Substructural Proof/Type Theory

CAS CS 392: Rust, in Theory and in Practice

March 18, 2025 (Lecture 13)

Outline

Intuitionistic Propositional Logic

Syntax:

$$
\begin{aligned}
V &::= p \mid q \mid r \ldots \\
T &::= V \mid \bot \mid T \to T \mid T \wedge T \mid T \vee T
\end{aligned}
$$

Proof System:

$$
\frac{}{\Gamma, \phi, \Delta \vdash \phi} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash \phi} \qquad \frac{\Gamma \vdash \phi \to \psi \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi}
$$

$$
\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi} \qquad \frac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}
$$

$$
\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi} \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi} \qquad \frac{\Gamma \vdash \phi \vee \psi \qquad \Gamma, \phi \vdash \xi \qquad \Gamma, \psi \vdash \xi}{\Gamma \vdash \xi}
$$

Untyped Lambda Calculus

Syntax:

$$V ::= x \mid y \mid z \ldots$$
$$T ::= V \mid \lambda V.T \mid TT$$

Small-Step Semantics:

$$\frac{M \longrightarrow M'}{\lambda x.M \longrightarrow \lambda x.M'} \qquad \frac{M \longrightarrow M'}{MN \longrightarrow M'N} \qquad \frac{N \longrightarrow N'}{MN \longrightarrow MN'}$$

$$\frac{}{(\lambda x.M)N \longrightarrow M[N/x]}$$

Simply Typed Lambda Calculus (STLC)

Syntax:

$$\begin{aligned} V_{Ty} &::= a \mid b \mid c \ldots \\ Ty &::= V_{Ty} \mid \bot \mid Ty \to Ty \\ V_T &::= x \mid y \mid z \ldots \\ T &::= V_T \mid \lambda V.T \mid TT \end{aligned}$$

Type System:

$$\frac{}{\Gamma, x : A, \Delta \vdash x : A} \qquad \frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \to B}$$

Curry-Howard Isomorphism

STLC Type System:

$$\frac{}{\Gamma, x : A, \Delta \vdash x : A} \qquad \frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \to B}$$

IPL Proof System:

$$\frac{}{\Gamma, \phi, \Delta \vdash \phi} \qquad \frac{\Gamma \vdash \phi \to \psi \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}$$

STLC+ (Syntax)

$$
\begin{aligned}
V_{Ty} &::= a \mid b \mid c \ldots \\
Ty &::= V_{Ty} \mid \bot \mid \top \mid Ty \rightarrow Ty \mid T \wedge T \mid T \vee T \\
V_T &::= x \mid y \mid z \ldots \\
T &::= V_T \mid \lambda V.T \mid TT \mid \langle T, T \rangle \mid \pi_1(T) \mid \pi_2(T) \\
&\quad \mid \iota_1(T) \mid \iota_2(T) \mid \text{case } T \text{ of } \iota_1(V) \rightarrow T; \iota_2(V) \rightarrow T \\
&\quad \mid \text{explode(M)} \mid \bullet
\end{aligned}
$$

STLC+ (Product Types)

STLC+ (Union Types)

STLC+ (Unit type and Empty Type)

Example

$$f : A \to B, g : A \to C, x : A \vdash \langle fx, gx \rangle : B \wedge C$$

Aside: Proof Reduction

Proofs can have unnecessary parts, e.g., building a pair only to immediately destruct it

This is also related to the notion of *cut-elimination*, an important topic in the area of proof theory

Proof reduction corresponds to *evaluation* in the CH isomorphism

Theme of the Day

A type system "draws a circle" around a class of programs with nice properties, which often manifest in the *semantics*

Theme of the Day

A type system "draws a circle" around a class of programs with nice properties, which often manifest in the *semantics*

Type systems open possibilities to better semantics

Theme of the Day

A type system "draws a circle" around a class of programs with nice properties, which often manifest in the *semantics*

Type systems open possibilities to better semantics

Rust, for example, can avoid using a garbage collector, not because you can write drastically different programs than in C, but because it restricts the kinds of C-like programs you can write

Outline

Assumptions

$$\frac{}{\Gamma, x : A, \Delta \vdash x : A}$$

The assumption rule is actually doing quite a bit of heavy lifting. In our system, we *cannot* add variables to our context mid-proof

Assumptions

$$\frac{}{\Gamma, x : A, \Delta \vdash x : A}$$

The assumption rule is actually doing quite a bit of heavy lifting. In our system, we *cannot* add variables to our context mid-proof

This is not a huge problem, we can change our contexts in the *meta-theory*

Admissible Rules

A rule is **admissible** or **derivable** if adding the rule to the system does not change what judgments can be derived

Lemma. If $\Gamma \vdash M : B$ and $x \notin \Gamma$, then $\Gamma, x : A \vdash M : B$.

Structural Rules

Structural rules allow us to change the state of our context mid-proof

All structural rules are admissible in STLC (and IPL)

Alternative System

We can rewrite the type system to include structural rules instead of the assumptions rule

Substructural Logics

Once we write are system to have structural rules, we have a degree of freedom to define *new systems*

Substructural logics/type systems disallow certain structural rules

System	Weakening	Contraction	Variable use
Unrestricted	yes	yes	any number of times
Affine	yes	no	at most once
Relevant	no	yes	at least once
Linear	no	no	exactly once

Outline

Linearity in Rust

We cannot use a variable more than once (without references):

```
// This does not compile
fn dup<T>(t: T) -> (T, T) {
  (t, t)
}
```

Linearity in Rust

We cannot use a variable more than once (without references):

```rust
// This does not compile
fn dup<T>(t: T) -> (T, T) {
  (t, t)
}
```

Rust without references is *linear*

Linearity in Rust

We can't implement the example from before:

```
// This does not compile
fn example<T, U, V, F, G>(f: F, g: G, x: T) -> (U, V)
where
    F : Fn(T) -> U,
    G : Fn(T) -> V,
{
    (f(x), g(x))
}
```

Question. How can we fix this?

Linear Logic

"**Truth is free**. Having proved a theorem, you may use this proof as many times as you wish, at no extra cost. **Food, on the other hand, has a cost.** Having baked a cake, you may eat it only once. If traditional logic is about truth, then linear logic is about food." (Walder)

Jean-Yves Girard introduced linear logic in the 80s as a *resource-sensitive* logic which made explicit certain dualities between classical and intuitionsitic logic

It is now most commonly used in PL and Quantum

Linear Typed λ-Calculus (LTLC)

Syntax:

$$\begin{aligned} V_{Ty} &::= a \mid b \mid c \ldots \\ Ty &::= V_{Ty} \mid \bot \mid Ty \multimap Ty \\ V_T &::= x \mid y \mid z \ldots \\ T &::= V_T \mid \lambda V.T \mid TT \end{aligned}$$

Type system:

$$\frac{}{x : A \vdash x : A} \qquad \frac{\Gamma \vdash M : A}{\pi(\Gamma) \vdash M : A}$$

$$\frac{\Gamma \vdash M : A \multimap B \qquad \Delta \vdash N : A}{\Gamma, \Delta \vdash MN : B} \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \multimap B}$$

Example

$$\vdash \lambda f.\lambda x.fx : (A \multimap B) \multimap A \multimap B$$

Non-Example

$$\vdash \lambda x.\lambda y.x : A \multimap B \multimap A$$

The Key Lemma

Lemma. If $\Gamma \vdash M : A$ then

- x is free in M if and only if x appears in Γ
- each free variables appears exactly *once* in M

This is what allows us to develop semantics which allow for a unique pointer to the heap (more on that next week)

LTLC+

It is natural to want more data types in LTLC

Furthermore, we might also want to *combine* linearity and nonlinerity (as is done in Rust)

In the reading, Wadler introduces Girard's *Logic of Unity* as a way of combining these ideas

LTLC+ (Intuitionistic Assumptions)

LTLC+ (Unlimited Resources)

LTLC+ (Sum Types)

LTLC+ (Product Types)

Linearity in Rust

If Rust was *really* linear this would not be possible:

```rust
fn proj<S, T>(p: (S, T)) -> S {
    p.0
}
```

Linearity in Rust

If Rust was *really* linear this would not be possible:

```rust
fn proj<S, T>(p: (S, T)) -> S {
    p.0
}
```

This code is morally equivalent to:

```rust
fn proj<S, T>(p: (S, T)) -> S {
    let out = p.0;
    drop(p.1);
    out
}
```

`drop` is also non-linear. Is `drop` as implicit? Is `drop` a language construct? (more on that in this week's assignment)

Closing Remarks: Array Updates

Closing Remarks: Revisiting Intuitionistic Assumptions