

Nominal logic for reasoning about terms with variable bindings

(Logika dziedzinowa do wnioskowania
o termach z wiązaniem zmiennych)

Dominik Gulczyński

Praca magisterska

Promotor: dr Piotr Polesiuk

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Informatyki

3 sierpnia 2023

Abstract

We describe logic for reasoning about terms with variable bindings.

Streszczenie

Przedstawiamy logikę dziedzinową do wnioskowania o termach z wiązaniem zmiennych.

Contents

1	Introduction	7
1.1	Problem statement	7
1.2	Motivation	7
1.3	Related work	7
1.3.1	Nominal logics & permutations	7
1.4	Contributions	7
2	Terms and constraints	9
3	Constraint solver	11
3.1	Implementation	15
4	Higher Order Logic	19
4.1	Kinds	19
4.2	Subkinding	20
4.3	Formulas	20
4.4	Fixpoint	21
4.5	Proof theory	22
5	Proof assistant	25
6	Case study: Progress and Preservation of STLC	27
7	Conclusion and future work	33
	Bibliography	35

Chapter 1

Introduction

1.1 Problem statement

...

1.2 Motivation

...

1.3 Related work

1.3.1 Nominal logics & permutations

1.4 Contributions

...

Chapter 2

Terms and constraints

In classical first-order logic, terms are built from variables and applications of functional symbols to other terms. In this work we expand terms with expressions closely resembling the syntax of lambda calculus, aiming to provide a flexible framework for reasoning about the lambda calculus and its derivations.

To this end we introduce an infinite set of *atoms* (denoted by lower-case letters), representing the bound variables in terms — i.e. the variables in the sense of lambda calculus. That set is disjoint with the set of variables commonly found in first-order logic, which from now on we will call *variables* (and denote by upper-case letters) as apposed to *atoms*.

Terms are given by the following grammar:

$$\begin{aligned}\pi &::= \text{id} \mid (\alpha \alpha)\pi && \text{(permutations)} \\ \alpha &::= \pi a && \text{(atom expressions)} \\ t &::= \alpha \mid \pi X \mid \alpha.t \mid t t \mid s && \text{(terms)}\end{aligned}$$

It is important to note that terms do not incorporate any inherent notions of computation, reduction, or binding. These expressions simply *look* like the lambda calculus but they lack the operational semantics of it. However, the intuitions associated with such expressions are not unfounded. We will observe their practical application in the sublogic of constraints that we define on top of terms to reason about notions of *freshness*, *variable binding* and *structural* order and its logical model.

Constraints are given by the following grammar:

$$c ::= \alpha \# t \mid t = t \mid t \sim t \mid t \prec t \quad \text{(constraints)}$$

with following semantics:

- $\alpha \# t$ — atom α is Fresh in term t , i.e. does not occur in t as a free variable
- $t_1 = t_2$ — terms t_1 and t_2 are alpha-equivalent
- $t_1 \sim t_2$ — terms t_1 and t_2 possess an identical shape,
i.e. after erasing all atoms, terms t_1 and t_2 would be equal
- $t_1 \prec t_2$ — shape of term t_1 is structurally smaller than the shape of term t_2 ,
i.e. after erasing all atoms t_1 would be equal to some subterm of t_2

We use metavariable Γ for finite sets of constraints.

- $T ::= A \mid n \mid \$T \mid T@T \mid s$ (semantic terms)
- $S ::= _ \mid _.S \mid S@S \mid s$ (semantic shapes)

$$\begin{aligned}
 \llbracket \pi a \rrbracket_\rho &= \llbracket \pi \rrbracket_\rho(\rho(a)) \\
 \llbracket \pi X \rrbracket_\rho &= \llbracket \pi \rrbracket_\rho(\rho(X)) \\
 \llbracket \alpha.t \rrbracket_\rho &= \$(\llbracket t \rrbracket_\rho \uparrow) \{ \llbracket \alpha \rrbracket_\rho \mapsto 0 \} \\
 \llbracket t_1 t_2 \rrbracket_\rho &= \llbracket t_1 \rrbracket_\rho @ \llbracket t_2 \rrbracket_\rho \\
 \llbracket s \rrbracket_\rho &= s
 \end{aligned}$$

$$\begin{aligned}
 |A| &= _ \\
 |n| &= _ \\
 |\$T| &= _.|T| \\
 1|T_1@T_2| &= |T_1|@|T_2|
 \end{aligned}$$

$$\begin{aligned}
 \rho \models t_1 = t_2 &\text{ iff } \llbracket t_1 \rrbracket_\rho = \llbracket t_2 \rrbracket_\rho \\
 \rho \models \alpha \# t &\text{ iff } \llbracket \alpha \rrbracket_\rho \notin \text{FreeAtoms}(\llbracket t \rrbracket_\rho) \\
 \rho \models t_1 \sim t_2 &\text{ iff } |\llbracket t_1 \rrbracket_\rho| = |\llbracket t_2 \rrbracket_\rho| \\
 \rho \models t_1 \prec t_2 &\text{ iff } |\llbracket t_1 \rrbracket_\rho| \text{ is a strict subshape of } |\llbracket t_2 \rrbracket_\rho|
 \end{aligned}$$

We write $\rho \models \Gamma$ iff for all $c \in \Gamma$ we have $\rho \models c$. We write $\Gamma \models c$ iff for every ρ such that $\rho \models \Gamma$ we have $\rho \models c$.

With this model in mind we will see that there exists a decidable algorithm for determining whether $C_1, \dots, C_n \models C_0$, i.e. a deterministic way of checking if constraints c_1, \dots, c_n imply c_0 . We present such algorithm in the next chapter.

Chapter 3

Constraint solver

Bird's eye view: Solver breaks down constraints (on both sides of the turnstile) to irreducible components that are solved easily.

At the core of our work lies the Solver — the algorithm of resolving the constraints. Given a list of assumptions c_1, \dots, c_n it checks whether given goal c_0 holds. In other words it is an algorithm that verifies whether, for every possible substitution of closed terms (in terms of variables, not atoms) for variables in c_0, c_1, \dots, c_n such that the constraints c_1, \dots, c_n are satisfied, c_0 is also satisfied.

For convenience and effectiveness of implementation, the Solver works with constraints a little different constraints (although not more expressive) than those occurring in formulas and kinds, main difference being use of *shapes* instead of terms for shape constraints. Solver constraints and shapes are given by the following grammar:

$\mathcal{C} ::= \alpha \# t \mid t = t \mid S \sim S \mid S \prec S$ (solver constraints)

$S ::= _ \mid X \mid _.S \mid S S \mid s$ (shapes)

Solver erases atoms from terms in shape constraints, effectively transforming them from *constraints* to *solver constraints*.

We add another environment Δ to distinguish between the potentially-reducible assumptions in Γ . For convenience we will write $a \neq \alpha$ instead of $a \# \alpha$ as it gives good intuition of atom freshness implying inequality and for $\alpha = \pi a$ we will write $\alpha \# t$ meaning $a \# \pi^{-1}t$. Irreducible constraints are:

- $a_1 \neq a_2$ — atoms a_1 and a_2 are different
- $a \# X$ — atom a is Fresh in variable X
- $X_1 \sim X_2$ — variables X_1 and X_2 possess the same shape
- $X \sim t$ — variable X has a shape of term t
- $t \prec X$ — term t strictly subshapes variable X

After all the constraints are reduced to such simple constraints we reduce the

goal-constraint and repeat the reduction procedure on new assumptions and goal. We either arrive on a contradictory environment or all the assumptions and goal itself are reduced to irreducible constraints which is as simple as checking if the goal occurs on the left side of the turnstile.

$$\frac{\mathcal{C} \in \Delta}{\Gamma; \Delta \models \mathcal{C}}$$

Decidability of atom equality plays an important role in the reduce procedure:

$$\begin{array}{c} \frac{a \neq \alpha_1, a \neq \alpha_2, \Gamma; \Delta \models a = \alpha}{\Gamma; \Delta \models a = \pi^{-1}\alpha} \quad \frac{a = \alpha_1, a \neq \alpha_2, \Gamma; \Delta \models \alpha_2 = \alpha \quad a = \alpha_2, \Gamma; \Delta \models \alpha_1 = \alpha}{\Gamma; \Delta \models a = (\alpha_1 \ \alpha_2)\alpha} \\[10pt] \frac{\Gamma; \Delta \models \pi \text{ idempotent on } X}{\Gamma; \Delta \models X = \pi X} \quad \frac{\Gamma; \Delta \models X_1 = \pi_1^{-1}\pi_2 X_2}{\Gamma; \Delta \models \pi_1 X_1 = \pi_2 X_2} \\[10pt] \frac{\Gamma; \Delta \models \alpha_1 \# t_2 \quad \Gamma; \Delta \models t_1 = (\alpha_1 \ \alpha_2)t_2}{\Gamma; \Delta \models \alpha_1.t_1 = \alpha_2.t_2} \quad \frac{\Gamma; \Delta \models t_1 = t_2 \quad \Gamma; \Delta \models t'_1 = t'_2}{\Gamma; \Delta \models t_1 t'_1 = t_2 t'_2} \\[10pt] \frac{}{\Gamma; \Delta \models a = a} \quad \frac{}{\Gamma; \Delta \models X = X} \quad \frac{}{\Gamma; \Delta \models s = s} \\[10pt] \frac{\forall a \in \pi. \Gamma; \Delta \models a = \pi a \ \vee \ \Gamma; \Delta \models a \# X}{\Gamma; \Delta \models \pi \text{ idempotent on } X} \\[10pt] \frac{a_1 \neq a_2 \in \Delta}{\Gamma; \Delta \models a_1 \# a_2} \quad \frac{a \neq \alpha_1, a \neq \alpha_2, \Gamma; \Delta \models a \# \alpha \quad a = \alpha_1, a \neq \alpha_2, \Gamma; \Delta \models \alpha_1 \# \alpha \quad a = \alpha_2, \Gamma; \Delta \models \alpha_2 \# \alpha}{\Gamma; \Delta \models a \# (\alpha_1 \ \alpha_2)\alpha} \\[10pt] \frac{a \# X \in \Delta}{\Gamma; \Delta \models a \# X} \quad \frac{a \neq \alpha_1, a \neq \alpha_2, \Gamma; \Delta \models a \# \pi X \quad a = \alpha_1, a \neq \alpha_2, \Gamma; \Delta \models \alpha_1 \# \pi X \quad a = \alpha_2, \Gamma; \Delta \models \alpha_2 \# \pi X}{\Gamma; \Delta \models a \# (\alpha_1 \ \alpha_2)\pi X} \\[10pt] \frac{a \neq \alpha, \Gamma; \Delta \models a \# t}{\Gamma; \Delta \models a \# \alpha.t} \quad \frac{\Gamma; \Delta \models a \# t_1 \quad \Gamma; \Delta \models a \# t_2}{\Gamma; \Delta \models a \# t_1 t_2} \quad \frac{}{\Gamma; \Delta \models a \# s} \\[10pt] \frac{X_1 \sim X_2 \in \Delta}{\Gamma; \Delta \models X_1 \sim X_2} \quad \frac{X \sim S' \in \Delta \quad \Gamma; \Delta \models S' \sim S}{\Gamma; \Delta \models X \sim S} \\[10pt] \frac{\Gamma; \Delta \models S_1 \sim S_2}{\Gamma; \Delta \models _ . S_1 \sim _ . S_2} \quad \frac{\Gamma; \Delta \models S_1 \sim S_2 \quad \Gamma; \Delta \models S'_1 \sim S'_2}{\Gamma; \Delta \models S_1 S'_1 \sim S_2 S'_2} \quad \frac{}{\Gamma; \Delta \models s \sim s} \\[10pt] \frac{S_2 \prec X \in \Delta \quad \Gamma; \Delta \models S_2 \sim X}{\Gamma; \Delta \models S_1 \prec X} \quad \frac{S_2 \prec X \in \Delta \quad \Gamma; \Delta \models S_2 \prec X}{\Gamma; \Delta \models S_1 \prec X} \\[10pt] \frac{\Gamma; \Delta \models S_1 \sim S_2}{\Gamma; \Delta \models S_1 \prec _ . S_2} \quad \frac{\Gamma; \Delta \models S_1 \prec S_2}{\Gamma; \Delta \models S_1 \prec _ . S_2} \end{array}$$

$$\begin{array}{c}
\frac{\Gamma; \Delta \models S_1 \sim S_2}{\Gamma; \Delta \models S_1 \prec S_2 S'_2} \quad \frac{\Gamma; \Delta \models S_1 \sim S'_2}{\Gamma; \Delta \models S_1 \prec S_2 S'_2} \quad \frac{\Gamma; \Delta \models S_1 \prec S_2}{\Gamma; \Delta \models S_1 \prec S_2 S'_2} \quad \frac{\Gamma; \Delta \models S_1 \prec S'_2}{\Gamma; \Delta \models S_1 \prec S_2 S'_2} \\
\\
\frac{a_1 \neq a_2 \in \Delta}{a_1 = a_2, \Gamma; \Delta \models \mathcal{C}} \quad \frac{\Gamma\{a_1 \mapsto a_2\}; \Delta\{a_1 \mapsto a_2\} \models \mathcal{C}\{a_1 \mapsto a_2\}}{a_1 = a_2, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{a \neq \alpha_1, a \neq \alpha_2, a = \alpha, \Gamma; \Delta \models \mathcal{C} \quad a = \alpha_1, a \neq \alpha_2, \alpha_2 = \alpha, \Gamma; \Delta \models \mathcal{C} \quad a = \alpha_2, \alpha_1 = \alpha, \Gamma; \Delta \models \mathcal{C}}{a = (\alpha_1 \ \alpha_1)\alpha, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{a = \pi^{-1}\alpha, \Gamma; \Delta \models \mathcal{C}}{\pi a = \alpha, \Gamma; \Delta \models \mathcal{C}} \quad \frac{}{a = t_1 t_2, \Gamma; \Delta \models \mathcal{C}} \quad \frac{}{a = \alpha.t, \Gamma; \Delta \models \mathcal{C}} \quad \frac{}{a = s, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{\models \text{ idempotent on } X}{X = \pi X, \Gamma; \Delta \models \mathcal{C}} \quad \frac{\pi \text{ idempotent on } X, \Gamma; \Delta \models \mathcal{C}}{X = \pi X, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{\Gamma\{X \mapsto t\}; \Delta\{X \mapsto t\} \models \mathcal{C}\{X \mapsto t\}}{X = t, \Gamma; \Delta \models \mathcal{C}} \quad \frac{X = \pi^{-1}t, \Gamma; \Delta \models \mathcal{C}}{\pi X = t, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{\alpha_1 \# \alpha_2.t_2, t_1 = (\alpha_1 \ \alpha_2)t_2, \Gamma; \Delta \models \mathcal{C}}{\alpha_1.t_1 = \alpha_2.t_2, \Gamma; \Delta \models \mathcal{C}} \quad \text{Other term constructors trivial} \\
\\
\frac{t_1 = t_2, t'_1 = t'_2, \Gamma; \Delta \models \mathcal{C}}{t_1 t'_1 = t_2 t'_2, \Gamma; \Delta \models \mathcal{C}} \quad \text{Other term constructors trivial} \\
\\
\frac{s_1 \neq s_2}{s_1 = s_2, \Gamma; \Delta \models \mathcal{C}} \quad \frac{}{s = s, \Gamma; \Delta \models \mathcal{C}} \quad \text{Other term constructors trivial} \\
\\
\frac{(\forall a \in \pi. \Gamma; \Delta \models a = \pi a \ \vee \ \Gamma; \Delta \models a \# X), \Gamma; \Delta \models \mathcal{C}}{\pi \text{ idempotent on } X, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{}{a \neq a, \Gamma; \Delta \models \mathcal{C}} \quad \frac{\Gamma; \{a_1 \neq a_2\} \cup \Delta \models \mathcal{C}}{a_1 \neq a_2, \Gamma; \Delta \models \mathcal{C}} \quad \frac{\Gamma; \{a \# X\} \cup \Delta \models \mathcal{C}}{a \# X, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{a \neq \alpha_1, a \neq \alpha_2, a \# \alpha, \Gamma; \Delta \models \mathcal{C} \quad a = \alpha_1, a \neq \alpha_2, \alpha_2 \# \alpha, \Gamma; \Delta \models \mathcal{C} \quad a = \alpha_2, \alpha_1 \# \alpha, \Gamma; \Delta \models \mathcal{C}}{a \# (\alpha_1 \ \alpha_1)\alpha, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{a \neq \alpha_1, a \neq \alpha_2, a \# X, \Gamma; \Delta \models \mathcal{C} \quad a = \alpha_1, a \neq \alpha_2, \alpha_2 \# X, \Gamma; \Delta \models \mathcal{C} \quad a = \alpha_2, \alpha_1 \# X, \Gamma; \Delta \models \mathcal{C}}{a \# (\alpha_1 \ \alpha_1)X, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{a \# \alpha, \Gamma; \Delta \models \mathcal{C} \quad a \# \alpha, a \# t, \Gamma; \Delta \models \mathcal{C}}{a \# \alpha.t, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{a \# t_1, \Gamma; \Delta \models \mathcal{C} \quad a \# t_2, \Gamma; \Delta \models \mathcal{C}}{a \# t_1 t_2, \Gamma; \Delta \models \mathcal{C}}
\end{array}$$

$$\begin{array}{c}
\frac{\Gamma; \Delta \models \mathcal{C}}{a \# s, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{\Gamma; \{X_1 \sim X_2\} \cup \Delta \models \mathcal{C}}{X_1 \sim X_2, \Gamma; \Delta \models \mathcal{C}} \quad \frac{\Gamma; \{X \sim S\} \cup \Delta \models \mathcal{C}}{X \sim S, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{\Gamma; \Delta \models \mathcal{C}}{a_1 \sim a_2, \Gamma; \Delta \models \mathcal{C}} \quad \text{Other term constructors trivial} \\
\\
\frac{t_1 \sim t_2, \Gamma; \Delta \models \mathcal{C}}{_.t_1 \sim _.t_2, \Gamma; \Delta \models \mathcal{C}} \quad \text{Other term constructors trivial} \\
\\
\frac{t_1 \sim t_2, \Gamma; \Delta \models \mathcal{C} \quad t'_1 \sim t'_2, \Gamma; \Delta \models \mathcal{C}}{t_1 t'_1 \sim t_2 t'_2, \Gamma; \Delta \models \mathcal{C}} \quad \text{Other term constructors trivial} \\
\\
\frac{s_1 \neq s_2}{s_1 \sim s_2, \Gamma; \Delta \models \mathcal{C}} \quad \frac{}{s \sim s, \Gamma; \Delta \models \mathcal{C}} \quad \text{Other term constructors trivial} \\
\\
\frac{\Gamma; \{t \prec X\} \cup \Delta \models \mathcal{C}}{t \prec X, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{t_1 \sim t_2, \Gamma; \Delta \models \mathcal{C} \quad t_1 \prec t_2, \Gamma; \Delta \models \mathcal{C}}{t_1 \prec _.t_2, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{t_1 \sim t_2, \Gamma; \Delta \models \mathcal{C} \quad t_1 \sim t'_2, \Gamma; \Delta \models \mathcal{C} \quad t_1 \prec t_2, \Gamma; \Delta \models \mathcal{C} \quad t_1 \prec t'_2, \Gamma; \Delta \models \mathcal{C}}{t_1 \prec t_2 t'_2, \Gamma; \Delta \models \mathcal{C}} \\
\\
\frac{}{t \prec \alpha, \Gamma; \Delta \models \mathcal{C}} \quad \frac{}{t \prec s, \Gamma; \Delta \models \mathcal{C}}
\end{array}$$

TODO: explain what is $\{\mathcal{C}\} \cup \Delta$ Additional rule for arriving in contradictory Δ :

$$\frac{}{\Gamma; \not\models \mathcal{C}}$$

Define state of the solver by triple $(\Gamma, \Delta, \mathcal{C}_0)$ and such ordering of the states:

1. Number of distinct variables in $\Gamma, \Delta, \mathcal{C}_0$.
2. Depth of \mathcal{C}_0 .
3. Number of assumptions of given depth in Γ and Δ .
4. Number of assumptions of given depth in Γ .

Then by analysing each rule we can see the reductions always arrive in a smaller state.

3.1 Implementation

Environment Δ is a quintuple $(NeqAtoms_\Delta, Fresh_\Delta, VarShape_\Delta, Shape_\Delta, Subshape_\Delta)$ where:

$NeqAtoms$ is a set of pairs of atoms that we know are different,

$Fresh$ is a mapping from atoms to variables that we know the atom is Fresh in,

$VarShape$ is a mapping from variables to shape-representative variables (i.e. all variables that are mapped in $VarShape$ to the same variable are of the same shape),

$Shape$ is a mapping from shape-representative variables to shape that we know this variable must have,

$SubShape$ is a mapping from shape-representative variables to sets of shapes that we know this variable must supershape.

We can now define a way to compute the shape-representative variable:

$$X_\Delta := \begin{cases} X & \text{if } VarShape_\Delta(X) = \emptyset \\ X'_\Delta & \text{if } VarShape_\Delta(X) = X' \end{cases}$$

And shape-reconstruction:

$$\begin{aligned} |X|_\Delta &:= \begin{cases} |X'|_\Delta & \text{if } VarShape_\Delta(X) = X' \\ S & \text{if } Shape_\Delta(X) = S \\ X & \text{otherwise} \end{cases} \\ |_|_\Delta &:= _ \\ |_ . S|_\Delta &:= _ . |S|_\Delta \\ |S_1 S_2|_\Delta &:= |S_1|_\Delta |S_2|_\Delta \\ |s|_\Delta &:= s \\ |t|_\Delta &:= ||t||_\Delta \end{aligned}$$

Now we can easily check for irreducible constraints in Δ :

$$\begin{aligned} (a_1 \neq a_2) \in \Delta &:= (a_1 \neq a_2) \in NeqAtoms_\Delta \\ (a \# X) \in \Delta &:= X \in Fresh_\Delta(a) \\ (X_1 \sim X_2) \in \Delta &:= |X_1|_\Delta = |X_2|_\Delta \\ (X \sim S) \in \Delta &:= S = Shape_\Delta(X_\Delta) \\ (S \prec X) \in \Delta &:= S \in SubShape_\Delta(X_\Delta) \end{aligned}$$

Now we can define rules for the special occurs check:

$$\frac{X_\Delta \text{ occurs syntactically in } |S|_\Delta}{\Delta \models X \text{ occurs in } S}$$

$$\frac{X'_\Delta \text{ occurs syntactically in } |S|_\Delta \quad (S' \prec X') \in \Delta \quad \Delta \models X \text{ occurs in } S'}{\Delta \models X \text{ occurs in } S}$$

And finally the rules for $\mathcal{C} \cup \Delta$. Note that we are using meta-field of *Assumptions* to indicate that some of the assumptions in Δ are no longer "simple" and escape from Δ back to Γ to be broken up by the *Solver*.

$$\{a \# X\} \cup \Delta := \Delta[\text{Fresh}(a) += X]$$

$$\{a \neq a'\} \cup \Delta := \begin{cases} \text{false} & \text{if } a = a' \\ \Delta[\text{NeqAtoms} += (a \neq a')] & \text{otherwise.} \end{cases}$$

$$\{X \sim S\} \cup \Delta := \begin{cases} \text{false} & \text{if } \Delta \models X \text{ occurs in } S \\ \Delta' & \text{otherwise.} \end{cases}$$

$$\begin{aligned} \text{where } \Delta' &= \Delta.\text{Symbols}\{X_\Delta \rightsquigarrow |S|_\Delta\} \\ &\quad .\text{Subshapes}\{X_\Delta \rightsquigarrow |S|_\Delta\} \\ &\quad .\text{Shape}\{X_\Delta \rightsquigarrow |S|_\Delta\} \end{aligned}$$

$$\{X \sim X'\} \cup \Delta := \begin{cases} \Delta & \text{if } X_\Delta = X'_\Delta \\ \Delta & \text{if } |X|_\Delta = |X'|_\Delta \\ \text{false} & \text{if } X_\Delta \text{ occurs in } |X'|_\Delta \\ \text{false} & \text{if } X'_\Delta \text{ occurs in } |X|_\Delta \\ \Delta' & \text{otherwise.} \end{cases}$$

$$\begin{aligned} \text{where } \Delta' &= \Delta.\text{Symbols}\{X_\Delta \rightsquigarrow X'_\Delta\} \\ &\quad .\text{Subshapes}\{X_\Delta \rightsquigarrow X'_\Delta\} \\ &\quad .\text{TransferShape}\{X_\Delta \rightsquigarrow X'_\Delta\} \\ &\quad [\text{Shape} -= (X_\Delta) \\ &\quad , \text{SubShape} -= (X_\Delta) \\ &\quad , \text{VarShape} += (X_\Delta \mapsto X'_\Delta) \\ &\quad] \end{aligned}$$

$$\Delta.\text{Symbols}\{X \rightsquigarrow S\} := \begin{cases} \Delta[\text{Symbols} -= X, \text{Assumptions} += \text{symbol } S] & \text{if } X_\Delta \in \Delta.\text{Symbols} \\ \Delta & \text{otherwise.} \end{cases}$$

$$\Delta.\text{Shape}\{X \rightsquigarrow S\} := \begin{cases} \Delta[\text{Assumptions} += (S \sim S')] & \text{if } \text{Shape}_\Delta(X_\Delta) = S' \\ \Delta[\text{Shapes} += (X \mapsto S)] & \text{otherwise.} \end{cases}$$

$$\Delta.\text{SubShapes}\{X \rightsquigarrow S\} := \Delta[\text{Assumptions} += \text{Subshapes}_\Delta(X) \prec S]$$

$$\Delta.TransferShape\{X \rightsquigarrow X'\} := \begin{cases} \Delta.Shape\{termv' \rightsquigarrow S'\} & \text{if } Shape_{\Delta}(X_{\Delta}) = S \\ \Delta & \text{otherwise.} \end{cases}$$

$$\Delta\{X \mapsto t\} := \{X \sim |t|_{\Delta}\} \cup \Delta.Fresh\{X \mapsto t\}$$

$$\Delta.Fresh\{X \mapsto t\} := \Delta[Fresh.map(\text{fun } (a \# \mathbb{X}) \mapsto a \# (\mathbb{X} \setminus \{X\}))] \cup \bigcup_{\substack{(a \# \mathbb{X}) \in Fresh_{\Delta} \\ X \in \mathbb{X}}} \{a \# t\}$$

$$\Delta\{a \mapsto a'\} := \Delta.Fresh\{a \mapsto a'\}.NeqAtoms\{a \mapsto a'\}$$

$$\Delta.Fresh\{a \mapsto a'\} := \Delta[Fresh \text{ -- } a][Fresh \text{ += } \{a' \# \Delta.Fresh(a)\}]$$

$$\Delta.NeqAtoms\{a \mapsto a'\} := \Delta[NeqAtoms = \emptyset] \cup \bigcup_{(a_1 \neq a_2) \in NeqAtoms_{\Delta}} \{a_1\{a \mapsto a'\} \neq a_2\{a \mapsto a'\}\}$$

Chapter 4

Higher Order Logic

On top of sublogic of constraints we build an higher order logic. Due to involvement of atoms, terms, binders and constraints, we introduce kinds to make sure the formulas we deal with *make sense*.

4.1 Kinds

$\kappa ::= \star \mid \kappa \rightarrow \kappa \mid \forall_A a. \kappa \mid \forall_T X. \kappa \mid [c]\kappa \quad (\text{kinds})$

- $\varphi :: \star$ — φ is a propositional formula.
- $\varphi :: \kappa_1 \rightarrow \kappa_2$ — φ is function that takes a formula of kind κ_1 , and produces a formula of kind κ_2 .
- $\varphi :: \forall_A a. \kappa$ — φ is function that takes an an atom expression, binds it to a and produces a formula of kind κ .
- $\varphi :: \forall_T X. \kappa$ — φ is function that takes a term, binds it to X and produces a formula of kind κ .
- $\varphi :: [c]\kappa$ — φ is a formula of kind κ as long as c is satisfied.

Notice that as constraints occur in kinds, we cannot simply give functions from atoms some kind $Atom \rightarrow \kappa$, but we must know *which* atom is bound there, to substitute for it in κ the same way we substitute that atom for an atom expression in the function body when applying it to the formula. The *guarded kind* $[c]\kappa$ is most importantly used in kinding of the fixpoint formulas that we will explain in later sections.

4.2 Subkinding

Kinding relation is relaxed through the *subkinding*, a relation that is naturally reflexive and transitive:

$$\frac{}{\Gamma \vdash \kappa <: \kappa} \quad \frac{\Gamma \vdash \kappa_1 <: \kappa_2 \quad \Gamma \vdash \kappa_2 <: \kappa_3}{\Gamma \vdash \kappa_1 <: \kappa_3}$$

Universally quantified kinds only subkind if they are quantified over the same name:

$$\frac{\Gamma \vdash \kappa_1 <: \kappa_2}{\Gamma \vdash \forall_A a. \kappa_1 <: \forall_A a. \kappa_2} \quad \frac{\Gamma \vdash \kappa_1 <: \kappa_2}{\Gamma \vdash \forall_T X. \kappa_1 <: \forall_T X. \kappa_2}$$

Function kind is contravariant to the subkinding relation on the left argument:

$$\frac{\Gamma \vdash \kappa'_1 <: \kappa_1 \quad \Gamma \vdash \kappa_2 <: \kappa'_2}{\Gamma \vdash \kappa_1 \rightarrow \kappa_2 <: \kappa'_1 \rightarrow \kappa'_2}$$

Constraints that are solved through \models relation can be dropped:

$$\frac{\Gamma \models c}{\Gamma \vdash [c] \kappa <: \kappa}$$

And constraints can be moved to the enviroment from the right-hand side:

$$\frac{\Gamma, c \vdash \kappa_1 <: \kappa_2}{\Gamma \vdash \kappa_1 <: [c] \kappa_2}$$

Note that there is no structural subkinding rule for guarded kinds like

$$\frac{\Gamma \vdash \kappa_1 <: \kappa_2}{\Gamma \vdash [c] \kappa_1 <: [c] \kappa_2} \times$$

Such a rule can be derived from both subkinding rules for guarded kind, transitivity, and weakening.

4.3 Formulas

Formulas include standard connectives (of kind \star):

$$\varphi ::= \perp \mid \top \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \varphi \rightarrow \varphi \mid \dots \quad (\text{formulas})$$

Quantification over atoms and terms (on formulas of kind \star):

$$\varphi ::= \dots \mid \forall_A a. \varphi \mid \forall_T X. \varphi \mid \exists_A a. \varphi \mid \exists_T X. \varphi \mid \dots \quad (\text{formulas})$$

Constraints, guards, and propositional variables:

$$\varphi ::= \dots \mid c \mid [c] \wedge \varphi \mid [c] \rightarrow \varphi \mid P \mid \dots \quad (\text{formulas})$$

$$\frac{}{\Gamma; \Sigma \vdash c :: \star} \quad \frac{\Gamma, c; \Sigma \vdash \varphi :: \star}{\Gamma; \Sigma \vdash [c] \wedge \varphi :: \star} \quad \frac{\Gamma, c; \Sigma \vdash \varphi :: \star}{\Gamma; \Sigma \vdash [c] \rightarrow \varphi :: \star} \quad \frac{(P :: \kappa) \in \Sigma}{\Gamma; \Sigma \vdash P :: \kappa}$$

Propositional variables, functions and applications:

$$\varphi ::= \dots \mid \lambda_A a. \varphi \mid \lambda_T X. \varphi \mid \lambda P :: \kappa. \varphi \mid \varphi \alpha \mid \varphi t \mid \varphi \varphi \mid \dots \quad (\text{formulas})$$

$$\begin{array}{c} \frac{\Gamma; \Sigma \vdash \varphi :: \kappa}{\Gamma; \Sigma \vdash \lambda_A a. \varphi :: \forall_A a. \kappa} \quad \frac{\Gamma; \Sigma \vdash \varphi :: \kappa}{\Gamma; \Sigma \vdash \lambda_T X. \varphi :: \forall_T X. \kappa} \quad \frac{\Gamma; \Sigma, P :: \kappa_1 \vdash \varphi :: \kappa_2}{\Gamma; \Sigma \vdash \lambda P :: \kappa_1. \varphi :: \kappa_1 \rightarrow \kappa_2} \\[10pt] \frac{\Gamma; \Sigma \vdash \varphi :: \forall_A a. \kappa}{\Gamma; \Sigma \vdash \varphi \alpha :: \kappa\{a \mapsto \alpha\}} \quad \frac{\Gamma; \Sigma \vdash \varphi :: \forall_T X. \kappa}{\Gamma; \Sigma \vdash \varphi t :: \kappa\{X \mapsto t\}} \quad \frac{\Gamma; \Sigma \vdash \varphi_1 :: \kappa' \rightarrow \kappa \quad \Gamma; \Sigma \vdash \varphi_2 :: \kappa'}{\Gamma; \Sigma \vdash \varphi_1 \varphi_2 :: \kappa} \end{array}$$

4.4 Fixpoint

And finish the definition of formulas with *fixpoint* function:

$$\varphi ::= \dots \mid \text{fix } P(X) :: \kappa = \varphi \quad (\text{formulas})$$

$$\frac{\Gamma; \Sigma, (P :: \forall_T Y. [Y \prec X] \kappa\{X \mapsto Y\}) \vdash \varphi :: \kappa}{\Gamma; \Sigma \vdash (\text{fix } P(X) :: \kappa = \varphi) :: \forall_T X. \kappa}$$

Fixpoint constructor allows us to express *recursive* predicates over terms, but only such that the recursive applications are on structurally smaller terms, which we express in the kinding rule through the kinding $(P :: \forall_T Y. [Y \prec X] \kappa\{X \mapsto Y\})$. To evaluate a fixpoint function applied on a term, simply substitute the bound variable with given term and recursive calls inside fixpoint's body with the fixpoint itself.

$$(\text{fix } P(X) :: \kappa = \varphi) t \equiv \varphi\{X \mapsto t\}\{P \mapsto (\text{fix } P(X) :: \kappa = \varphi)\}$$

Because the applied term is finite and we always recurse on structurally smaller terms, the final formula after all substitutions must also be finite — thanks to semantics of constraints and kinds.

To familiarize the reader with the fixpoint formulas we present how peano arithmetic can be modeled in our logic. Given symbols 0 and S for natural numbers construction one can write a predicate that a term models some natural number:

$$\text{fix } \text{Nat}(N) :: \star = (N = 0) \vee (\exists_T M. [N = S M] \wedge (\text{Nat } M))$$

Notice how the constraint $(N = S M)$ guards the recursive call to Nat , ensuring that constraint $(M \prec N)$ will be satisfied during kind checking of $(\text{Nat } M)$ in the kind derivation of the whole formula $(\text{Nat} :: \forall_T N. \star)$.

Similarly, we can define addition:

$$\text{fix } \text{PlusEq}(N) :: \forall_T M. \forall_T K. \star = \lambda_T M. \lambda_T K.$$

$$([N = 0] \wedge (M = K)) \vee (\exists_T N'. K'. [N = S N'] \wedge [K = S K'] \wedge (\text{PlusEq } N' M K'))$$

TODO: Write how N is treated differently from M and K ?

See more interesting examples of fixpoints usage in the chapter on STLC.

4.5 Proof theory

Finally we can define proof-theoretic rules. Starting with inference rules for assumption, we can already define its constraint-sublogic analogues that employ the solver. And while the \vdash relation we define is purely syntactic, we can still use semantic \models because of its decidability.

$$\frac{\varphi \in \Theta}{\Gamma; \Theta \vdash \varphi} \text{ (Assumption)} \quad \frac{\Gamma \models c}{\Gamma; \Theta \vdash c} \text{ (constr}^i\text{)}$$

Again for *ex falso* we define analogic proof constructor for dealing with contradictory constraint environment. Note that there are many constraints that can be used as \perp_c , i.e. constraints that are always false and solver will only *prove* them if we supply it with contradictory assumptions

$$\frac{\Gamma; \Theta \vdash \perp}{\Gamma; \Theta \vdash \varphi} (\perp^e) \quad \frac{\Gamma \models \perp_c}{\Gamma; \Theta \vdash \varphi} \text{ (constr}^e\text{)}$$

Inference rules for implication are standard and the reason we present them here is not to bore the reader but to point the similarities to their constraint analogues.

$$\frac{\Gamma; \Theta, \varphi_1 \vdash \varphi_2}{\Gamma; \Theta \vdash \varphi_1 \rightarrow \varphi_2} (\rightarrow^i) \quad \frac{\Gamma_1; \Theta_1 \vdash \varphi_1 \quad \Gamma_2; \Theta_2 \vdash \varphi_1 \rightarrow \varphi_2}{\Gamma_1 \cup \Gamma_2; \Theta_2 \cup \Theta_2 \vdash \varphi_2} (\rightarrow^e)$$

$$\frac{\Gamma, c; \Theta \vdash \varphi}{\Gamma; \Theta \vdash [c] \rightarrow \varphi} ([\cdot] \rightarrow^i) \quad \frac{\Gamma_1; \Theta_1 \vdash c \quad \Gamma_2; \Theta_2 \vdash [c] \rightarrow \varphi}{\Gamma_1 \cup \Gamma_2; \Theta_2 \cup \Theta_2 \vdash \varphi} ([\cdot] \rightarrow^e)$$

Notice that in the case constraint-and-guard the rule for elimination is restricted to only formulas of kind \star . This is due to nature of the guard — if we want to eliminate it, we can only do so with formulas that *make sense* on their own, without that c guard.

$$\frac{\Gamma_1; \Theta_1 \vdash \varphi_1 \quad \Gamma_2; \Theta_2 \vdash \varphi_2}{\Gamma_1 \cup \Gamma_2; \Theta_2 \cup \Theta_2 \vdash \varphi_1 \wedge \varphi_2} (\wedge^i) \quad \frac{\Gamma; \Theta \vdash \varphi_1 \wedge \varphi_2}{\Gamma; \Theta \vdash \varphi_1} (\wedge_1^e) \quad \frac{\Gamma; \Theta \vdash \varphi_1 \wedge \varphi_2}{\Gamma; \Theta \vdash \varphi_2} (\wedge_2^e)$$

$$\frac{\Gamma \models c \quad \Gamma, c; \Theta \vdash \varphi}{\Gamma; \Theta \vdash [c] \wedge \varphi} ([\cdot] \wedge^i) \quad \frac{\Gamma; \Theta \vdash [c] \wedge \varphi}{\Gamma; \Theta \vdash c} ([\cdot] \wedge_1^e) \quad \frac{\Gamma \vdash [c] \wedge \varphi \quad \Gamma; \Theta \vdash \varphi : \star}{\Gamma; \Theta \vdash \varphi} ([\cdot] \wedge_2^e)$$

Inference rules for disjunction and quantifiers are rather straightforward. As one would expect we restrict generalized name to be *fresh* in the environment (it may not occur in any of the assumptions) and the names given to witnesses of existential quantification must also be *fresh*. Rules for quantifiers always come in pairs — one for the atoms and one for the variables.

$$\frac{\Gamma; \Theta \vdash \varphi_1}{\Gamma; \Theta \vdash \varphi_1 \vee \varphi_2} (\vee_1^i) \quad \frac{\Gamma; \Theta \vdash \varphi_2}{\Gamma; \Theta \vdash \varphi_1 \vee \varphi_2} (\vee_2^i) \quad \frac{\Gamma; \Theta \vdash \varphi_1 \vee \varphi_2}{\Gamma; \Theta, \varphi_1 \vdash \psi \quad \Gamma; \Theta, \varphi_2 \vdash \psi} (\vee^e)$$

$$\frac{a \notin \text{FV}(\Gamma; \Theta) \quad \Gamma; \Theta \vdash \varphi}{\Gamma; \Theta \vdash \forall_A a. \varphi} (\forall_A. i) \quad \frac{\Gamma; \Theta \vdash \forall_A a. \varphi}{\Gamma; \Theta \vdash \varphi\{a \mapsto a'\}} (\forall_A. e)$$

$$\frac{X \notin \text{FV}(\Gamma; \Theta) \quad \Gamma; \Theta \vdash \varphi}{\Gamma; \Theta \vdash \forall_T X. \varphi} (\forall_T. i) \quad \frac{\Gamma; \Theta \vdash \forall_T X. \varphi}{\Gamma; \Theta \vdash \varphi\{X \mapsto X'\}} (\forall_T. e)$$

$$\begin{array}{c}
\frac{\Gamma; \Theta \vdash \varphi\{a \mapsto a'\}}{\Gamma; \Theta \vdash \exists_A a. \varphi} \quad (\exists_A.^i) \qquad \frac{\Gamma_1; \Theta_1 \vdash \exists_A a. \varphi \quad \Gamma_2; \Theta_2, \varphi\{a \mapsto a'\} \vdash \psi \quad a' \notin \text{FV}(\Gamma_1 \cup \Gamma_2; \Theta_2 \cup \Theta_2)}{\Gamma_1 \cup \Gamma_2; \Theta_2 \cup \Theta_2 \vdash \psi} \quad (\exists_A.^e) \\
\\
\frac{\Gamma; \Theta \vdash \varphi\{X \mapsto X'\}}{\Gamma; \Theta \vdash \exists_T X. \varphi} \quad (\exists_T.^i) \qquad \frac{\Gamma_1; \Theta_1 \vdash \exists_T X. \varphi \quad \Gamma_2; \Theta_2, \varphi\{X \mapsto X'\} \vdash \psi \quad X' \notin \text{FV}(\Gamma_1 \cup \Gamma_2; \Theta_2 \cup \Theta_2)}{\Gamma_1 \cup \Gamma_2; \Theta_2 \cup \Theta_2 \vdash \psi} \quad (\exists_T.^e)
\end{array}$$

To make the framework more flexible we introduce a way for using equivalent formulas:

$$\frac{\Gamma; \Theta \vdash \psi \quad \Gamma; \Theta \vdash \psi \equiv \varphi}{\Gamma; \Theta \vdash \varphi} \quad (Equiv)$$

And a way to substitute atoms for atomic expression and variables for terms, if the solver can prove their equality:

$$\frac{\Gamma \models a = \alpha \quad \Gamma; \Theta \vdash \varphi}{\Gamma\{a \mapsto \alpha\}; \Theta\{a \mapsto \alpha\} \vdash \varphi\{a \mapsto \alpha\}} \quad (\mapsto_A) \qquad \frac{\Gamma \models X = t \quad \Gamma; \Theta \vdash \varphi}{\Gamma\{X \mapsto t\}; \Theta\{X \mapsto t\} \vdash \varphi\{X \mapsto t\}} \quad (\mapsto_T)$$

Finall we define induction over term structure, and thanks to the constraints sublogic we can easily define the notion of *smaller terms* for inductive hypothesis:

$$\frac{\Gamma; \Theta, (\forall_T X'. [X' \prec X] \rightarrow \varphi(X')) \vdash \varphi(X)}{\Gamma; \Theta \vdash \forall_T X. \varphi(X)} \quad (Induction)$$

We also define some axioms about constraint sublogic:

1. Atoms can be compared in a deterministic fashion,

$$\frac{}{\vdash \forall_A a, a'. (a = a') \vee (a \neq a')} \quad (Axiom_{Compare})$$

2. There are always exists a *fresh* atom,

$$\frac{}{\vdash \forall_T X. \exists_A a. (a \# X)} \quad (Axiom_{Fresh})$$

3. We can deduce the structure of a term.

$$\frac{}{\vdash \forall_T X. (\exists_A a. X = a) \vee (\exists_A a. \exists_T X'. X = a.X') \vee (\exists_T X_1, X_2. X = a.X') \vee (symbol\ X)} \quad (Axiom_{Inversion})$$

The equivalence relation ($\varphi_1 \equiv \varphi_2$) is a bit complicated due to the presence of environment with variable mapping, subkinding and formulas with fixpoints, functions, and applications. Nonetheless, it's simply that - *an equivalence relation* - and it behaves as expected. We will only highlighting the interesting parts.

$$\frac{\Gamma; \Sigma \vdash \varphi_1[X_1 \mapsto t_1] \equiv \varphi_2[X_2 \mapsto t_2]}{\Gamma; \Sigma \vdash (\lambda_T X_1. \varphi_1) t_1 \equiv (\lambda_T X_2. \varphi_2) t_2}$$

Otherwise we compute weak head normal form (up to some *depth*) and recurse on subformulas:

$$\frac{\Gamma; \Sigma; Sn \vdash (\text{fix } P(X) :: \kappa = \varphi) t}{\Gamma; \Sigma, P \mapsto \varphi; n \vdash \varphi[X \mapsto t]}$$

Until we reach WHNF computation *depth* or cannot compute the formula further, we resort to *naive* checking:

$$\begin{array}{c} \frac{\Gamma \models t_1 = t_2 \quad \Gamma; \Sigma \vdash \varphi_1 \equiv \varphi_2}{\Gamma; \Sigma \vdash \varphi_1 t_1 \equiv \varphi_2 t_2} \\ \\ \frac{\begin{array}{c} X \notin \text{FV}(\Gamma; \Sigma) \\ \Gamma; \Sigma \vdash \varphi_1[X_1 \mapsto X] \equiv \varphi_2[X_2 \mapsto X] \end{array}}{\Gamma; \Sigma \vdash \lambda_T X_1. \varphi_1 \equiv \lambda_T X_2. \varphi_2} \\ \\ \frac{\begin{array}{c} \kappa_1 <: \kappa_2 \\ \Gamma; \Sigma \vdash \varphi_1[P_1 \mapsto P] \equiv \varphi_2[P_2 \mapsto P] \end{array}}{\Gamma; \Sigma \vdash \lambda P_1 :: \kappa_1. \varphi_1 \equiv \lambda P_2 :: \kappa_2. \varphi_2} \\ \\ \frac{\begin{array}{c} \kappa_1 <: \kappa_2 \quad P \notin \text{FV}(\Gamma; \Sigma) \quad X \notin \text{FV}(\Gamma; \Sigma) \\ \Gamma; \Sigma \vdash \varphi_1[P_1 \mapsto P, X_1 \mapsto X] \equiv \varphi_2[P_2 \mapsto P, X_2 \mapsto X] \end{array}}{\Gamma; \Sigma \vdash \text{fix } P_1(X_1) :: \kappa_1 = \varphi_1 \equiv \text{fix } P_2(X_2) :: \kappa_2 = \varphi_2} \end{array}$$

Note that we allow *different terms* in equivalent formulas as long as constraints-environment Γ ensures their equality is provable. Quantifiers are handled the same way as function above — as they all a form of bind.

$$\frac{\Gamma \vdash c_1 \equiv c_2 \quad \Gamma; \Sigma \vdash \varphi_1 \equiv \varphi_2}{\Gamma; \Sigma \vdash [c_1] \wedge \varphi_1 \equiv [c_2] \wedge \varphi_2} \quad \frac{\Gamma \models a_1 = a_2 \quad \Gamma \models t_1 = t_2}{\Gamma \vdash (a_1 \# t_1) \equiv (a_2 \# t_2)}$$

To handle formulas with constraints we introduce constraint equivalence relation, which does nothing more than use solver to check that arguments and constructors of constraint are equal in the solver sense.

Chapter 5

Proof assistant

All the stuff mentioned above has their implementation in OCaml, in modules `Solver` and `SolverEnv`, `KindChecker` and `KindCheckerEnv`, `Proof` and `ProofEnv`, respectively.

Constraints, kinds and formulas constructors mirror the grammars we defined in previous chapters. Atoms and variables are represented internally by integers (but still are disjoint sets) — and their string *names* are kept in the environment and binders (quantifiers and functions).

Additionally, we provide a *proof assistant* (in module `Prover`), that enables the user to conveniently work with *backwards* and incomplete proof — inspired by the HOL family of theorem provers. While simple it is also powerful and easy to use.

The interface to the Prover provides multiple *tactics* (functions that manipulate *prover state*) and ways to combine them:

```
1 type goal_env = (string * formula) ProofEnv.env
2
3 type goal = goal_env * formula
4
5 type prover_state = S_Unfinished of {goal: goal; context: proof_context}
6                   | S_Finished of proof
7
8 type tactic = prover_state -> prover_state
9
10 val proof : goal_env -> formula -> prover_state
11
12 val qed : prover_state -> proof
13
14 val (|>) : prover_state -> tactic -> prover_state
15
16 val (%>) : tactic -> tactic -> tactic
17
18 val repeat : tactic -> tactic
19
20 val try_tactic : tactic -> tactic
```

We will use \bullet to indicate *holes* in the incomplete proofs:

$$\begin{array}{l}
\text{intro} \\
\Gamma; \Theta; \Sigma \vdash \bullet :: [c] \rightarrow \varphi \quad \rightsquigarrow \quad \Gamma, c; \Theta; \Sigma \vdash \bullet :: \varphi \\
\\
\text{intro' "x"} \\
\Gamma; \Theta; \Sigma \vdash \bullet :: \psi \rightarrow \varphi \quad \rightsquigarrow \quad \Gamma; \Theta, x :: \psi; \Sigma \vdash \bullet :: \varphi \\
\Gamma; \Theta; \Sigma \vdash \bullet :: \forall_A a. \varphi \quad \rightsquigarrow \quad \Gamma; \Theta; \Sigma, x :: a \vdash \bullet :: \varphi \\
\Gamma; \Theta; \Sigma \vdash \bullet :: \forall_T X. \varphi \quad \rightsquigarrow \quad \Gamma; \Theta; \Sigma, x :: X \vdash \bullet :: \varphi \\
\\
\text{apply_assm "H"} \\
\Gamma; \Theta; \Sigma \vdash \bullet :: \varphi \quad \rightsquigarrow \quad \Gamma; \Theta; \Sigma \vdash \bullet :: \psi \\
\text{when } (H :: \psi) \in \Theta \\
\\
\text{apply } (\psi \rightarrow \varphi) \\
\Gamma; \Theta; \Sigma \vdash \bullet :: \varphi \quad \rightsquigarrow \quad \Gamma; \Theta; \Sigma \vdash \bullet :: \psi \\
\Gamma; \Theta; \Sigma \vdash \bullet :: \psi \rightarrow \varphi \\
\\
\text{ex_false} \\
\Gamma; \Theta; \Sigma \vdash \bullet :: \varphi \quad \rightsquigarrow \quad \Gamma; \Theta; \Sigma \vdash \bullet :: \perp \\
\\
\text{by_solver} \\
\Gamma; \Theta; \Sigma \vdash \bullet :: c \quad \rightsquigarrow \quad \Gamma; \Theta; \Sigma \vdash c \\
\text{when } \Gamma \models c \\
\\
\text{compare_atoms "a" "b"} \\
\Gamma; \Theta; \Sigma \vdash \bullet :: \varphi \quad \rightsquigarrow \quad \Gamma; \Theta; \Sigma \vdash \bullet :: (a = a' \vee a \neq a') \rightarrow \varphi \\
\text{when } (a :: a) \in \Sigma \text{ and } (b :: a') \in \Sigma
\end{array}$$

Chapter 6

Case study: Progress and Preservation of STLC

The ultimate gold of our work is to create a logic for dealing with variable binding, and there's no better way to use than to prove some things about lambda calculus.

We will take a look on simply typed lambda calculus and examine proofs of its two major properties of *type soundness*: *progress* and *preservation*. Before we delve into the proofs, let's first establish needed relations:

$$\begin{aligned} \text{fix } \text{Type}(t) :: \star = & \quad (t = \text{base}) \\ & \vee \quad (\exists_T t_1, t_2. [X = \text{arrow } t_1 \ t_2] \wedge (\text{Type } T_1) \wedge (\text{Type } t_2)) \\ \text{fix } \text{InEnv}(\text{env}) :: \forall_A a. \forall_T t. \star = & \lambda_A a. \lambda_T t. \quad (\exists_T \text{env}'. \text{env} = \text{cons } a \ t \ \text{env}') \\ & \vee \quad (\exists_A b. \exists_T t', \text{env}'. [\text{env} = \text{cons } b \ t' \ \text{env}'] \wedge [a \neq b] \wedge (\text{InEnv} \\ & \dots \quad \dots \end{aligned}$$

As one would expect, we will need a lemma about *canonical forms*, which states all values are of *arrow* type and can be *inversed* into an abstraction term. (because we did not consider any true base type like a **Bool** or **Int**). Other lemmas are unimportant boilerplate.

```
1 let empty_contradiction_thm = lambda_thm
2   "forall a :atom. forall t :term. (InEnv nil a t) => false"
3
4 let typing_terms_thm = lambda_thm
5   "forall e env t : term. (Typing e env t) => (Term e)"
6
7 let canonical_form_thm = lambda_thm $ concat
8   [ "forall v t :term."
9     ; " (Value v) =>"
10    ; " (Typing v nil t) =>"
11    ; " (exists a :atom. exists e :term. [v = lam (a.e)] /\ (Term e))"
```

```

12     ; " /\ "
13     ; " (exists t1 t2 :term. [t = arrow t1 t2])" ]
14
15 let subst_exists_thm = lambda_thm $ unwords
16   [ "forall a :atom."
17     ; "forall v :term. (Value v) =>"
18     ; "forall e :term. (Term e) =>"
19     ; "exists e' :term. (Sub e a v e')" ]
20
21 let progress_thm = lambda_thm
22   "forall e t :term. (Typing e nil t) => (Progressive e)"

```

Otherwise the proof goes the same way as usual, simple induction over *Typing*.

```

1 let progress =
2   proof' progress_thm
3   |> by_induction "e0" "IH" %> intro %> destr_intro
4   |> intros' ["Ha"; "a"; ""]
5     (* e is a var in empty env - contradiction *)
6     %> ex_falso
7     %> apply_thm_specialized empty_contradiction ["a"; "t"]
8     %> assumption
9   |> intros' ["Hlam"; "a"; "e_a"; "t1"; "t2"; " "; " "; " "]
10     (* e is a lambda - value *)
11     %> case "value"
12     %> case "lam"
13     %> exists' ["a"; "e_a"]
14     %> by_solver
15     %> apply_thm_specialized typing_terms ["e_a"; "cons a t1 nil"; "t2"]
16     %> assumption
17   |> intros' ["Happ"; "e1"; "e2"; "t2"; " "; " "]
18     (* e is an application - steps *)
19   |> add_assumption_parse "He1" "Progressive e1"
20   |> add_assumption_parse "He2" "Progressive e2"
21   |> destruct_assm "He1"
22     %> intros ["Hv1"]
23     %> destruct_assm "He2"
24     %> intros ["Hv2"] (* Value e1, Value e2 *)
25     %> ( add_assumption_thm_specialized "He1lam" canonical_form' ["e1";
26       "t2"; "t"]
27       (* He1lam: [e1 = lam (a.e_a)] /\ (Term e_a) *)
28       %> apply_in_assm "He1lam" "Hv1"
29       %> apply_in_assm "He1lam" "Happ_1"
30       %> destruct_assm' "He1lam" ["a"; "e_a"; " "] )
31     %> ( add_assumption_thm_specialized "He_a" subst_exists ["a"; "e2";
32       "e_a"]
33       %> apply_in_assm "He_a" "Hv2"
34       %> apply_in_assm "He_a" "He1lam"
35       %> destruct_assm' "He_a" ["e_a'"] (* He_a: Sub e_a a e2 e_a' *) )
36     %> case "steps"
37     %> exists "e_a'"
38     %> case "app"
39     %> exists' ["a"; "e_a"; "e2"]
40     %> by_solver

```

```

39     %> destruct_goal
40     %> apply_assm "Hv2"
41     %> apply_assm "He_a"
42 |> intros' ["Hs2"; "e2'"] (* Value e1, Steps e2 e2' *)
43     %> case "steps"
44     %> exists "app e1 e2'"
45     %> case "app_r"
46     %> exists' ["e1"; "e2"; "e2'"]
47     %> by_solver
48     %> by_solver
49     %> destruct_goal
50     %> apply_assm "Hv1"
51     %> apply_assm "Hs2"
52 |> intros' ["Hs1"; "e1'"] (* Steps e1 *)
53     %> case "steps"
54     %> exists "app e1' e2"
55     %> case "app_l"
56     %> exists' ["e1"; "e1'"; "e2"]
57     %> by_solver
58     %> by_solver
59     %> apply_assm "Hs1"
60 |> apply_assm_specialized "IH" ["e2"; "t2"] %> by_solver
61     %> apply_assm "Happ_2" (* Progressive e2 *)
62 |> apply_assm_specialized "IH" ["e1"; "arrow t2 t"] %> by_solver
63     %> apply_assm "Happ_1" (* Progressive e1 *)
64 |> qed

```

To prove *Preservation*, we will need more lemmas:

1. Substitution lemma: if term e has a type t in environment $\text{cons } a \text{ ta env}$, then we can substitute a for any value v of type ta in e without breaking the typing.

```
1 let sub_lemma_thm = lambda_thm $ concat
2   [ "forall e env t :term."
3     ; "forall a : atom. forall ta :term."
4     ; "forall v e' :term."
5     ; " (Typing v env ta) =>"
6     ; " (Typing e {cons a ta env} t) =>"
7     ; " (Sub e a v e') =>"
8     ; " (Typing e' env t)" ]
```

2. Swap lemma: If we have a typing of e in env then we can swap a with (*fresh enough*) b in both e and env without breaking the typing. This is particularly useful for manipulating the abstraction terms — we can have any atom we want in the argument position while preserving typing.

```
1 let swap_lambda_typing_lemma_thm = lambda_thm $ unwords
2   [ "forall e env t :term. "
3     ; "forall a b :atom. forall t' :term. "
4     ; " [b # a e] => "
5     ; " (Typing {e} {cons a t' env} t) => "
6     ; " (Typing {[a b]e} {cons b t' env} t)" ]
```

3. Weakening lemma: for any environment env_1 , we can use larger environment env_2 without breaking the typing.

```
1 let weakening_lemma_thm = lambda_thm $ concat
2   [ "forall e env1 t env2 : term."
3     ; " (Typing e env1 t) =>"
4     ; " (EnvInclusion env1 env2) =>"
5     ; " (Typing e env2 t)" ]
```

Now to the proof:

```
1 let preservation =
2   let contra_var = intros' ["contra"; "_"; ""] %> discriminate in
3   let contra_app = intros' ["contra"; "_e1"; "_e2"; "_t2"; ""] %>
4     discriminate in
5   let deduce_app_typing =
6     destruct_assm "Htyp"
7     %> (intros' ["contra"; "_"; ""] %> discriminate)
8     %> (intros' ["contra"; "_"; "e_"; "t1"; "t2"; ""] %> discriminate)
9     %> intros' ["Happ"; "e_1"; "e_2"; "t2"; ""; ""]
10  in
11  proof' preservation_thm
12  |> by_induction "e0" "IH"
13  |> intro %> intro %> intro %> intros ["Htyp"; "Hstep"]
14  |> destruct_assm "Hstep"
15  |> intros' ["He1"; "e1"; "e1'"; "e2"; ""; ""]
16    (* e = app e1 e2, Steps e1 e1' *)
17    %> deduce_app_typing
```

```

17   %> case "app"
18   %> exists' ["e1'"; "e2"; "t2"]
19   %> by_solver
20   %> destruct_goal
21   %> apply_asm_specialized "IH" ["e1"; "e1'"; "env"; "arrow t2 t"]
22   (* Typing e1 env {arrow t2 t} =>
23     Steps e1 e1' => Typing e1' env {arrow t2 t} *)
24   %> by_solver
25   %> apply_asm "Happ_1"
26   %> apply_asm "He1"
27   (* Typing e2 env t2 *)
28   %> apply_asm "Happ_2"
29 |> intros' ["He2"; "v1"; "e2"; "e2'"; ""; ""; ""]
30   (* e = app v1 e2, Value e1, Steps e2 e2' *)
31   %> deduce_app_typing
32   %> case "app"
33   %> exists' ["v1"; "e2'"; "t2"]
34   %> by_solver
35   %> destruct_goal
36   (* Typing e1 env {arrow t2 t} *)
37   %> apply_asm "Happ_1"
38   (* Typing e2 env t2 => Steps e2 e2' => Typing e2' env t2*)
39   %> apply_asm_specialized "IH" ["e2"; "e2'"; "env"; "t2"]
40   %> by_solver
41   %> apply_asm "Happ_2"
42   %> apply_asm "He2_2"
43 |> intros' ["Hbeta"; "a"; "e_a"; "v"; ""; ""]
44   (* e = app (lam (a.e_a)) v, Value v *)
45   %> deduce_app_typing
46   %> destruct_asm "Happ_1"
47   %> contra_var (* e_1 /= var *)
48   %> intros' ["Hlam"; "b"; "e_b"; "t1b"; "t2b"; ""; ""; ""] (* e_1 = b
49   .e_b *)
50   %> apply_thm_specialized sub_lemma ["e_a"; "env"; "t"; "a"; "t2"; "v
51   "; "e'"]
52   (* Typing v env t2 => Typing e_a {cons a t2 env} t =>
53     Sub e_a a v e' => Typing e' env t *)
54   %> apply_asm "Happ_2" (* Typing v env t2 *)
55   %> compare_atoms "a" "b" (* Typing e_a cons a t2 env t *)
56   %> destr_intro
57   (* a = b *) %> apply_asm "Hlam_2"
58   %> destr_intro (* a /= b *)
59   (* [a # b e_b] => Typing e_b {cons b t2 env} t =>
60     Typing {[b a]e_b} {cons a t2 env} t *)
61   %> apply_thm_specialized
62     swap_lambda_typing ["e_b"; "env"; "t"; "b"; "a"; "t2"]
63   %> by_solver
64   %> apply_asm "Hlam_2"
65   %> apply_asm "Hbeta_2" (* Sub e_a a v e' *)
66   %> contra_app (* e_1 /= app _ _ *)
67 |> qed

```


Chapter 7

Conclusion and future work

...

Bibliography

[1] ...