

# A Solution to the CIV Challenge in Isabelle

Iavor S. Diatchki  
diatchki@galois.com

Galois Connections, Inc.

May 22, 2007

# The CIV Challenge

- ▶ **C**ompiler **I**mplementation **V**erification
- ▶ Andrew W. Appel and Xavier Leroy
  - “*A List-Machine Benchmark for Mechanized Metatheory*”
- ▶ Defines a simple list-machine language (in the spirit of TAL)
- ▶ The challenge:
  - ▶ Formalize the language
  - ▶ Prove that its type system is sound
  - ▶ Implement a type checking algorithm (**todo**)
  - ▶ Prove that the algorithm is sound (and complete?) (**todo**)

# Overview

- ▶ Language:
  - ▶ Syntax: what is a program?
  - ▶ Semantics: what do programs do?
  - ▶ Programs that do not crash.
- ▶ Type System:
  - ▶ Types and sub-typing.
  - ▶ Associating types with programs.
  - ▶ Associating types with machine values (or the semantics of types)
- ▶ Soundness of the Type System:

*Type-correct programs do not crash.*

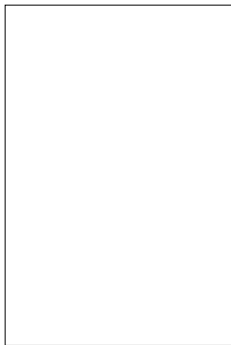
# Hardware

Instruction Pointer

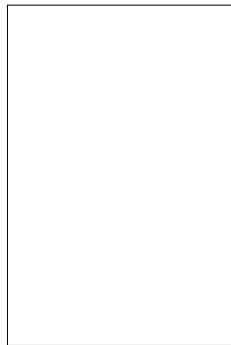


Data Registers

V1	V2	V3	...
----	----	----	-----



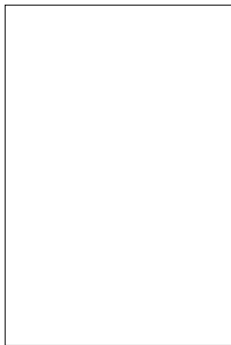
Code Region



Data Region

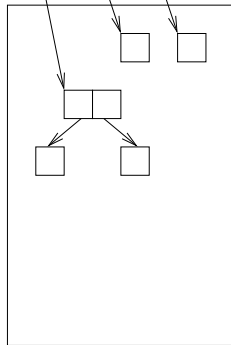
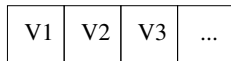
# Hardware

Instruction Pointer



Code Region

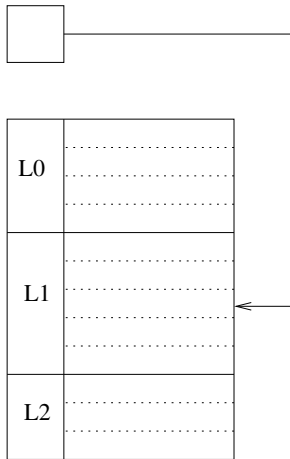
Data Registers



Data Region

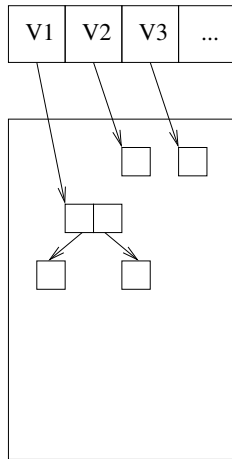
# Hardware

Instruction Pointer



Code Region

Data Registers



Data Region