Exercise 1 : Curry-Howard Isomorphism (8 points)

Give proofs of the following propositional formula using the Curry-Howard isomorphism between constructive logic and typed λ-calculus with products and sums (see Appendix A for details).

1. $(A \wedge B) \Rightarrow C \Rightarrow ((C \wedge A) \wedge B)$

   Solution: $\lambda x : (A * B).\ (\lambda y : C.((y, x.\_1), x.\_2))$

2. $(A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow (A \vee B) \Rightarrow C$

   Solution: $\lambda x : (A \rightarrow C).\lambda y : (B \rightarrow C).\lambda z : (A+B).(\texttt{ case } z \texttt{ of } \texttt{inl } a \Rightarrow x\ a \mid \texttt{inr } b \Rightarrow y\ b)$

3. $((A \vee B) \Rightarrow C) \Rightarrow ((A \Rightarrow C) \wedge (B \Rightarrow C))$

   Solution: $\lambda k : (A + B) \rightarrow C.\ (\lambda a : A.\ k\ (\texttt{inl}\ a), \lambda b : B.\ k\ (\texttt{inr}\ b))$

4. $((A \Rightarrow B \vee C) \wedge (B \Rightarrow D) \wedge (C \Rightarrow D)) \Rightarrow (A \Rightarrow D)$

   Solution: $\lambda fgh : (A \rightarrow B + C) * (B \rightarrow D) * (C \rightarrow D).\ \lambda x : A.\ \texttt{case}\ fgh.\_1\ x\ \texttt{of}\ \texttt{inl}\ b \Rightarrow g\ b \mid \texttt{inr}\ c \Rightarrow h\ c)$

Exercise 2 : Type reconstruction for lists (10 points)

In this exercise, we consider the simply-typed lambda calculus (Appendix B) with booleans and natural numbers (Appendix C) but with no other extensions (in particular, there's no subtyping or `Bot` type). We extend this calculus with primitives for lists and operations on lists with operational semantics provided in Appendix D:

t	::=	...	**Terms**
	|	`nil`	Empty list
	|	`cons t t`	List constructor
	|	`head t`	Head of a list
	|	`tail t`	Tail of a list
	|	`isnil t`	Test for empty list

v	::=	...	**Values**
	|	`nil`	Empty list
	|	`cons v v`	List constructor

T	::=	...	**Types**
	|	`List T`	Type of a list with elements of type `T`

Now, your task is to extend the type system of the original calculus with rules for type reconstruction that accommodate additional syntactic forms, without adding new terms or types to the calculus. In order to fulfill the assignment, do one of the following for the new terms:

- Specify additional cases for the type reconstruction algorithm TP introduced at the lecture of Week 9 of the course.
- *Or* provide additional constraint-based typing rules for the type reconstruction algorithm explained in Chapter 22 of "Types and Programming Languages".

A refresher: `cons`, `head` and `tail` work like in all functional languages. `cons` prepends an element in its first argument to a list in its second argument. `head` cuts the 1st element from a list and returns it. `tail` cuts the 1st element from a list and returns the remaining list. Examples: `head (cons x xs) == x`, `tail (cons x xs) == xs` for all `x` and `xs`.

Solution:

$\Gamma \vdash \texttt{nil} : \texttt{List T1} \mid \emptyset,\ \texttt{T1}\ \textit{fresh}$

$$\frac{\Gamma \vdash t_1 : \texttt{T1} \mid \texttt{C1} \qquad \Gamma \vdash t_2 : \texttt{T2} \mid \texttt{C2}}{\Gamma \vdash \texttt{cons}\ t_1\ t_2 : \texttt{T2} \mid \texttt{C1} \cup \texttt{C2} \cup \{\texttt{List T1} = \texttt{T2}\}}$$

$$\frac{\Gamma \vdash t_1 : \texttt{T1} \mid \texttt{C1}}{\Gamma \vdash \texttt{head}\ t_1 : \texttt{T2} \mid \texttt{C1} \cup \{\texttt{T1} = \texttt{List T2}\},\ \texttt{T2}\ \textit{fresh}}$$

$$\frac{\Gamma \vdash t_1 : \texttt{T1} \mid \texttt{C1}}{\Gamma \vdash \texttt{tail}\ t_1 : \texttt{T1} \mid \texttt{C1} \cup \{\texttt{T1} = \texttt{List T2}\},\ \texttt{T2}\ \textit{fresh}}$$

$$\frac{\Gamma \vdash t_1 : \texttt{T1} \mid \texttt{C1}}{\Gamma \vdash \texttt{isnil}\ t_1 : \texttt{Bool} \mid \texttt{C1} \cup \{\texttt{T1} = \texttt{List T2}\},\ \texttt{T2}\ \textit{fresh}}$$

Exercise 3 : Subtyping for products (10 points)

The subtyping rule for products can be stated as:

$$\frac{S_1 <: T_1 \quad S_2 <: T_2}{S_1 \times S_2 \ <: \ T_1 \times T_2} \qquad (S-PROD)$$

In the course you were presented with the inversion lemma for subtyping with function types i.e., `S-ARROW`. Your task for this exercise is to write a proof for the following theorem for STLC with products and subtyping.

Theorem: If $S_1 \times S_2 <: T$, then either $T = Top$ or else $T = T_1 \times T_2$, with $S_1 <: T_1$ and $S_2 <: T_2$. Hint: Proof the theorem by induction on the last used subtyping rule. State any lemmas that you use (without proof).

Solution:

We prove the theorem by induction on the subtyping derivation rule size. The last subtyping rule applied can be:

- `S-REFL` - immediate from the result we know that $T = S_1 \times S_2$ and by using `S-REFL` (twice, on S_1 and S_2) we are done.
- `S-TRANS` - $S_1 \times S_2 <: U$ and $U <: T$ for some U. By IH we know that `U` is either `Top` or else $U = U_1 \times U_2$.
  - $U = Top$ - then $Top <: T$ and $T = Top$ (assuming a straightforward lemma saying that for any `S` such that $Top <: S$ we have that $S = Top$).
  - $U = U_1 \times U_2$ - by IH we know that since $U_1 \times U_2 <: T$ then either $T = Top$ or $T = T_1 \times T_2$ and $U_1 <: T_1$ and $U_2 <: T_2$. The first case, we are done, in the latter by `S-TRANS` we have that $S_1 <: T_1$ and $S_2 <: T_2$.
- `S-TOP` - the result is immediate since $T = Top$.
- `S-PROD` - $T = T_1 \times T_2$, and from the premises we know that $S_1 <: T_1$ and $S_2 <: T_2$.
- `S-ARROW` - not possible.

Appendix A: **Curry-Howard Isomorphism**

Curry-Howard isomorphism or *Curry-Howard correspondence* establishes a connection between type systems and logical calculi based on an observation that the ways we build types are structurally similar to the ways we build formulae.

According to Curry-Howard isomophism proofs can be represented as programs and formulae they prove can be represented as types of those programs. Here is a (non-comprehensive) list of some examples of how concepts from constructive logic are correlated with concepts from simply typed lambda calculus.

Constructive logic	Simply typed lambda calculus
Formula	Type
$A \Rightarrow B$	$A \longrightarrow B$
$A \wedge B$	$A \times B$
$A \vee B$	$A + B$
Proof of a formula	Term that inhabits a type

Appendix B: **The simply-typed lambda calculus**

$$
\begin{array}{llll}
t & ::= & & \textbf{terms}: \\
 & | & x & \textit{variable} \\
 & | & \lambda\, x\ :\ \mathtt{T}.\ t & \textit{abstraction} \\
 & | & t\ t & \textit{application} \\
 & & & \\
v & ::= & & \textbf{values}: \\
 & | & \lambda\, x\ :\ \mathtt{T}.\ t & \textit{abstraction} - \textit{value} \\
 & & & \\
\mathtt{T} & ::= & & \textbf{types}: \\
 & | & \mathtt{T} \to \mathtt{T} & \textit{type of functions}
\end{array}
$$

Evaluation rules:

$$\frac{t_1 \longrightarrow t_1'}{t_1\ t_2 \longrightarrow t_1'\ t_2} \qquad \text{(E-App1)}$$

$$\frac{t_2 \longrightarrow t_2'}{v_1\ t_2 \longrightarrow v_1\ t_2'} \qquad \text{(E-App2)}$$

$$(\lambda\, x\colon \mathtt{T}_1.\ t_1)\ v_2 \longrightarrow [x \to v_2]\ t_1 \qquad \text{(E-AppAbs)}$$

Typing rules:

$$\frac{x\ :\ \mathtt{T} \in \Gamma}{\Gamma \vdash x\ :\ \mathtt{T}} \qquad \text{(T-Var)}$$

$$\frac{\Gamma,\ x\ :\ \mathtt{T}_1 \vdash t_2\ :\ \mathtt{T}_2}{\Gamma \vdash (\lambda\, x\colon \mathtt{T}_1.\ t_2)\ :\ \mathtt{T}_1 \to \mathtt{T}_2} \qquad \text{(T-Abs)}$$

$$\frac{\Gamma \vdash t_1\ :\ \mathtt{T}_1 \to \mathtt{T}_2 \quad \Gamma \vdash t_2\ :\ \mathtt{T}_1}{\Gamma \vdash t_1\ t_2\ :\ \mathtt{T}_2} \qquad \text{(T-App)}$$

Appendix C: **Booleans, natural numbers and unit**

$$
\begin{array}{lll|lll}
t & ::= & \textbf{terms}: & v & ::= & \textbf{values}: \\
 & \mid \texttt{true} & \textit{constant true} & & \mid \texttt{true} & \textit{true value} \\
 & \mid \texttt{false} & \textit{constant false} & & \mid \texttt{false} & \textit{false value} \\
 & \mid \texttt{if}\ t\ \texttt{then}\ t\ \texttt{else}\ t & \textit{condition} & & \mid \texttt{unit} & \textit{unit value} \\
 & \mid \texttt{unit} & \textit{constant unit} & & & \\
 & \mid \texttt{0} & \textit{constant zero} & & \mid nv & \textit{numeric value} \\
 & \mid \texttt{succ}\ t & \textit{successor} & nv & ::= & \textbf{numeric values}: \\
 & \mid \texttt{pred}\ t & \textit{predecessor} & & \mid \texttt{0} & \textit{zero value} \\
 & \mid \texttt{iszero}\ t & \textit{zero test} & & \mid \texttt{succ}\ nv & \textit{successor value}
\end{array}
$$

Evaluation rules

(E-PredZero) $\texttt{pred 0} \longrightarrow \texttt{0}$

(E-PredSucc) $\texttt{pred}\ (\texttt{succ}\ nv_1) \longrightarrow nv_1$

(E-Succ) $\dfrac{t_1 \longrightarrow t_1'}{\texttt{succ}\ t_1 \longrightarrow \texttt{succ}\ t_1'}$

(E-Pred) $\dfrac{t_1 \longrightarrow t_1'}{\texttt{pred}\ t_1 \longrightarrow \texttt{succ}\ t_1'}$

(E-IsZeroZero) $\texttt{iszero}\ 0 \longrightarrow \texttt{true}$

(E-IsZeroPred) $\texttt{iszero}\ (\texttt{succ}\ nv_1) \longrightarrow \texttt{false}$

(E-IsZero) $\dfrac{t_1 \longrightarrow t_1'}{\texttt{iszero}\ t_1 \longrightarrow \texttt{iszero}\ t_1'}$

(E-If) $\dfrac{t_1 \longrightarrow t_1'}{\texttt{if}\ t_1\ \texttt{then}\ t_2\ \texttt{else}\ t_3 \longrightarrow \texttt{if}\ t_1'\ \texttt{then}\ t_2\ \texttt{else}\ t_3}$

(E-IfTrue) $\texttt{if true then}\ t_2\ \texttt{else}\ t_3 \longrightarrow t_2$

(E-IfFalse) $\texttt{if false then}\ t_2\ \texttt{else}\ t_3 \longrightarrow t_3$

Typing rules

(T-True) $\texttt{true} : \texttt{Bool}$

(T-False) $\texttt{false} : \texttt{Bool}$

(T-If) $\dfrac{t_1 : \texttt{Bool} \quad t_2 : \texttt{T} \quad t_3 : \texttt{T}}{\texttt{if}\ t_1\ \texttt{then}\ t_2\ \texttt{else}\ t_3 : \texttt{T}}$

(T-Zero) $\texttt{0} : \texttt{Nat}$

(T-Succ) $\dfrac{t_1 : \texttt{Nat}}{\texttt{succ}\ t_1 : \texttt{Nat}}$

(T-Pred) $\dfrac{t_1 : \texttt{Nat}}{\texttt{pred}\ t_1 : \texttt{Nat}}$

(T-IsZero) $\dfrac{t_1 : \texttt{Nat}}{\texttt{iszero}\ t_1 : \texttt{Bool}}$

(T-Unit) $\texttt{unit} : \texttt{Unit}$

Appendix D: **STLC with lists**

$$
\begin{array}{lcll}
t & ::= & & \textbf{Terms} \\
 & | & \ldots & (\textit{STLC terms}) \\
 & | & \texttt{nil} & \text{Empty list} \\
 & | & \texttt{cons t t} & \text{List constructor} \\
 & | & \texttt{head t} & \text{Head of a list} \\
 & | & \texttt{tail t} & \text{Tail of a list} \\
 & | & \texttt{isnil t} & \text{Test for empty list}
\end{array}
$$

$$
\begin{array}{lcll}
v & ::= & & \textbf{Values} \\
 & | & \ldots & (\textit{STLC values}) \\
 & | & \texttt{nil} & \text{Empty list} \\
 & | & \texttt{cons v v} & \text{List constructor}
\end{array}
$$

$$
\begin{array}{lcll}
T & ::= & & \textbf{Types} \\
 & | & \ldots & (\textit{STLC types}) \\
 & | & \texttt{List T} & \text{Type of a list with elements of type } \texttt{T}
\end{array}
$$

Evaluation rules (omitted STLC rules):

$$\frac{t_1 \longrightarrow t_1'}{\texttt{cons}\ t_1\ t_2 \longrightarrow \texttt{cons}\ t_1'\ t_2} \quad \text{(E-Cons1)}$$

$$\frac{t_2 \longrightarrow t_2'}{\texttt{cons}\ v_1\ t_2 \longrightarrow \texttt{cons}\ v_1\ t_2'} \quad \text{(E-Cons2)}$$

$$\texttt{isnil}\ (\texttt{nil}) \longrightarrow \texttt{true} \quad \text{(E-IsNilNil)}$$

$$\texttt{isnil}\ (\texttt{cons}\ v_1\ v_2) \longrightarrow \texttt{false} \quad \text{(E-IsNilCons)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{isnil}\ t_1 \longrightarrow \texttt{isnil}\ t_1'} \quad \text{(E-IsNil)}$$

$$\texttt{head}\ (\texttt{cons}\ v_1\ v_2) \longrightarrow v_1 \quad \text{(E-HeadCons)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{head}\ t_1 \longrightarrow \texttt{head}\ t_1'} \quad \text{(E-Head)}$$

$$\texttt{tail}\ (\texttt{cons}\ v_1\ v_2) \longrightarrow v_2 \quad \text{(E-TailCons)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{tail}\ t_1 \longrightarrow \texttt{tail}\ t_1'} \quad \text{(E-Tail)}$$

Typing rules (omitted STLC rules):

Typing rules for this calculus constitute the problem statement of exercise 2.

Appendix E: **Subtyping extension to STLC**

(S-Refl) $\mathtt{S} <: \mathtt{S}$

(S-Trans) $\dfrac{\mathtt{S} <: \mathtt{U} \quad \mathtt{U} <: \mathtt{T}}{\mathtt{S} <: \mathtt{T}}$

(S-Top) $\mathtt{S} <: \mathtt{Top}$

(S-Arrow) $\dfrac{\mathtt{T}_1 <: \mathtt{S}_1 \quad \mathtt{S}_2 <: \mathtt{T}_2}{\mathtt{S}_1 \to \mathtt{S}_2 <: \mathtt{T}_1 \to \mathtt{T}_2}$

Appendix F: **Product extension to STLC**

$$
\begin{array}{lcll}
t & ::= & \ldots & \textbf{terms}: \\
  & | & \{t, t\} & \textit{pair} \\
  & | & t.\mathtt{1} & \textit{first projection} \\
  & | & t.\mathtt{2} & \textit{second projection} \\
\\
v & ::= & \ldots & \textbf{values}: \\
  & | & \{v, v\} & \textit{pair value} \\
\\
\mathtt{T} & ::= & \ldots & \textbf{types}: \\
  & | & \mathtt{T}_1 \times \mathtt{T}_2 & \textit{product type}
\end{array}
$$

Typing rules:

$$\frac{\Gamma \vdash t_1 : \mathtt{T}_1 \quad \Gamma \vdash t_2 : \mathtt{T}_2}{\Gamma \vdash \{t_1, t_2\} : \mathtt{T}_1 \times \mathtt{T}_2} \qquad \text{(T-Pair)}$$

$$\frac{\Gamma \vdash t : \mathtt{T}_1 \times \mathtt{T}_2}{\Gamma \vdash t.\mathtt{1} : \mathtt{T}_1} \qquad \text{(T-Proj1)}$$

$$\frac{\Gamma \vdash t : \mathtt{T}_1 \times \mathtt{T}_2}{\Gamma \vdash t.\mathtt{2} : \mathtt{T}_2} \qquad \text{(T-Proj2)}$$

New evaluation rules:

$$\{v_1, v_2\}.\mathtt{1} \longrightarrow v_1 \qquad \text{(E-PairBeta1)}$$

$$\{v_1, v_2\}.\mathtt{2} \longrightarrow v_2 \qquad \text{(E-PairBeta2)}$$

$$\frac{t \longrightarrow t'}{t.\mathtt{1} \longrightarrow t'.\mathtt{1}} \qquad \text{(E-Proj1)}$$

$$\frac{t \longrightarrow t'}{t.\mathtt{2} \longrightarrow t'.\mathtt{2}} \qquad \text{(E-Proj2)}$$

$$\frac{t_1 \longrightarrow t_1'}{\{t_1, t_2\} \longrightarrow \{t_1', t_2\}} \qquad \text{(E-Pair1)}$$

$$\frac{t_2 \longrightarrow t_2'}{\{v_1, t_2\} \longrightarrow \{v_1, t_2'\}} \qquad \text{(E-Pair2)}$$