \wedge_i \qquad \frac{}{\Gamma \blacktriangleright_c \Delta_1, \varphi, \Delta_2 \vdash_{\mathcal{N}} \varphi} \text{Hyp}$$

What?

$$\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \psi\,,$$

1. We cheat, of course.

What?

$$\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \psi \,,$$

1. We cheat, of course.
2. Global (theory) and local contexts have different semantics.

What?

$$\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \psi \,,$$

1. We cheat, of course.
2. Global (theory) and local contexts have different semantics.
3. Semantics: if every model element matches every formula of Γ, then every model element which matches every formula of Δ matches also ψ.

What?

$$\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \psi \,,$$

1. We cheat, of course.
2. Global (theory) and local contexts have different semantics.
3. Semantics: if every model element matches every formula of Γ, then every model element which matches every formula of Δ matches also ψ.

Lemma (Correspondence lemma)

$$\Gamma \blacktriangleright_c \varphi_1, \ldots, \varphi_k \vdash_{\mathcal{N}} \psi \implies \Gamma \vdash^c_{\mathcal{H}} \varphi_1 \to \ldots \to \varphi_k \to \psi$$

Back to Hilbert

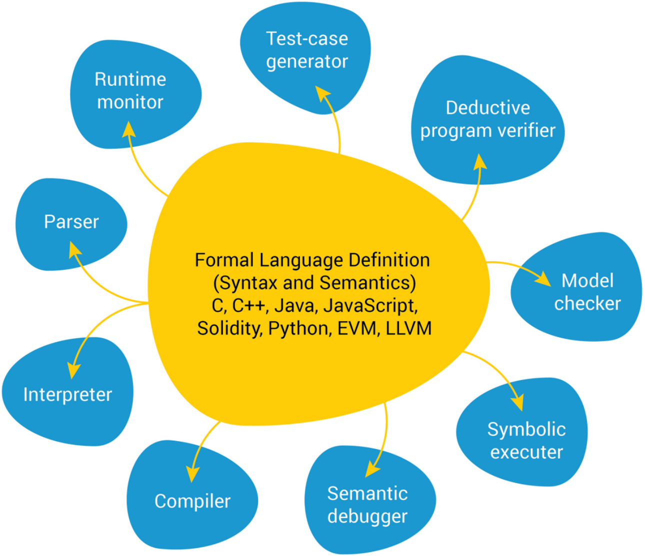
$$\frac{\Gamma \blacktriangleright_c \Delta \vdash_{\mathcal{N}} \varphi \to \psi}{\Gamma \blacktriangleright_c \Delta, \varphi \vdash_{\mathcal{N}} \psi} \to_e \qquad \frac{(\Gamma \vdash^c_{\mathcal{H}} \psi)}{\Gamma \blacktriangleright_c [] \vdash_{\mathcal{N}} \psi}$$

Coq Implementation

`https://github.com/harp-project/AML-Formalization`

An interactive theorem prover inside an interactive theorem prover.

$\mathbb{K}$ Framework



Future Challenges

Conclusion

Locally Nameless

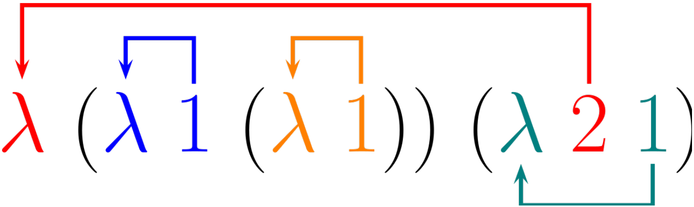


Figure: De Bruijn indexing.
https://en.wikipedia.org/wiki/De_Bruijn_index

Future Challenges

Conclusion

Conclusion

A paper is in preparation.

Questions!

MUNI
FACULTY
OF INFORMATICS