Concrete Semantics with Coq and CoqHammer

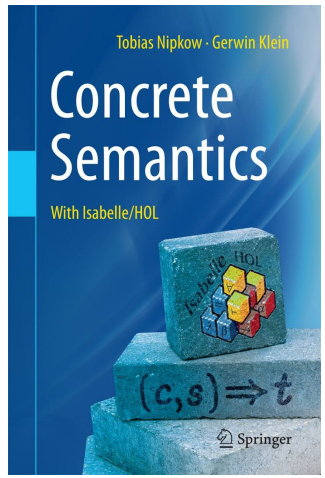
Łukasz Czajka[2], **Burak Ekici**[1], Cezary Kaliszyk[1]

[1]University of Innsbruck, Austria

[2]University of Copenhagen, Denmark

August 15, 2018

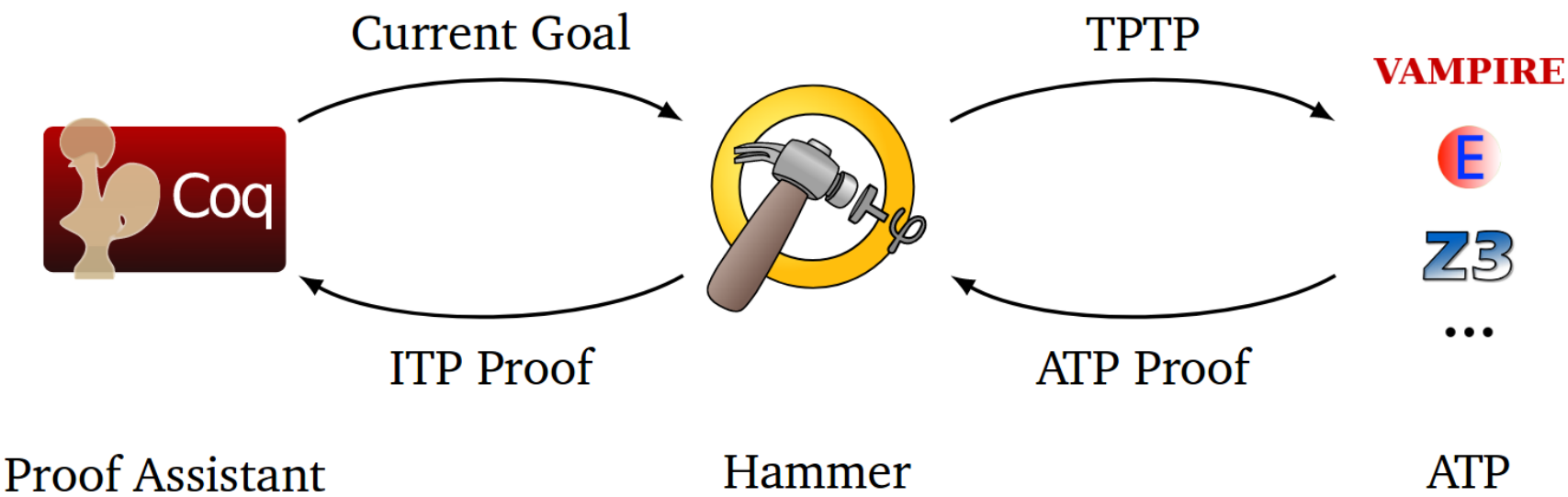
This work ...



... aims to evaluate of CoqHammer over some theories accompanying Concrete Semantics book.

1. reformalization of such theories in Coq,
2. run CoqHammer on goals, and test if we can achieve a similar brevity of the formal text in comparison with the original text.

CoqHammer: the overview



We have ...

... reproven approximately 100 theorems from

- Star, AExp, BExp, ASM, Com, Big_Step, Hoare, Small_Step, Compiler and Compiler2

Isabelle/HOL theories in Coq, using CoqHammer calls and some Ltac based decision procedures.

An example

```
Lemma strengthen_pre: ∀ (P P' Q: assn) c,
  (entails P' P) → hoaret P c Q → hoaret P' c Q.
Proof.
  hobvious Empty (@conseq) (@entails)
Qed.
```

lemma strengthen-pre:
⟦ ∀s. P s ⟶ P s; ⊢$_t$ {P} c {Q} ⟧ ⟹ ⊢$_t$ {P} c {Q}
by (metis conseq)

Benchs & Conclusion

	# of lines	# of words	# of tactics	# of hammer calls	time(secs)
Isabelle/HOL	2806	11278	544	-	31
Coq	3493	19292	1190	468	149

The number of Coq tactics we used to get the same lemmas proven is almost twice in number, as opposed to Isabelle/HOL, but about half of which benefits from the automation techniques that CoqHammer comes with.

Thank you for your attention!

&

Questions?