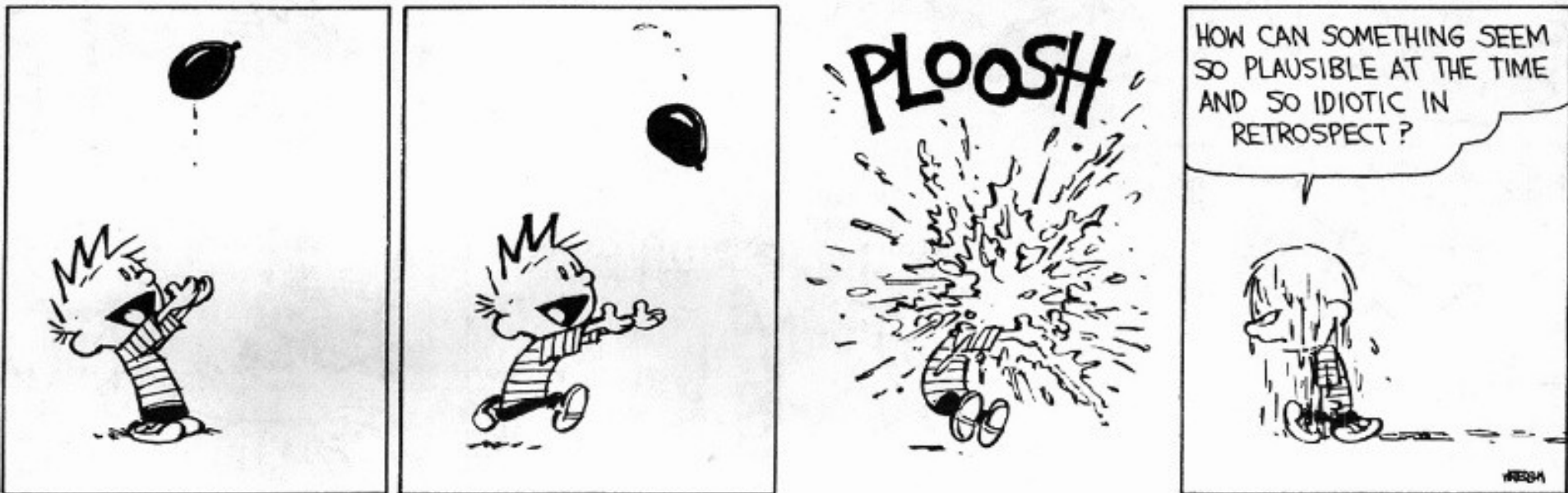


# Monomorphic Type Systems



# The Reading

- Explain the Xavier Leroy article to me ...

The correctness of the translation follows from a simulation argument between the executions of the Cminor source and the RTL translation, proved by induction on the Cminor evaluation derivation. In the case of expressions, the simulation property is summarized by the following diagram:

$$\begin{array}{ccc} sp, L, a, E, M & \xrightarrow{I \wedge P} & sp, n_s, R, M \\ \Downarrow & & \vdots^* \\ sp, L, v, E', M' & \xrightarrow{I \wedge Q} & sp, n_d, R', M' \end{array}$$

*On the choice of semantics* We used **big-step semantics** for the source language, “mixed-step” semantics for the intermediate languages, and **small-step semantics** for the target language. A consequence of this choice is that our semantic preservation theorems hold only for **terminating source programs**: they all have premises of the form **“if the source program evaluates to result  $r$ ”**, which do not hold for non-terminating programs. This is unfortunate for

- How did he do register allocation?

# One-Slide Summary

- The **simply-typed lambda calculus** is an important tool for studying and designing new programming language features.
- **Soundness** is a critical property of any type system (if  $\cdot \vdash e : \tau$  and  $e \Downarrow v$  then  $\cdot \vdash v : \tau$ ). We can prove it by induction.
- We can extend the type system to handle **tuples**, **unions**, and imperative **references**. We model meaning with **contextual** operational semantics.

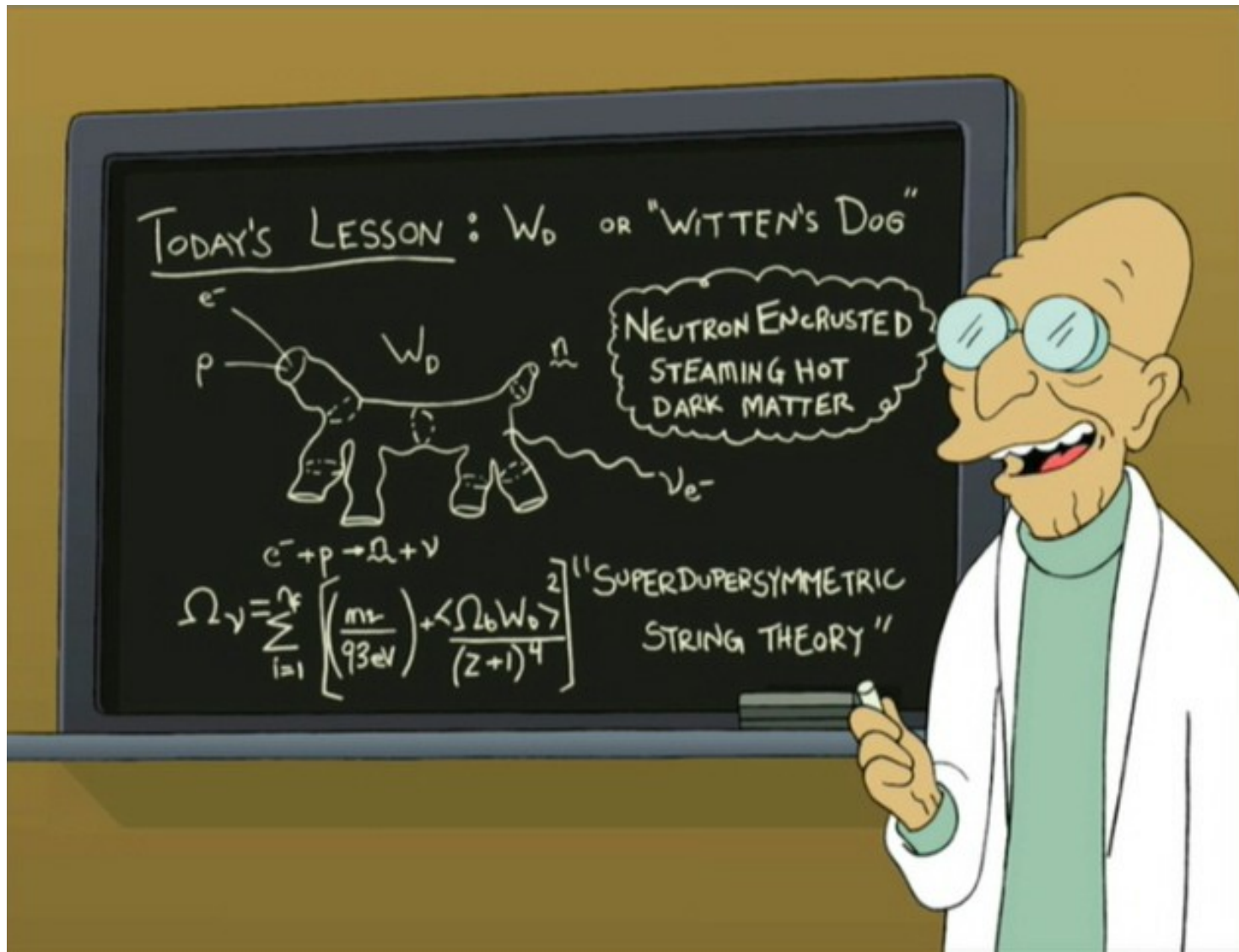
# Type Soundness for $F_1$

What does  
this mean?

- Theorem: **If  $\cdot \vdash e : \tau$  and  $e \Downarrow v$  then  $\cdot \vdash v : \tau$** 
  - Also called, subject reduction theorem, type preservation theorem
- This is one of the most important sorts of theorems in PL
- Whenever you make up a new safe language you are expected to prove this
  - Examples: Vault, TAL, CCured, ...

# How Might We Prove It?

- Theorem: **If  $\cdot \vdash e : \tau$  and  $e \Downarrow v$  then  $\cdot \vdash v : \tau$**



# Proof Approaches To Type Safety

- Theorem: **If  $\cdot \vdash e : \tau$  and  $e \Downarrow v$  then  $\cdot \vdash v : \tau$**
- Try to prove by **induction on  $e$** 
  - Won't work because  $[v_2/x]e'_1$  in the evaluation of  $e_1 e_2$
  - Same problem with induction on  $\cdot \vdash e : \tau$
- Try to prove by induction on  $\tau$ 
  - Won't work because  $e_1$  has a “bigger” type than  $e_1 e_2$
- ???

# Proof Approaches To Type Safety

- Theorem: **If  $\cdot \vdash e : \tau$  and  $e \Downarrow v$  then  $\cdot \vdash v : \tau$**
- Try to prove by **induction on  $e$** 
  - Won't work because  $[v_2/x]e'_1$  in the evaluation of  $e_1 e_2$
  - Same problem with induction on  $\cdot \vdash e : \tau$
- Try to prove by induction on  $\tau$ 
  - Won't work because  $e_1$  has a “bigger” type than  $e_1 e_2$
- **Try to prove by induction on  $e \Downarrow v$** 
  - To address the issue of  $[v_2/x]e'_1$
  - **This is it!**

# Type Soundness Proof

- Consider the *function application* case

$$\mathcal{E} :: \frac{e_1 \Downarrow \lambda x : \tau_2 . e'_1 \quad e_2 \Downarrow v_2 \quad [v_2/x]e'_1 \Downarrow v}{e_1 e_2 \Downarrow v}$$

and by inversion on the derivation of  $e_1 e_2 : \tau$

$$\mathcal{D} :: \frac{\cdot \vdash e_1 : \tau_2 \longrightarrow \tau \quad \cdot \vdash e_2 : \tau_2}{\cdot \vdash e_1 e_2 : \tau}$$

- From IH on  $e_1 \Downarrow \dots$  we have  $\cdot, x : \tau_2 \vdash e'_1 : \tau$
- From IH on  $e_2 \Downarrow \dots$  we have  $\cdot \vdash v_2 : \tau_2$
- Need to infer that  $\cdot \vdash [v_2/x]e'_1 : \tau$  and use the IH
  - We need a [substitution lemma](#) (by induction on  $e'_1$ )



# Significance of Type Soundness

- The theorem says that the **result of an evaluation has the same type as the initial expression**
- The theorem **does not** say that
  - The evaluation *never gets stuck* (e.g., trying to apply a non-function, to add non-integers, etc.), nor that
  - The evaluation *terminates*
- Even though both of the above facts are true of  $F_1$
- **What formal system of semantics do we use to reason about programs that might not terminate?**

# Significance of Type Soundness

- The theorem says that the **result of an evaluation has the same type as the initial expression**
- The theorem **does not** say that
  - The evaluation *never gets stuck* (e.g., trying to apply a non-function, to add non-integers, etc.), nor that
  - The evaluation *terminates*
- Even though both of the above facts are true of  $F_1$
- We need a ***small-step semantics*** to prove that the execution never gets stuck
- I Assert: the execution always terminates in  $F_1$ 
  - When does the base lambda calculus ever not terminate?

# Small-Step Contextual Semantics for $F_1$

- We define **redexes**

$$r ::= n_1 + n_2 \mid \text{if } b \text{ then } e_1 \text{ else } e_2 \mid (\lambda x:\tau. e_1) v_2$$

- and **contexts**

$$H ::= H_1 + e_2 \quad \mid n_1 + H_2 \quad \mid \text{if } H \text{ then } e_1 \text{ else } e_2 \\ \mid H_1 e_2 \quad \mid (\lambda x:\tau. e_1) H_2 \quad \mid \bullet$$

- and **local reduction rules**

$$n_1 + n_2 \quad \rightarrow \quad n_1 \text{ plus } n_2$$

$$\text{if true then } e_1 \text{ else } e_2 \quad \rightarrow \quad e_1$$

$$\text{if false then } e_1 \text{ else } e_2 \quad \rightarrow \quad e_2$$

$$(\lambda x:\tau. e_1) v_2 \quad \rightarrow \quad [v_2/x]e_1$$

- and one **global reduction rule**

$$H[r] \rightarrow H[e] \quad \text{iff } r \rightarrow e$$

# Decomposition Lemmas for $F_1$

- If  $\cdot \vdash e : \tau$  and  $e$  is not a (final) value then there exist (unique)  $H$  and  $r$  such that  $e = H[r]$ 
  - any well typed expression can be decomposed
  - any well-typed non-value can make progress
- Furthermore, there exists  $\tau'$  such that  $\cdot \vdash r : \tau'$ 
  - the redex is closed and well typed
- Furthermore, there exists  $e'$  such that  $r \rightarrow e'$  and  $\cdot \vdash e' : \tau'$ 
  - local reduction is type preserving
- Furthermore, for any  $e'$ ,  $\cdot \vdash e' : \tau'$  implies  $\cdot \vdash H[e'] : \tau$ 
  - the expression preserves its type if we replace the redex with an expression of same type

# Type Safety of $F_1$

- Type preservation theorem

- If  $\cdot \vdash e : \tau$  and  $e \rightarrow e'$  then  $\cdot \vdash e' : \tau$
- Follows from the decomposition lemma

- Progress theorem

- If  $\cdot \vdash e : \tau$  and  $e$  is not a value then there exists  $e'$  such that  $e$  can make progress:  $e \rightarrow e'$

- Progress theorem says that execution can make progress *on a well typed expression*

- From type preservation we know the execution of well *typed expressions never gets stuck*

- This is a (very!) common way to *state and prove type safety* of a language

# What's Next?

- We've got the basic simply-typed monomorphic lambda calculus
- Now let's make it **more complicated** ...
- By adding features!



# Product Types: Static Semantics

- Extend the syntax with (binary) tuples

$$e ::= \dots \mid (e_1, e_2) \mid \text{fst } e \mid \text{snd } e$$
$$\tau ::= \dots \mid \tau_1 \times \tau_2$$

- This language is sometimes called  $F_1^\times$

- Same typing judgment  $\Gamma \vdash e : \tau$

$$\frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash (e_1, e_2) : \tau_1 \times \tau_2}$$
$$\frac{\Gamma \vdash e : \tau_1 \times \tau_2}{\Gamma \vdash \text{fst } e : \tau_1}$$
$$\frac{\Gamma \vdash e : \tau_1 \times \tau_2}{\Gamma \vdash \text{snd } e : \tau_2}$$

# Dynamic Semantics and Soundness

- New form of values:  $v ::= \dots \mid (v_1, v_2)$

- New (big step) evaluation rules:

$$\frac{e_1 \Downarrow v_1 \quad e_2 \Downarrow v_2}{(e_1, e_2) \Downarrow (v_1, v_2)}$$

$$\frac{e \Downarrow (v_1, v_2)}{\text{fst } e \Downarrow v_1} \quad \frac{e \Downarrow (v_1, v_2)}{\text{snd } e \Downarrow v_2}$$

- New contexts:  $H ::= \dots \mid (H_1, e_2) \mid (v_1, H_2) \mid \text{fst } H \mid \text{snd } H$

- New redexes:

$$\text{fst } (v_1, v_2) \rightarrow v_1$$

$$\text{snd } (v_1, v_2) \rightarrow v_2$$

- Type soundness holds just as before



## Q: General (454 / 842)

- In traditional logic this is an inference in which one proposition (the conclusion) necessarily follows from two others (the premises). An overused example is: *"All humans are mortal. Socrates is a human. Therefore, Socrates is a mortal."*

## Q: General (473 / 842)

- Which of the following chemical processes or reactions would be the most difficult to conduct in a high school chemistry lab?
  - Hall-Heroult (Aluminum Extraction) Process
  - Making Nitrocellulose (Guncotton)
  - Making Slime (disodium tetraborate)
  - Thermite Reaction (which reaches 5000(F))

**Q: Games (534 / 842)**

- **Each face of this 1974 six-sided plastic puzzle is subdivided into nine smaller faces, each of which can be one of six colors.**

# Computer Science

- This American Turing award winner is known for foundational work in data structures and algorithms. Examples include off-line least common ancestors, strongly connected components, the Fibonacci heap, the splay tree, and the disjoint-set data structure. This prolific author has about 300 refereed publications.

## Q: Games (547 / 842)

- This viscoelastic silicone plastic "clay" came out of efforts to find a rubber substitute in World War II. It is now sold in plastic eggs as a toy for children. It bounces and can absorb the ink from newsprint. It was also used by the crew of Apollo 8 to secure tools in zero gravity.

# General PL Feature Plan

- The general plan for language feature design
- You **invent** a new feature (tuples)
- You add it to the **lambda calculus**
- You **invent typing rules** and **opsem rules**
- You extend the basic **proof of type safety**
- You declare moral victory, and milling throngs of cheering admirers wait to carry you on their shoulders to be knighted by the Queen, etc.

# Records

- Records are like tuples with labels (w00t!)

- New form of expressions

$e ::= \dots \mid \{L_1 = e_1, \dots, L_n = e_n\} \mid e.L$

- New form of values

$v ::= \{L_1 = v_1, \dots, L_n = v_n\}$

- New form of types

$\tau ::= \dots \mid \{L_1 : \tau_1, \dots, L_n : \tau_n\}$

- ... follows the model of  $F_1^\times$

- typing rules
- derivation rules
- type soundness

“On the board!”



# Sum Types

- We need disjoint union types of the form:
  - either an int or a float
  - either 0 or a pointer
  - either a (binary tree node with two children) or a (leaf)

- New expressions and types

$e ::= \dots \mid \text{injl } e \mid \text{injrl } e \mid$   
 $\text{case } e \text{ of injl } x \rightarrow e_1 \mid \text{injrl } y \rightarrow e_2$

$\tau ::= \dots \mid \tau_1 + \tau_2$

- A value of type  $\tau_1 + \tau_2$  is *either* a  $\tau_1$  or a  $\tau_2$
- Like union in C or Pascal, but safe
  - distinguishing between components is *under compiler control*
- **case** is a *binding operator* (like “let”):  $x$  is bound in  $e_1$  and  $y$  is bound in  $e_2$  (like OCaml’s “match ... with”)



# Examples with Sum Types

- Consider the type unit with a single element called `*` or `()`
- The type integer option defined as “`unit + int`”
  - Useful for optional arguments or return values
    - No argument: `injl *` ( OCaml’s “None”)
    - Argument is 5: `inj r 5` ( OCaml’s “Some(5)”)
  - To use the argument you must test the kind of argument
  - `case arg of injl x ⇒ “no_arg_case” | injr y ⇒ “...y...”`
  - `injl` and `inj r` are tags and case is tag checking
- bool is the union type “`unit + unit`”
  - `true` is `injl *`
  - `false` is `inj r *`
  - `if e then e1 else e2` is `case e of injl x ⇒ e1 | injr y ⇒ e2`

# Static Semantics of Sum Types

- New **typing rules**

$$\frac{\Gamma \vdash e : \tau_1}{\Gamma \vdash \text{injl } e : \tau_1 + \tau_2} \quad \frac{\Gamma \vdash e : \tau_2}{\Gamma \vdash \text{injr } e : \tau_1 + \tau_2}$$

$$\frac{\Gamma \vdash e_1 : \tau_1 + \tau_2 \quad \Gamma, x : \tau_1 \vdash e_l : \tau \quad \Gamma, y : \tau_2 \vdash e_r : \tau}{\Gamma \vdash \text{case } e_1 \text{ of } \text{injl } x \Rightarrow e_l \mid \text{injr } y \Rightarrow e_r : \tau}$$

- Types are **not unique** anymore

`injl 1 : int + bool`

`injl 1 : int + (int → int)`

- this complicates type checking, but it is still doable

# Dynamic Semantics of Sum Types

- New values  $v ::= \dots \mid \text{injl } v \mid \text{injrl } v$
- New evaluation rules

$$\frac{e \Downarrow v}{\text{injl } e \Downarrow \text{injl } v} \quad \frac{e \Downarrow v}{\text{injrl } e \Downarrow \text{injrl } v}$$

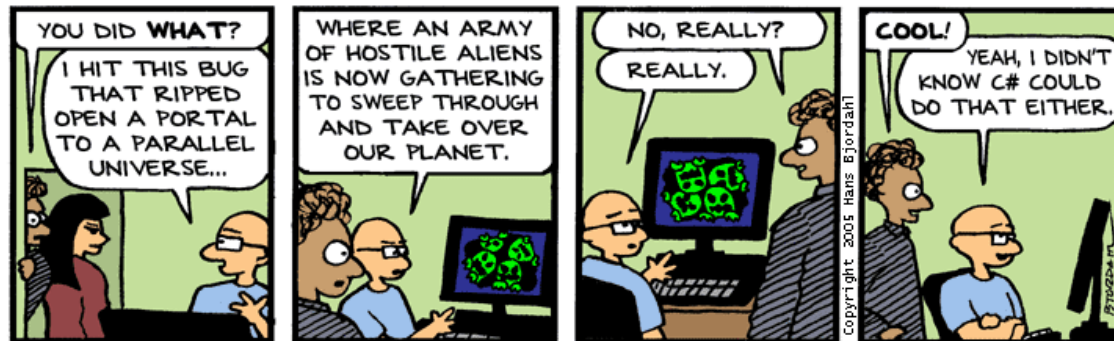
$$\frac{e \Downarrow \text{injl } v \quad [v/x]e_l \Downarrow v'}{\text{case } e \text{ of } \text{injl } x \Rightarrow e_l \mid \text{injrl } y \Rightarrow e_r \Downarrow v'}$$

$$\frac{e \Downarrow \text{injrl } v \quad [v/y]e_r \Downarrow v'}{\text{case } e \text{ of } \text{injl } x \Rightarrow e_l \mid \text{injrl } y \Rightarrow e_r \Downarrow v'}$$

# Type Soundness for $F_1^+$

- Type soundness *still holds*
- No way to use a  $\tau_1 + \tau_2$  inappropriately
- The key is that the **only way to use a  $\tau_1 + \tau_2$  is with case**, which ensures that you are not using a  $\tau_1$  as a  $\tau_2$
- In C or Pascal checking the tag is the responsibility of the programmer!

- Unsafe



# Types for Imperative Features

- So far: types for **pure functional** languages
- Now: types for **imperative features**
- Such types are used to characterize **non-local effects**
  - assignments
  - exceptions
  - typestate
- **Contextual semantics** is useful here
  - Just when you thought it was safe to forget it ...

# Reference Types

- Such types are used for **mutable memory cells**
- Syntax (as in ML)

$e ::= \dots \mid \text{ref } e : \tau \mid e_1 := e_2 \mid ! e$

$\tau ::= \dots \mid \tau \text{ ref}$

Why do I need  $:\tau$ ?

- **ref**  $e : \tau$  - evaluates  $e$ , allocates a new memory cell, stores the value of  $e$  in it and returns the address of the memory cell
  - like malloc + initialization in C, or new in C++ and Java
- **$e_1 := e_2$** , evaluates  $e_1$  to a memory cell and updates its value with the value of  $e_2$
- **! e** - evaluates  $e$  to a memory cell and returns its contents

# Global Effects, Reference Cells

- A reference cell can escape the static scope where it was created

$(\lambda f:\text{int} \rightarrow \text{int ref. } !(f\ 5)) \quad (\lambda x:\text{int. } \text{ref } x : \text{int})$

- The value stored in a reference cell *must be visible from the entire program*
- The “result” of an expression must now include the **changes to the heap** that it makes (cf. IMP’s opsem)
- To model reference cells we must **extend the evaluation model**

# Modeling References

- A heap is a mapping from addresses to values

$$h ::= \cdot \mid h, a \leftarrow v : \tau$$

- $a \in \text{Addresses}$  (Addresses  $\neq \mathbb{Z}$  ?)
- We tag the heap cells with their types
- Types are useful only for static semantics. They are not needed for the evaluation  $\Rightarrow$  are not a part of the implementation
- We call a program an expression with a heap
$$p ::= \text{heap } h \text{ in } e$$
  - The initial program is “heap  $\cdot$  in  $e$ ”
  - Heap addresses act as bound variables in the expression
  - This is a trick that allows easy *reuse of properties of local variables for heap addresses*
    - e.g., we can rename the address and its occurrences at will



# Static Semantics of References

- **Typing rules** for expressions:

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash (\text{ref } e : \tau) : \tau \text{ ref}} \qquad \frac{\Gamma \vdash e : \tau \text{ ref}}{\Gamma \vdash !e : \tau}$$

$$\frac{\Gamma \vdash e_1 : \tau \text{ ref} \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1 := e_2 : \text{unit}}$$

- and for programs

$$\frac{\Gamma \vdash v_i : \tau_i \ (i = 1..n) \quad \Gamma \vdash e : \tau}{\vdash \text{heap } h \text{ in } e : \tau}$$

where  $\Gamma = a_1 : \tau_1 \text{ ref}, \dots, a_n : \tau_n \text{ ref}$

and  $h = a_1 \leftarrow v_1 : \tau_1, \dots, a_n \leftarrow v_n : \tau_n$

# Contextual Semantics for References

- Addresses are values:  $v ::= \dots \mid a$
- New contexts:  $H ::= \text{ref } H \mid H_1 := e_2 \mid a_1 := H_2 \mid ! H$
- No new *local* reduction rules
- But some *new global* reduction rules
  - $\text{heap } h \text{ in } H[\text{ref } v : \tau] \rightarrow \text{heap } h, a \leftarrow v : \tau \text{ in } H[a]$ 
    - where  $a$  is fresh (this models *allocation* - the heap is extended)
  - $\text{heap } h \text{ in } H[! a] \rightarrow \text{heap } h \text{ in } H[v]$ 
    - where  $a \leftarrow v : \tau \in h$  (heap lookup - can we get stuck?)
  - $\text{heap } h \text{ in } H[a := v] \rightarrow \text{heap } h[a \leftarrow v] \text{ in } H[*]$ 
    - where  $h[a \leftarrow v]$  means a heap like  $h$  except that the part “ $a \leftarrow v_1 : \tau$ ” in  $h$  is replaced by “ $a \leftarrow v : \tau$ ” (memory update)
- Global rules are used to *propagate the effects of a write* to the entire program (eval order matters!)

# Example with References

- Consider these (the redex is underlined)
  - heap · in  $(\lambda f:\text{int} \rightarrow \text{int ref. } !(f\ 5))$   $(\lambda x:\text{int. ref } x : \text{int})$
  - heap · in  $!((\lambda x:\text{int. ref } x : \text{int})\ 5)$
  - heap · in  $!(\text{ref } 5 : \text{int})$
  - heap a = 5 : int in !a
  - heap a = 5 : int in 5
- The resulting program has a **useless memory cell**
- An equivalent result would be  
$$\text{heap} \cdot \text{in } 5$$
- This is a simple way to model **garbage collection**

# Homework

- The usual :-)

