- se $M_1$ è un valore, per il lemma delle forme canoniche sappiamo che $M_1 = \mathsf{fn}\, x{:}T_1.N_1$, quindi $M = \mathsf{fn}\, x{:}T_1.N_1\ M_2$. Per ipotesi induttiva sappiamo anche che $M_2$ è un valore oppure $\exists M_2'$ tale che $M_2 \longrightarrow M_2'$. Dunque, se $M_2$ è un valore $v_2$ allora $M \longrightarrow N_1\{x := v_2\}$ per la regola (BETA) della valutazione, altrimenti $M \longrightarrow \mathsf{fn}\, x{:}T_1.N_1\ M_2'$ per la regola (APP 2).
- Se invece $M_1 \longrightarrow M_1'$, allora per la regola (APP 1) della valutazione si ha che $M \longrightarrow M_1'\ M_2$.

In entrambi i casi quindi abbiamo dimostrato che $M$ fa un passo di riduzione, in accordo quindi con la tesi del teorema.

□

Per provare il teorema di preservazione dei tipi, enunciamo prima un paio di lemmi strutturali che ci permetteranno di manipolare le derivazioni di tipo. Il primo lemma ci dice che possiamo permutare gli elementi di un contesto senza cambiare l'insieme di giudizi di tipo derivabili da quel contesto. Si ricordi che abbiamo assunto che le variabili che appaiono in un contesto sono distinte, e che quando aggiungiamo una variabile ad un contesto, assumiamo che quella variabile non sia già presente. Il secondo lemma permette di indebolire il giudizio in ipotesi aumentando il numero di assunzioni all'interno del contesto.

**Lemma 2.9** (Permutazione)**.** *Se $\Gamma \vdash M : T$ è un giudizio derivabile, e $\Delta$ è una permutazione di $\Gamma$, allora anche il giudizio $\Delta \vdash M : T$ è derivabile, ed ha una derivazione della stessa altezza del precedente.* □

**Lemma 2.10** (Weakening)**.** *Se $\Gamma \vdash M : T$ è un giudizio derivabile e $x \notin Dom(\Gamma)$, allora $\Gamma, x : S \vdash M : T$ è derivabile, e la sua derivazione ha la stessa altezza della precedente.* □

Entrambi i lemmi si dimotrano facilmente per induzione sulla derivazione del giudizio $\Gamma \vdash M : T$. Questi due lemmi ci permettono di di provare una proprietà importante del sistema di tipi: il typing si preserva quando una variabile viene sostituita con un termine del tipo appropriato.

**Lemma 2.11** (Substitution)**.** *Se $\Gamma, x : S \vdash M : T$ e $\Gamma \vdash N : S$, allora $\Gamma \vdash M\{x := N\} : T$.*

*Proof.* Per induzione sull'altezza della derivazione del giudizio $\Gamma, x : S \vdash M : T$. Iniziamo dai casi base:

- Il giudizio in ipotesi è $\Gamma, x : S \vdash \mathsf{true} : \mathsf{Bool}$. In questo $M\{x := N\} = \mathsf{true}\{x := N\} = \mathsf{true}$, quindi la tesi è $\Gamma \vdash \mathsf{true} : \mathsf{Bool}$, che è vera per la regola (T-TRUE). I casi in cui il giudizio in ipotesi è un'istanza dell'assioma (T-FALSE) o (T-NAT) sono analoghi.
- Il giudizio in ipotesi è $\Gamma, x : S \vdash y : T$ con $y \neq x$. Per il Lemma di Inversione $y : T \in \Gamma, x : S$, e poiché $x \neq y$ si ha $y : T \in \Gamma$, da cui, per la regola (T-VAR), si ottiene $\Gamma \vdash y : T$ che è proprio la tesi perché $y\{x := N\} = y$.
- Il giudizio in ipotesi è $\Gamma, x : S \vdash x : T$ perché $M = x$. Si osservi che per il Lemma di Inversione $T = S$. In questo caso dobbiamo dimostrare $\Gamma \vdash x\{x := N\} : S$, cioè $\Gamma \vdash N : S$, che è vero per la seconda ipotesi.

Dimostriamo ora il lemma per i casi induttivi assumendo che sia vero per i giudizi della forma $\Gamma, x' : S' \vdash M' : T'$ con derivazione di altezza minore o uguale a $k$. Assumiamo quindi che l'ipotesi $\Gamma, x : S \vdash M : T$ sia derivabile con caltezza $k+1$ procediamo per casi distinguendo l'ultima regola usata per derivare questo giudizio:

- Caso (T-SUM). In questo il caso $M = M_1 + M_2$ poiché l'ipotesi è $\Gamma, x : S \vdash M_1 + M_2 : \mathsf{Nat}$, che viene da $\Gamma, x : S \vdash M_1 : \mathsf{Nat}$ e $\Gamma, x : S \vdash M_2 : \mathsf{Nat}$, entrambi dunque derivabili con altezza minore o uguale a $k$. Per induzione si ha quindi $\Gamma \vdash M_1\{x := N\} : \mathsf{Nat}$ e $\Gamma \vdash M_2\{x := N\} : \mathsf{Nat}$, e dunque per la regola di tipo (T-SUM) si ha $\Gamma \vdash M_1\{x := N\} + M_2\{x := N\} : \mathsf{Nat}$ e si conclude osservando che $M\{x := N\} = M_1\{x := N\} + M_2\{x := N\}$.
- I casi in cui il giudizio in ipotesi è derivato usando la regola (T-MINUS) o la regola (T-IFTHENELSE) sono analoghi al caso precedente.

- Caso (T-FUN). In questo caso $M = \mathsf{fn}\, y{:}T_1.M_1$ poiché l'ipotesi è $\Gamma, x : S \vdash \mathsf{fn}\, y{:}T_1.M_1 : T_1 \to T_2$, dove, per $\alpha$-equivalenza, possiamo assumere senza perdita di generalità che $y \neq x$ e $y \notin \mathrm{fn}(N)$. In questo caso l'ipotesi viene da $\Gamma, x : S, y : T_1 \vdash M_1 : T_2$, derivabile con altezza $k$, quindi per il Lemma di Permutazione si ha che anche $\Gamma, y : T_1, x : S \vdash M_1 : T_2$ è derivabile con altezza $k$. Dall'ipotesi iniziale $\Gamma \vdash N : S$ per il Lemma di Weakening si ha $\Gamma, y : T_1 \vdash N : S$; da questo giudizio, insieme al precedente $\Gamma, y : T_1, x : S \vdash M_1 : T_2$, per ipotesi induttiva si ha $\Gamma, y : T_1 \vdash M_1\{x := N\} : T_2$. Da questo giudizio per la regola di tipo (T-FUN) si ha anche $\Gamma \vdash \mathsf{fn}\, y{:}T_1.M_1\{x := N\} : T_1 \to T_2$, che è proprio la tesi, perché $(\mathsf{fn}\, y{:}T_1.M_1)\{x := N\} = \mathsf{fn}\, y{:}T_1.(M_1\{x := N\})$.

- Caso (T-APP). in questo caso $M = M_1\ M_2$ poiché l'ipotesi è $\Gamma, x : S \vdash M_1\ M_2 : T$, che viene dalle premesse $\Gamma, x : S \vdash M_1 : T_1 \to T$ e $\Gamma, x : S \vdash M_2 : T_1$, entrambe derivabili con altezza minore o uguale a $k$. Allora per ipotesi induttiva si ha $\Gamma \vdash M_1\{x := N\} : T_1 \to T$ e $\Gamma \vdash M_2\{x := N\} : T_1$, e applicando a questi giudizi la regola (T-APP) si ha $\Gamma \vdash M_1\{x := N\}\ M_2\{x := N\} : T$, che è proporio la tesi perché $M\{x := N\} = M_1\{x := N\}\ M_2\{x := N\}$.

□

**Theorem 2.12** (Preservazione dei tipi-Subject Reduction)**.**
*Se* $\Gamma \vdash M : T$ *e* $M \longrightarrow M'$*, allora* $\Gamma \vdash M' : T$.

*Proof.* Per induzione sull'altezza della derivazione di $M \longrightarrow M'$. Iniziamo dai casi base, quelli cioè in cui $M \longrightarrow M'$ viene da uno degli assiomi delle regole di semantica operazionale:

- caso (SUM). In questo caso $M \longrightarrow M'$ è $n_1 + n_2 \longrightarrow n$. Dall'ipotesi $\Gamma \vdash M : T$, poiché $M = n_1 + n_2$, per il Lemma di Inversione, si ha $T = \mathsf{Nat}$. La tesi da dimostrare è quindi $\Gamma \vdash n : \mathsf{Nat}$, che è derivabile per la regola di tipo (T-NAT). Il caso (MINUS) in cui $M = m_1 - m_2 \longrightarrow m$ è analogo.

- caso (IF-TRUE). In questo caso $M \longrightarrow M'$ è $\mathsf{if\,true\,then}\ M_1\ \mathsf{else}\ M_2 \longrightarrow M_1$. Dall'ipotesi $\Gamma \vdash M : T$, poiché $M = \mathsf{if\,true\,then}\ M_1\ \mathsf{else}\ M_2$, per il Lemma di Inversione, si ha (tra le altre cose) $\Gamma \vdash M_1 : T$, che è proprio la tesi. Il caso (IF-FALSE) in cui $M = \mathsf{if\,false\,then}\ M_1\ \mathsf{else}\ M_2$ è analogo.

- caso (BETA). Caso in cui $M = (\mathsf{fn}\, x{:}T_1.M_1\ v)$ e $M' = M_1\{x := v\}$. Dall'ipotesi $\Gamma \vdash M : T$, poiché $M$ è un termine applicazione, per il Lemma di Inversione, si ha che $\exists T'$ tale che $\Gamma \vdash v : T'$ e $\Gamma \vdash \mathsf{fn}\, x{:}T_1.M_1 : T' \to T$. Dall'ultimo giudizio, per il Lemma di Inversione, si ha che $T' = T_1$ e $\Gamma, x : T_1 \vdash M_1 : T$. Quindi, da quest'ultimo giudizio insieme al precedente $\Gamma \vdash v : T_1$ per il Lemma di Sostituzione si conclude $\Gamma \vdash M_1\{x := v\} : T$, che è proprio la tesi.

Procediamo ora con i casi induttivi, assumendo l'ipotesi induttiva "se $\Gamma \vdash N : T'$, e $N \longrightarrow N'$ con una derivazione di altezza minore o uguale a $k$, allora $\Gamma \vdash N' : T'$". Assumiamo quindi che valga l'ipotesi del teorema, cioè che $\Gamma \vdash M : T$ e che $M \longrightarrow M'$ sia derivabile con una derivazione di altezza $k + 1$. Distinguiamo diversi casi a seconda dell'ultima regola usata in questa derivazione:

- caso (SUM LEFT). In questo caso $M \longrightarrow M'$ è $M_1 + M_2 \longrightarrow M_1' + M_2$ poichè $M_1 \longrightarrow M_1'$, derivato con una derivazione di altezza $k$. Dall'ipotesi $\Gamma \vdash M : T$ con $M = M_1 + M_2$, per il Lemma di inversione, si ha che $T = \mathsf{Nat}$ e sono derivabili i giudizi $\Gamma \vdash M_1 : \mathsf{Nat}$ e $\Gamma \vdash M_2 : \mathsf{Nat}$. Da $\Gamma \vdash M_1 : \mathsf{Nat}$ e $M_1 \longrightarrow M_1'$, derivato con altezza $k$, per ipotesi induttiva si ha $\Gamma \vdash M_1' : \mathsf{Nat}$. Quest'ultimo giudizio insieme al precedente $\Gamma \vdash M_2 : \mathsf{Nat}$ permettono di derivare con la regola di tipo (T-SUM) il giudizio $\Gamma \vdash M_1' + M_2 : T$, che è proprio la tesi.

- caso (SUM RIGHT). il caso in cui $M \longrightarrow M'$ poiché $M = v + M_2$, $M' = v + M_2'$ e $M_2 \longrightarrow M_2'$ è analogo al precedente.

- casi (MINUS LEFT), (MINUS RIGHT), (IF). In questi casi $M = M_1 - M_2$ oppure $M = \mathsf{if}\ M_1\ \mathsf{then}\ M_2\ \mathsf{else}\ M_3$ e sono analoghi al precedente.

- caso (APP 1). Caso in cui $M \longrightarrow M'$ poiché $M = M_1\ M_2$, $M' = M_1'\ M_2$ e $M_1 \longrightarrow M_1'$, derivato con un'altezza $k$. Dall'ipotesi $\Gamma \vdash M : T$, per il Lemma di Inversione, si ha che $\exists T_1$ tale che $\Gamma \vdash M_1 : T_1 \to T$ e $\Gamma \vdash M_2 : T_1$. Quindi, poiché $\Gamma \vdash M_1 : T_1 \to T$ e $M_1 \longrightarrow M_1'$, derivato con altezza $k$, per ipotesi induttiva si ha $\Gamma \vdash M_1' : T_1 \to T$. Da quest'ultimo giudizio e il precedente $\Gamma \vdash M_2 : T_1$, applicando la regola di tipo (T-APP) si ottiene $\Gamma \vdash M_1'\ M_2 : T$, che è proprio la tesi.
- caso (APP 2). Il caso in cui $M \longrightarrow M'$ poiché $M = v\ M_2$, $M' = v\ M_2$ e $M_2 \longrightarrow M_2'$ è analogo al precedente.

□

Osserva che il teorema di preservazione vale per i termini qualsiasi, anche quelli che contengono variabili libere. Per dimosrare il teorema di safety ci serve solo per i termini chiusi.

**Corollary 2.13.** *Se $\varnothing \vdash M : T$ e $M \longrightarrow^* M'$, allora $\varnothing \vdash M' : T$.*

*Proof.* Per induzione sulla lunghezza di $M \longrightarrow^* M'$. Se la lunghezza è 0, allora $M' = M$ e la tesi è immediata. Sia invece $M \longrightarrow^* M'$ in $k+1$ passi, cioè $M \longrightarrow^* M_1$ in $k$ passi e $M_1 \longrightarrow M'$. Da $\Gamma \vdash M : T$, per ipotesi induttiva si ha $\Gamma \vdash M_1 : T$, e per il teorema di Preservazione dei tipi si conclude $\Gamma \vdash M' : T$. □

**Theorem 2.14** (Safety)**.** *Se $M$ è un termine chiuso ben tipato, allora non evolve in un termine stuck, cioè sia $\emptyset \vdash M : T$ e $M \longrightarrow^* M'$ con $M' \not\longrightarrow$, allora $M'$ è un valore.*

*Proof.* Da $\emptyset \vdash M : T$ per il corollario precedente si ottiene $\emptyset \vdash M' : T$, e per il teorema di progressione si hanno due casi: $M'$ è un valore, oppure $\exists M''$ tale che $M' \longrightarrow M''$. Poiché per ipotesi si ha $M' \not\longrightarrow$, allora si può concludere che $M'$ è un valore. □

EXERCISE 2.15. Dimostrare subject reduction per induzione sulla derivazione di $\Gamma \vdash M : T$. □

EXERCISE 2.16. Vale l'opposto di subject reduction, i.e. se $\Gamma \vdash M' : T$ e $M \longrightarrow M'$, allora $\Gamma \vdash M : T$ (detto subject expansion)? Dimostrarlo oppure dare un controesempio. □

EXERCISE 2.17. Se al posto della regola (APP) si definisse la regola seguente

$$\frac{\Gamma \vdash M : T \to T \quad \Gamma \vdash N : T}{\Gamma \vdash M\ N : T}\ (\text{APP'})$$

sarebbe ancora vero il teorema di safety? □

EXERCISE 2.18. Se al posto delle regole (APP) e (FUN) si definissero le regole seguenti

$$\frac{\Gamma \vdash M : T \to T \quad \Gamma \vdash N : T}{\Gamma \vdash M\ N : T}\ (\text{APP'}) \qquad \frac{\Gamma, x : T_1 \vdash M : T}{\Gamma \vdash \mathsf{fn}\, x{:}T_1.M : T \to T}\ (\text{FUN'})$$

sarebbe ancora vero il teorema di safety? □

EXERCISE 2.19. Se si aggiungessero al sistema di tipi i seguenti due assiomi

$$\frac{}{\Gamma \vdash \mathsf{true} : \mathsf{Nat}}\ (\text{TRUE'}) \qquad \frac{}{\Gamma \vdash \mathsf{false} : \mathsf{Nat}}\ (\text{FALSE'})$$

sarebbe ancora vero il teorema di safety? □

EXERCISE 2.20. Dimostrare il seguente fatto: se $\Gamma \vdash M : T$ è derivabile allora $\mathrm{fv}(M) \subseteq Dom(\Gamma)$. □

EXERCISE 2.21. Ricostruire il tipo dei seguenti termini:

- fn $x$:$T_1$.fn $y$:$T_2$.if $y$ then $x$ else true
- fn $x$:Nat $\to$ Bool.$x$
- fn $f$:$T$.fn $x$:$T'$.$f$ (if true then $x$ else $f\ x$)
- fn $f$:$T_1$.fn $g$:$T_2$.if $(f\ (g\ \text{true}))$ then $f$ (fn $x$:$T_3$.true) else $f$(fn $x$:$T_4$.$x$)

□