Part II
Barbanera and Berardi’s proof of strong normalisation for 2nd-order classical logic

Barbanera and Berardi’s calculus is a 1-sided version of Curien-Herbelin-Wadler’s: terms and continuations are merged into 1 syntax (this gives half as many cases to treat in your proofs).

Types  
\[ A, B, C, \ldots ::= \alpha | \alpha^\perp | A \lor B | A \land B | \exists \alpha.A | \forall \alpha.A \]

Terms  
\[ t, u, v, \ldots ::= x | \mu x.p | \text{inj}_1(t) | \text{inj}_2(t) | \langle t, u \rangle | \langle \_ , t \rangle | \Lambda_{\_} t \]

Commands  
\[ p ::= (t \cdot u) \]

Negation:
\[ (\alpha^\perp)^t ::= \alpha \]
\[ (A \land B)^t ::= A^\perp \lor B^\perp \]
\[ (A \lor B)^t ::= A^\perp \land B^\perp \]
\[ (\forall \alpha. A)^t ::= \exists \alpha. A^\perp \]
\[ (\exists \alpha. A)^t ::= \forall \alpha. A^\perp \]

The following reduction rules apply anywhere in terms and commands:
\[ \langle \mu x.p \cdot t \rangle \rightarrow [\gamma_x]p \]
\[ \langle \langle t_1, t_2 \rangle \cdot \text{inj}_1(t) \rangle \rightarrow \langle t_1, t \rangle \]
\[ \langle \Lambda_{\_} t \cdot \langle \_ , u \rangle \rangle \rightarrow \langle \_ , u \rangle \]

Let \text{Var} denote the set of term variables, and \text{SN} (resp. \text{SN}^\perp) denote the set of strongly normalising terms (resp. commands) for the reduction relation induced by the above rules.

Notice that the calculus does not satisfy confluence, with the obvious critical pair:
\[ \langle \mu x.p_1 \cdot \mu y.p_2 \rangle \]
\[ \langle \mu y.p_x \rangle p_1 \quad \langle \mu x.p_y \rangle p_2 \]

Exercise 1: Orthogonality and saturation
We start with a few definitions:
- \[ t \perp u \text{ if } \langle t \cdot u \rangle \in \text{SN}^\perp \]
- A pair \((\mathcal{U}, \mathcal{V})\) of sets of terms is
  - orthogonal if \( \forall t \in \mathcal{U}, \forall u \in \mathcal{V}, t \perp u \)
  - saturated if the following two conditions hold
    1. \( \text{Var} \subseteq \mathcal{U} \) and \( \mathcal{V} \subseteq \mathcal{V} \)
    2. \( \{ \mu x.(t \cdot u) | \forall v \in \mathcal{V}, \langle \gamma_x t \rangle \perp \langle \gamma_x u \rangle \} \subseteq \mathcal{U} \) and
       \( \{ \mu x.(t \cdot u) | \forall v \in \mathcal{U}, \langle \gamma_x t \rangle \perp \langle \gamma_x u \rangle \} \subseteq \mathcal{V} \).

1. [*] Briefly justify (no full proof required) why
- \((\mathcal{U}, \mathcal{V})\) is orthogonal if and only if \( \mathcal{U} \subseteq \text{SN} \).
- If \( \langle \gamma_x \rangle (t \cdot u) \in \text{SN}^\perp \) then we have \( \langle t \cdot u \rangle \in \text{SN}^\perp \).
- As reduction is stable under substitution, an infinite reduction sequence starting from \( \langle t \cdot u \rangle \) would provide one starting from \( \langle \gamma_x \rangle (t \cdot u) \).
- If \( \langle \gamma_x \rangle (t \cdot u) \in \text{SN}^\perp \) and \( v \in \text{SN} \) is not of the form \( \mu x.p \), then we have \( \langle v \cdot \mu x.(t \cdot u) \rangle \in \text{SN}^\perp \) and \( \langle \mu x.(t \cdot u) \cdot v \rangle \in \text{SN}^\perp \).
- If \( \langle \gamma_x \rangle (t \cdot u) \in \text{SN}^\perp \) then from the previous point \( \langle t \cdot u \rangle \in \text{SN}^\perp \) and \( \mu x.(t \cdot u) \in \text{SN}^\perp \), so as \( v \in \text{SN} \) as well, an infinite reduction sequence starting from \( \langle v \cdot \mu x.(t \cdot u) \rangle \) has to reduce, at some point, the top-level redex, and the only possible way is
to \(\langle \gamma, x \rangle\) \(\langle t', u' \rangle\) for some reduced forms \(t', u', v'\) of \(t, u, v\); this would provide an infinite reduction sequence from \(\langle \gamma, x \rangle\) \(\langle t, u \rangle\).

A similar reasoning proves \(\langle \mu x (t \bullet u) \bullet v \rangle \in \text{SN}^c\), or alternatively we can use the symmetry of the calculus: given the reduction rules, a command \(\langle u \bullet v \rangle \in \text{SN}^c\) if and only if \(\langle v \bullet u \rangle \in \text{SN}^c\).

2. Given an orthogonal pair \((U, V)\) of non-empty sets, prove that \(U \subseteq \text{SN}\) and \(V \subseteq \text{SN}\).

Correction: For all \(u \in U\), take \(v\) the non-empty set \(V\); since \(u \perp v\) we have \(u \in \text{SN}\). Same argument for \(V\).

Exercise 2: Saturated extensions of simple pairs

A set of terms is said to be simple if it is non-empty and it contains no term of the form \(\mu x t\).

In this exercise we want to build a "saturating" function \(\text{sat}(\cdot, \cdot)\), i.e. a function such that, for any orthogonal pair \((U, V)\) of simple sets, \(\text{sat}(U, V)\) is a saturated and orthogonal pair of sets \((U', V')\) that extends \((U, V)\) (i.e. such that \(U \subseteq U'\) and \(V \subseteq V'\)).

1. For every set \(U\) of terms, we define a function
\[
\Phi_U(W) := U \cup \text{Var} \cup \{\mu x (t \bullet u) \mid \forall v \in W, \langle \gamma, x \rangle t \perp \langle \gamma, x \rangle u\}
\]
Prove that \(\Phi_U\) is anti-monotonic (i.e. if \(W \subseteq W'\) then \(\Phi_U(W) \supseteq \Phi_U(W')\)).

Correction: If \(W \subseteq W'\) then for any \(t, u, v \in W', \langle \gamma, x \rangle t \perp \langle \gamma, x \rangle u\) implies \(\forall v \in W, \langle \gamma, x \rangle t \perp \langle \gamma, x \rangle u\), so \(\Phi_U(W') \supseteq \Phi_U(W)\).

2. Given two sets of terms \(U\) and \(V\), prove that \(\Phi_U \circ \Phi_V\) admits a fixed point (a set \(U'\) such that \(\Phi_U(\Phi_V(U')) = U'\)).

Correction: From the previous question, \(\Phi_U \circ \Phi_V\) is a monotonic set transformation, so it admits the fixpoint \(\bigcup_{n \in \mathbb{N}} (\Phi_U \circ \Phi_V)^n(\emptyset)\).

3. Let \(U'\) be a fixed point of \(\Phi_U \circ \Phi_V\), and let \(V' := \Phi_V(U')\). Prove the following:
\[
\begin{align*}
U' &= U \cup \text{Var} \cup \{\mu x (t \bullet u) \mid \forall v \in V', \langle \gamma, x \rangle t \perp \langle \gamma, x \rangle u\} \\
V' &= V \cup \text{Var} \cup \{\mu x (t \bullet u) \mid \forall v \in U', \langle \gamma, x \rangle t \perp \langle \gamma, x \rangle u\}
\end{align*}
\]

Correction: Just by unfolding the definitions: the first equality is the unfolding of the fixpoint equality \(U' = \Phi_U(\Phi_V(U'))\); then second one is the unfolding of \(V' := \Phi_V(U')\).

4. Prove that the pair \((U', V')\) is saturated and extends \((U, V)\).

Correction: This can be read directly on the above equations.

5. [*] Assume that \((U, V)\) is an orthogonal pair of simple sets; prove that the pair \((U', V')\) is orthogonal.

Correction: First, notice that as \(U\) and \(V\) are assumed simple, they are in particular non-empty and, by Ex.1-Q.2, \(U \subseteq \text{SN}\) and \(V \subseteq \text{SN}\).

Second, by induction on \(n \in \mathbb{N}\), notice that \((\Phi_U \circ \Phi_V)^n(\emptyset) \subseteq \text{SN}\) and \(\Phi_V(\Phi_U \circ \Phi_V)^n(\emptyset) \subseteq \text{SN}\) (each induction step uses Ex.1-Q.1.2).

Third, we conclude from this that \(U' \subseteq \text{SN}\) and \(V' \subseteq \text{SN}\).

Now let \(u \in U'\) and \(v \in V'\). We show \(u \perp v\) by case analysis on the different subsets composing \(U'\) and \(V'\):

<table>
<thead>
<tr>
<th>(u)(\mid v)</th>
<th>(\text{Var})</th>
<th>({\mu x (v_1 \bullet v_2) \mid \forall u \in U', \langle \gamma, x \rangle v_1 \perp \langle \gamma, x \rangle v_2})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(U)</td>
<td>(\langle U, V \rangle) assumed orthogonal</td>
<td>1</td>
</tr>
<tr>
<td>(\text{Var})</td>
<td>1</td>
<td>No reduction</td>
</tr>
<tr>
<td>({\mu x (u_1 \bullet u_2) \mid \forall v \in V', \langle \gamma, x \rangle u_1 \perp \langle \gamma, x \rangle u_2})</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

1: By Ex.1-Q.1.1. \(\langle U, \text{Var} \rangle\) and \(\langle V, \text{Var} \rangle\) are orthogonal pairs.
2 and 3: By Ex.1-Q.1.3.
4: This is the interesting case: \(u = \mu x (u_1 \bullet u_2)\) and \(v = \mu x (v_1 \bullet v_2)\).

Assume there is an infinite reduction sequence from \(\{\mu x (u_1 \bullet u_2) \bullet \mu y (v_1 \bullet v_2)\}\). As both
where we write valuation

\[ A \]

3. Prove that

\[
\{\mu x.(u_1 \bullet u_2)^y\} \in SN \text{ and } \mu y.(v_1 \bullet v_2) \in SN, \text{ the reduction sequence must reduce the}
\]

top-level redex at some point, to either \( \{\mu y.(v_1 \bullet v_2)^y\}\) or \( \{\mu x.(u_1 \bullet u_2)^y\}\)

for some reduced forms \( u_1', u_2', v_1', v_2' \) of \( u_1, u_2, v_1, v_2 \).

We treat both cases: \( \{\mu y.(v_1 \bullet v_2)^y\}\) is a reduced form of \( \{\gamma y\} \), which is in

\( SN; \{\mu x.(u_1 \bullet u_2)^y\}\) is a reduced form of \( \{\gamma y\} \), which is in \( SN \). We finally define \( \text{sat}r(U, V) := \langle U', V' \rangle \).

**Exercise 3: Semantics**

The general idea: a type \( A \) is interpreted

- first as an orthogonal pair of simple sets
- then as an orthogonal and saturated pair of sets

where we write \( \mathcal{P}^+ \) (resp. \( \mathcal{P}^- \)) for the first (resp. second) component of a pair \( \mathcal{P} \).

Let \( \mathcal{H} \) be the set of all orthogonal pairs of simple sets (of terms). A valuation \( \sigma \) is a mapping from type variables to \( \mathcal{H} \).

1. Given some sets of terms \( U \) and \( V \), we define the following set constructions:

\[
\text{inj}_1(U) := \{t \in U \} \quad \langle U, V \rangle := \{(u, v) \mid u \in U, v \in V\}
\]

\[
\text{inj}_2(U) := \{t \in U \} \quad \Lambda U := \{u \in U \}
\]

Prove that these sets are always simple if \( U \) and \( V \) are non-empty.

**Correction:** None of these sets contains any term of the form \( \mu x.c \), and none of them is empty if \( U \) and \( V \) are non-empty.

We define the following semantics \( _\alpha \) and \( _\alpha \) :

\[
[a]_\sigma := \sigma(\alpha)
\]

\[
[A \cup B]_\sigma^+ := \text{inj}_1([A]_\sigma^+) \cup \text{inj}_2([B]_\sigma^+)
\]

\[
[A \cup B]_\sigma^- := ([A]_\sigma^- \cup [B]_\sigma^-)
\]

\[
[[\alpha, A]_\sigma := \bigcup_{h \in H} [A]_{\sigma, a \mapsto h}
\]

\[
[[A]_\sigma^+, [A]_\sigma^- := \Lambda \bigcap_{h \in H} [A]_{\sigma, a \mapsto h}
\]

\[
([A]_\sigma^+, [A]_\sigma^-) := \text{sat}(\{B_o\} A)_\sigma \quad \text{if } A \text{ is of the form } \alpha, A_1 \land A_2, \exists \alpha A.
\]

2. Prove that if \( [A]_\sigma = \langle U, V \rangle \) then \( [A]_\sigma^+ = \langle V, U \rangle \) and if \( [A]_\sigma = \langle U, V \rangle \) then \( [A]_\sigma^- = \langle U, V \rangle \).

**Correction:** If \( A \) is of the form \( \alpha, A_1 \lor A_2, \exists \alpha A \), the first point is by line 4 and the second point is by line 6. If \( \alpha \) the form \( \alpha, A_1 \land A_2, \forall \alpha A \) is the same lines again, noticing the involutivity of negation: \( A^{\perp} = A \).

3. Prove that \( [A]_{\sigma, A \Rightarrow B} = \{B_o\} A \) and \( [A]_{\sigma, A \Rightarrow B} = \{B_o\} A \).

**Correction:** By induction on \( A \).

4. [*] Prove, by induction on \( A \), that \( [A]_\sigma \) is an orthogonal pair of simple sets and \( [A]_\sigma \) is a saturated orthogonal pair extending \( [A]_\sigma \).

**Correction:** For \( A = \alpha \), the first point is by definition of \( \mathcal{H} \). For \( A = A_1 \lor A_2 \) or \( A = \exists \alpha A \), \( [A]_\sigma \) is a pair of simple sets by Q.1.

To prove that \( [A_1 \lor A_2]_\sigma \) is orthogonal, let \( u \in \text{inj}_1([A_1]_\sigma^+) \cup \text{inj}_2([A_2]_\sigma^+) \) and \( v \in ([A_1]_\sigma^+, [A_2]_\sigma^-) \).

We have \( u = \text{inj}_1(u_0) \) with \( u_0 \in [A_1]_\sigma^+ \) for either \( i = 1 \) or \( i = 2 \), while \( v = (v_1, v_2) \) with \( v_1 \in [A_1]_\sigma^+ \) and \( v_2 \in [A_2]_\sigma^+ \). Now the induction hypothesis gives that \( [A_1]_\sigma^+ \) and \( [A_2]_\sigma^+ \) are orthogonal pairs extending the pairs \( [A_1]_\sigma^+ \) and \( [A_2]_\sigma^+ \) of non-empty sets. So \( [A_1]_\sigma^+ \), \( [A_2]_\sigma^+ \), \( [A_1]_\sigma^- \), \( [A_2]_\sigma^- \) are themselves non-empty, and by Ex.1-Q.2 they are all included in \( SN \). Hence, \( u \) and \( v \) are in \( SN \). So an infinite
A substitution

Exercise 4: Proof of Strong Normalisation

1. [*] Prove the

\( \Gamma \vdash t: A \) for \( A = \forall a. A' \), \([A]_\sigma\) is an orthogonal pair of simple sets because it is \( ([A]^-_\sigma, [A]^+_\sigma) \).

For \( A = a \), \( A = A_1 \lor A_2 \) or \( A = \exists a. A' \), \([A]_\sigma\) is a saturated and orthogonal pair extending \([A]_\sigma\)

by Ex.3-Q.4 and Ex.2-Q.5.

For \( A = a \), \( A = A_1 \land A_2 \), \( A = \forall a. A' \), \([A]_\sigma\) a saturated and orthogonal pair extending \([A]_\sigma\)

because it is \( ([A]^-_\sigma, [A]^+_\sigma) \).

Exercise 4: Proof of Strong Normalisation

A substitution \( \rho \) is a mapping from term variables to terms. Applying a substitution \( \rho \) to a term \( t \) (in a capture-avoiding way) yields a term denoted \( t\rho \). For each typing context \( \Gamma \) we define the set

\( \Gamma^+ := \{ \rho \mid \forall x : A \in \Gamma, \rho(x) \in [A]_\sigma^+ \} \)

1. [*] Prove the Adequacy Lemma:

If \( \Gamma \vdash t : A \), then for all valuation \( \sigma \) and all substitutions \( \rho \in [\Gamma]_\sigma \) we have \( t\rho \in [A]_\sigma^+ \).

**Correction:** By induction on the typing tree, with the following statement for commands:

If \( \Gamma \vdash c \), then for all valuation \( \sigma \) and all substitutions \( \rho \in [\Gamma]_\sigma \) we have \( c\rho \in \text{SN}^c \).

- \( \Gamma \vdash x : A \)

Let \( \sigma \) be a valuation and \( \rho \in [\Gamma]_\sigma \). We have \( x\rho = \rho(x) \in [A]_\sigma^+ \) by assumption that \( \rho \in [\Gamma]_\sigma \).

- \( \Gamma, x : A \vdash p \)

\( \Gamma \vdash \mu x p : A^\perp \)

Let \( \sigma \) be a valuation and \( \rho \in [\Gamma]_\sigma \). We need to show \( (\mu x p)\rho \in [A]_\sigma^+ \). Let us rewrite \( (\mu x p)\rho \) as \( \mu x (pp) \) (avoiding variable capture). Since \([A]_\sigma^-\) is a saturated pair (Ex.3-Q.4), it suffices to show that for all \( v \in [A]_\sigma^+ \), we have \( \{v\} (pp) \in \text{SN}^c \). Let \( v \in [A]_\sigma^+ = [A^\perp]_\sigma^+ \) (Ex.3-Q.2). Notice that \( \{v\} (pp) = p(\rho, x \mapsto v) \), and that \( (\rho, x \mapsto v) \in [\Gamma, x : A^\perp]_\sigma \). The induction hypothesis concludes want we want.

- \( \Gamma \vdash t : A \quad \Gamma \vdash u : A^\perp \)

\( \Gamma \vdash (t \bullet u) \)

Let \( \sigma \) be a valuation and \( \rho \in [\Gamma]_\sigma \). The induction hypothesis gives \( t\rho \in [A]_\sigma^+ \) and \( u\rho \in [A^\perp]_\sigma^+ = [A]_\sigma^- \). Since \([A]_\sigma^-\) is an orthogonal pair (Ex.3-Q.4), \( (t \bullet u)\rho = (t\rho \bullet u\rho) \in \text{SN}^c \).
2. [*] Prove Strong Normalisation: If $\Gamma \vdash t : A$ then $t \in \text{SN}$. 
(Hint: choose a valuation $\sigma$ and a substitution $\rho$ appropriately.)

**Correction:** Take $\sigma$ to map every type variable $\alpha$ to the orthogonal pair $(\text{Var, Var})$ of simple sets. Take $\rho$ to be the identity substitution mapping every term variable to itself. We have $\rho \in [\Gamma]_\sigma$ since for every type $B$, $[B]_\sigma$ is saturated (Ex.3-Q.4), so $\text{Var} \subseteq [B]_\sigma^+$, and therefore for every declaration $x : B$ in $\Gamma$, $\rho(x) = x \in [B]_\sigma^+$. 

The Adequacy Lemma gives $t\rho \in [A]_\sigma^+$, and as $t\rho = t$ and $[A]_\sigma^+ \subseteq \text{SN}$ we have $t \in \text{SN}$. 

\[
\begin{align*}
\Gamma \vdash t : A & \quad \Gamma \vdash u : B \\
\Gamma \vdash (t,u) : A \land B
\end{align*}
\]

Let $\sigma$ be a valuation and $\rho \in [\Gamma]_\sigma$. The induction hypothesis gives $t\rho \in [A]_\sigma^+$ and $u\rho \in [B]_\sigma^+$. So $(t\rho,u\rho) \in [A \land B]_\sigma^+$, and since $[A \land B]_\sigma$ extends $[A \land B]_\sigma$ (Ex.3-Q.4), we have $(t,u)\rho = (t\rho,u\rho) \in [A \land B]_\sigma^+$.

\[
\begin{align*}
\Gamma \vdash t : A_i \\
\Gamma \vdash \text{inj}_i(t) : A_1 \lor A_2
\end{align*}
\]

Let $\sigma$ be a valuation and $\rho \in [\Gamma]_\sigma$. The induction hypothesis gives $t\rho \in [A_i]_\sigma^+$ and $\text{inj}_i(t\rho) \in [A_1 \lor A_2]_\sigma^+$, and since $[A_1 \lor A_2]_\sigma$ extends $[A_1 \lor A_2]_\sigma$ (Ex.3-Q.4), we have $(\text{inj}_i(t))\rho = \text{inj}_i(t\rho) \in [A_1 \lor A_2]_\sigma^+$.

\[
\begin{align*}
\Gamma \vdash t : B \\
\Gamma \vdash A_\forall t : \forall \alpha. B
\end{align*}
\]

Let $\sigma$ be a valuation and $\rho \in [\Gamma]_\sigma$. Since $\alpha \notin \text{FV}(\Gamma)$, $[\Gamma]_\sigma = [\Gamma]_{\sigma,\alpha \rightarrow h}$ for any $h \in \mathcal{H}$. So we can apply the induction hypothesis to obtain $t\rho \in [B]_{\sigma,\alpha \rightarrow h}^+$ for any $h \in \mathcal{H}$. So $A_\forall t\rho \in [\forall \alpha. B]_\sigma^+$, and since $[\forall \alpha. B]_\sigma$ extends $[\forall \alpha. B]_\sigma$ (Ex.3-Q.4), we have $(A_\forall t)\rho = A_\forall t\rho \in [\forall \alpha. B]_\sigma^+$.

\[
\begin{align*}
\Gamma \vdash t : \{B_\alpha\} A \\
\Gamma \vdash (\_ ,t) : \exists \alpha. A
\end{align*}
\]

Let $\sigma$ be a valuation and $\rho \in [\Gamma]_\sigma$. So we can apply the induction hypothesis to obtain $t\rho \in [\{B_\alpha\} A]_\sigma^+$, so by Ex.3-Q.3, $t\rho \in [A]_{\sigma,\alpha \rightarrow h}^+$. In other words, $t\rho \in [A]_{\sigma,\alpha \rightarrow h}^+$ for the particular choice of $h = |B|_\sigma$, and by Ex.3-Q.4, $h \in \mathcal{H}$. So $(\_ ,t)\rho \in [\exists \alpha. A]_\sigma^+$, and since $[\exists \alpha. A]_\sigma$ extends $[\exists \alpha. A]_\sigma$ (Ex.3-Q.4), we have $(\_ ,t)\rho = (\_ ,t\rho) \in [\exists \alpha. A]_\sigma^+$. 

\[7\]