Recap

A λ-calculus expression is defined as

\[ e ::= x \quad \text{variable} \]
\[ | \quad \lambda x. e \quad \text{abstraction} \]
\[ | \quad e \ e \quad \text{application} \]

**α-conversion**

\[ \lambda x. e \rightarrow_\alpha \lambda y. e[x \mapsto y] \quad \text{if} \ y \not\in \text{FV}(e) \]

**β-reduction**

\[ (\lambda x. e) \ e' \rightarrow_\beta \ e[x \mapsto e'] \]

**η-conversion**

\[ \lambda x. (e \ x) \rightarrow_\eta e \quad \text{if} \ x \not\in \text{FV}(e) \]
• A $\lambda$-calculus expression is defined as

$$e ::= x \quad \text{variable}$$

$$| \quad \lambda x.e \quad \text{abstraction}$$

$$| \quad e \ e \quad \text{application}$$

$\alpha$-conversion

$$\lambda x.e \rightarrow_\alpha \lambda y.e[x \mapsto y] \quad \text{if } y \notin \text{FV}(e)$$

$\beta$-reduction

$$(\lambda x.e) \ e' \rightarrow_\beta e[x \mapsto e']$$

$\eta$-conversion

$$\lambda x.(e \ x) \rightarrow_\eta e \quad \text{if } x \notin \text{FV}(e)$$
Paradoxes & Types

- One of the original motivations for type theory was to eliminate certain logical paradoxes in untyped \( \lambda \)-calculus.

Russell’s Paradox

- Consider the function \( R \) which negates its argument applied to itself.

\[
R = \lambda x. \text{NOT} (x \ x)
\]

- Now apply \( R \) to itself.

\[
(R \ R) = (\lambda x. \text{NOT} (x \ x)) \ R
= \beta \quad \text{NOT} (R \ R)
\]

- Simply typed-calculus forbids \( x \ x \) with a type system.
“A type system is a tractable syntactic method for proving the absence of certain program behaviors by classifying phrases according to the kinds of values they compute”
Benjamin Pierce, “Types and Programming Languages” (MIT, 2002)
Type System

**Narrow View**

- A mechanism for ensuring that variables only take values from predefined sets
  - e.g. Integers, Strings, Characters
- A mechanism for avoiding unchecked errors
  - by ruling out programs with undefined behaviors
  - by specifying how a program should fail (e.g. NullPointerException)

**Expansive View**

- A light-weight proof system and annotation mechanism for efficiently checking for a specific property of interest
- Address bugs that go beyond corner-cases in the semantics
  - Information flow violations
  - Deadlocks
  - ...
Types

- **Type**: A method of classifying objects (values) in a language
- $x : \tau$ says object $x$ has type $\tau$ or object $x$ belongs to a type $\tau$
- $\tau$ denotes a set of values
- This notion of types is different from types in languages like C, where a type is a storage class specifier

**Type Correctness**

- If $x : \tau$ then only those operations that are appropriate to set $\tau$ may be performed on $x$
- A program is **type correct** if it never performs a wrong operation on an object
  - Add an `Int` and a `Boolean`
  - Head of an `Int`
  - Square root of a `list`
Classification of Type Systems

- **Monomorphic:** Each identifier has exactly one type
- **Polymorphic:** An identifier can have multiple types
- **Static:** Type correctness is checked at compile time
- **Dynamic:** Type correctness is checked at run time

<table>
<thead>
<tr>
<th></th>
<th>static</th>
<th>dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>monomorphic</td>
<td>Pascal</td>
<td></td>
</tr>
<tr>
<td>polymorphic</td>
<td>ML, Haskell, Scala, Java</td>
<td>Lisp, Smalltalk</td>
</tr>
</tbody>
</table>
- Proper type systems provide strong guarantees
  - Scala, ML, Haskell: memory corruption impossible
- Sometimes frustrating: seen as a hurdle
- For some applications (rapid application development) are overly restrictive
  - Dynamic scripting languages (Perl, Tcl, Python, ...)

Type systems: a Discipline for Programming
Static Analysis

• Static type checking is the most widely used form of static analysis

• **Static Analysis:** analyze the program without running it

• Some other type of typical errors that static analysis can catch:
  
  • Security: Buffer overruns, improperly validated input
  • Memory safety: Null dereference, uninitialized data
  • Resource leaks: Memory, OS resources
  • Exceptions: Arithmetic/library/user-defined
  • Encapsulation: Accessing internal data, calling private functions
  • ...

Rice’s Theorem

“Any nontrivial property about the language recognized by a Turing machine is undecidable.”

• Many static analysis techniques are sound but incomplete
Space of Programs

All Programs

Unsafe Programs

Safe Programs

All Programs
Space of Programs

All Programs

Unsafe Programs

Safe Programs

Static analysis marks unsafe

Missed Programs

False Positives

True Positives
• Static analysis makes a number of approximations: it may raise false alarms
• False alarms often hated by users
  - Sometimes too many potential problems raised by tool
• Often programmers need to check errors to rule out false alarms
• True defects may be lost, buried in details
• Tools compete on false positive rate for usability
False Positives in Type Checking

```java
short s = 0;
int i = s;
short r = i;
```

$ javac test.java
test.java:7: error: incompatible types: possible lossy conversion from int to short
short r = i;
^
1 error
False Positives in Type Checking

```java
short s = 0;
int i = s;
short r = i;
```

```
$ javac test.java
```

test.java:7: error: incompatible types: possible lossy conversion from int to short
```java
short r = i;
  ^
```
1 error
int i = 0;
if (false) {
    i = i + "hello";
}

$ javac test.java

test.java:7: error: incompatible types:
String cannot be converted to int
i = i + "hello";
^
1 error
```java
int i = 0;
if (false) {
    i = i + "hello";
}
```

```
$ javac test.java

test.java:7: error: incompatible types:
    String cannot be converted to int
    i = i + "hello";
   ^
1 error
```
False Positives in Type Checking

- No false positives in Python

```python
i = 0;
if (False):
    i = i + "hello";
```

- Dynamic type checking has run-time overhead
- Not suitable for time-critical applications
Gradual Typing

• Static and dynamic type systems have complimentary strengths

• **Static typing:** full-coverage error checking, efficient execution, machine-checked documentation

• **Dynamic typing:** rapid development and fast adaption to changing requirements

• **Gradual typing:** an approach for integrating static and dynamic type checking

• Gives the programmer fine-grained control over
  - which regions of a program are statically checked
  - which regions of a program are dynamically checked
Polymorphism

• In a monomorphic language (e.g. Pascal): you define a different length function for each type of list
• In a polymorphic language (e.g. ML): you define a polymorphic type (list t), where t is a type variable, and a single function for computing the length
• Haskell and most modern functional languages have polymorphic types and follow the Hindley-Milner type system

Simple types = Non polymorphic types
• Type system is almost never orthogonal to the semantics of the language
  - The types in a program can affect its behavior
    (e.g. operator overloading)
• We don’t define the type system in isolation, we define a typed language including definitions of
  - The syntax
  - dynamic semantics (e.g. operational semantics)
  - static semantics
    • also known as typing rules
    • describe how types are assigned to elements in a program
  - type soundness argument
    • describe the relationship between static and dynamic semantics
Basic Notation

- Type system assigns types to elements in the language
  - Basic notation: \( e : T \) (\( e \) is of type \( T \))
- The types of some elements depends on the environment
  - Basic notation: \( \Gamma \vdash e : T \)
    (Given environment \( \Gamma \), we can derive that \( e \) is of type \( T \))
  - An environment associates types with free variables
  - This is called a **Judgment**
  - Example:
    \[
    x : \text{Int}, y : \text{Int} \vdash x + y : \text{Int}
    \]
Typing Rules

- Typing rules tell us how to derive typing judgments
- Very similar to derivation rules in Big Step Operational Semantics

\[\frac{x : T \in \Gamma}{\Gamma \vdash x : T}\]

\[\frac{\Gamma \vdash n : \text{Int}}{\Gamma \vdash e_1 + e_2 : \text{Int}}\]

Premises

Judgment

Example: Language of Expressions

\[\frac{\Gamma \vdash e_1 : \text{Int} \quad \Gamma \vdash e_2 : \text{Int}}{\Gamma \vdash e_1 + e_2 : \text{Int}}\]
Example: Language of Expressions

\[
\begin{aligned}
  & x : T \in \Gamma \\
  \quad \Downarrow \quad & \Gamma \vdash x : T \\
  & \Gamma \vdash n : \text{Int} \\
  & \Gamma \vdash e_1 : \text{Int} \quad \Gamma \vdash e_2 : \text{Int} \\
  \quad \Downarrow \quad & \Gamma \vdash e_1 + e_2 : \text{Int}
\end{aligned}
\]

- Show that the following Judgment is valid

\[
x : \text{Int}, y : \text{Int} \vdash x + (y + 5) : \text{Int}
\]

\[
\begin{aligned}
  & x : \text{Int} \in \{x : \text{Int}, y : \text{Int}\} \\
  \quad \Downarrow \quad & \Gamma \vdash x : \text{Int} \\
  & \Gamma \vdash n : \text{Int} \\
  & \Gamma \vdash e_1 : \text{Int} \quad \Gamma \vdash e_2 : \text{Int} \\
  \quad \Downarrow \quad & \Gamma \vdash e_1 + e_2 : \text{Int}
\end{aligned}
\]

\[
\begin{aligned}
  & y : \text{Int} \in \{x : \text{Int}, y : \text{Int}\} \\
  \quad \Downarrow \quad & \Gamma \vdash y : \text{Int} \\
  & \Gamma \vdash e_1 : \text{Int} \quad \Gamma \vdash e_2 : \text{Int} \\
  \quad \Downarrow \quad & \Gamma \vdash e_1 + e_2 : \text{Int}
\end{aligned}
\]

\[
\begin{aligned}
  & x : \text{Int}, y : \text{Int} \vdash y : \text{Int} \\
  \quad \Downarrow \quad & \Gamma \vdash y : \text{Int} \\
  & \Gamma \vdash e_1 : \text{Int} \quad \Gamma \vdash e_2 : \text{Int} \\
  \quad \Downarrow \quad & \Gamma \vdash e_1 + e_2 : \text{Int}
\end{aligned}
\]

\[
\begin{aligned}
  & x : \text{Int}, y : \text{Int} \vdash 5 : \text{Int} \\
  \quad \Downarrow \quad & \Gamma \vdash 5 : \text{Int} \\
  & \Gamma \vdash e_1 : \text{Int} \quad \Gamma \vdash e_2 : \text{Int} \\
  \quad \Downarrow \quad & \Gamma \vdash e_1 + e_2 : \text{Int}
\end{aligned}
\]

\[
\begin{aligned}
  & x : \text{Int}, y : \text{Int} \vdash x + (y + 5) : \text{Int} \\
  \quad \Downarrow \quad & \Gamma \vdash x + (y + 5) : \text{Int}
\end{aligned}
\]
Simply Typed $\lambda$-calculus ($F_1$)

- Modify the syntax of the $\lambda$-calculus to add type annotations for parameters of functions

**Syntax**

**Terms**
\[
e ::= x \mid \lambda x : \tau. e \mid e_1 \ e_2 \\
\mid n \mid e_1 + e_2 \mid e_1 = e_2 \\
\mid \text{if } e_1 \text{ then } e_t \text{ else } e_f
\]

**Types**
\[
\tau ::= \text{Int} \mid \text{Bool} \mid \tau_1 \rightarrow \tau_2
\]

- $\tau_1 \rightarrow \tau_2$ is the function type
- $\rightarrow$ associates to the right
- This language is also called $F_1$
Static Semantics of $F_1$

- **Basic Typing Rules**

\[
\begin{align*}
\frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau} & \quad \frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash (\lambda x : \tau_1. \ e) : \tau_1 \to \tau_2} & \quad \frac{\Gamma \vdash e_1 : \tau' \to \tau \quad \Gamma \vdash e_2 : \tau'}{\Gamma \vdash e_1 \ e_2 : \tau}
\end{align*}
\]

- **Extensions**

\[
\begin{align*}
\frac{\Gamma \vdash e_1 : \text{Int} \quad \Gamma \vdash e_2 : \text{Int}}{\Gamma \vdash n : \text{Int}} & \quad \frac{\Gamma \vdash e_1 + e_2 : \text{Int}}{\Gamma \vdash e_1 = e_2 : \text{Bool}} & \quad \frac{\Gamma \vdash e_1 : \text{Bool} \quad \Gamma \vdash e_t : \tau}{\Gamma \vdash \text{if } e \text{ then } e_t \text{ else } e_f : \tau}
\end{align*}
\]