l'insieme delle variabili che appaiono in Γ. I giudizi di tipo saranno della forma $\Gamma \vdash M : T$ che indica che "in un contesto Γ il termine M ha tipo T". I giudizi di tipo sono derivabili con il seguente sistema di regole.

$$\text{(T-TRUE)}\ \frac{}{\Gamma \vdash \mathsf{true} : \mathsf{Bool}} \qquad \text{(T-FALSE)}\ \frac{}{\Gamma \vdash \mathsf{false} : \mathsf{Bool}} \qquad \text{(T-NAT)}\ \frac{}{\Gamma \vdash n : \mathsf{Nat}}$$

$$\text{(T-SUM)}\ \frac{\Gamma \vdash M : \mathsf{Nat} \quad \Gamma \vdash N : \mathsf{Nat}}{\Gamma \vdash M + N : \mathsf{Nat}} \qquad \text{(T-MINUS)}\ \frac{\Gamma \vdash M : \mathsf{Nat} \quad \Gamma \vdash N : \mathsf{Nat}}{\Gamma \vdash M - N : \mathsf{Nat}}$$

$$\text{(T-IFTHENELSE)}\ \frac{\Gamma \vdash M_1 : \mathsf{Bool} \quad \Gamma \vdash M_2 : T \quad \Gamma \vdash M_3 : T}{\Gamma \vdash \mathsf{if}\ M_1\ \mathsf{then}\ M_2\ \mathsf{else}\ M_3 : T} \qquad \text{(T-VAR)}\ \frac{x : T \in \Gamma}{\Gamma \vdash x : T}$$

$$\text{(T-FUN)}\ \frac{\Gamma, x : T_1 \vdash M : T_2}{\Gamma \vdash \mathsf{fn}\, x{:}T_1.M : T_1 \to T_2} \qquad \text{(T-APP)}\ \frac{\Gamma \vdash M : T_1 \to T_2 \quad \Gamma \vdash N : T_1}{\Gamma \vdash M\ N : T_2}$$

La regola (T-FUN) ha come premessa un giudizio che dice che il termine M ha tipo T_2 assumendo che la variabile che compare in M abbia tipo T_1. Questa assunzione viene aggiunta al contesto, assumendo che questa aggiunta produca un nuovo contesto ben formato. Ciò succede quando la variabile x non compare già nel dominio di Γ. Grazie all'α-conversione, possiamo sempre rinominare la variabile legata del termine M in modo tale che sia distinta dalle altre variabili che compaiono in Γ.

Esempi: dare la derivazione dei seguenti giudizi di tipo:

- $\varnothing \vdash \mathsf{if\,true\,then}\ 5 + 7\ \mathsf{else}\ 2 : \mathsf{Nat}$,
- $\varnothing \vdash \mathsf{fn}\, x{:}T.x : T \to T$,
- $\varnothing \vdash (\mathsf{fn}\, x{:}\mathsf{Bool}.x)\ \mathsf{true}\ :\ \mathsf{Bool}$,
- $f : \mathsf{Bool} \to \mathsf{Bool} \vdash f\ (\mathsf{if\,false\,then\,true\,else\,false})\ :\ \mathsf{Bool}$
- $f : \mathsf{Bool} \to \mathsf{Bool} \vdash \mathsf{fn}\, x{:}\mathsf{Bool}.f\ (\mathsf{if}\ x\ \mathsf{then\,false\,else}\ x)\ :\ \mathsf{Bool} \to \mathsf{Bool}$.

Nota che abbiamo usato le regole per fare *type checking*. I giudizi di tipo sono delle asserzioni sul tipo dei programmi, le regole di tipo sono implicazioni tra giudizi di tipo, le derivazioni sono deduzioni basate sulle regole di tipo.

Definition 2.1. Diciamo che un termine *chiuso* M è *ben tipato* se esiste un tipo T tale che il giudizio $\varnothing \vdash M : T$ sia derivabile. □

Come altre tecniche di analisi statica, anche i sistemi di tipo in genere sono imprecisi, o meglio incompleti, esistono cioè dei termini ragionevolmente corretti, a cui però non si riesce a dare un tipo. Ad esempio, al termine $\mathsf{if\,true\,then}\ 0\ \mathsf{else\,false}$ non si riesce a dare un tipo (staticamente) anche se sicuramente questo termine si valuterà ad un numero. I tipi quindi fanno delle approssimazioni corrette. Si osservi che ad esmpio anche in C/C++ tutti i rami if/else del corpo di una funzione devono restituire valori dello stesso tipo. Ciò è importante perché se una funzione restituisse valori di tipo diverso, l'uso che il chiamante potrebbe fare di questa funzione sarebbe più limiato, o più complesso. Più che una limitazione, questa regola agevola quindi la scrittura di programmi più "maneggevoli" e più semplici da analizzare.

EXERCISE 2.2. Trovare un contesto Γ tale che $\Gamma \vdash f\ x\ y\ : \mathsf{Bool}$ sia derivabile. □

EXERCISE 2.3. Il giudizio $\Gamma \vdash x\ x\ : T$ è derivabile? Se sì trovare una derivazione per qualche Γ, T, altrimenti provare che non è derivabile. □

2.1 Proprietà del sistema di tipi

Abbiamo definito la relazione di typing come la più piccola relazione che soddisfa le regole indicate sopra, abbiamo detto che un termine chiuso M è ben tipato se esiste un tipo T tale per cui esiste una derivazione del giudizio $\varnothing \vdash M : T$.

Spesso quando si ragiona sulla relazione di typing si enunciano cose tipo "se un termina della forma $M + N$ è ben tipato, allora il suo tipo sarà Nat"...Questo genere di enunciati è formalizzato dai seguenti *lemmi di inversione* (o generation lemma), che raccolgono un insieme di osservazioni su come sono costruite le derivazioni di tipo. Per ogni formato di termine questi lemmi dicono "se un termine di questa forma è ben tipato, allora i suoi sottotermini devono avere queste forme..". In altre parole, dato un giudizio di tipo, il lemma di inversione ci dice in che modo questo giudizio è stato derivato.

Lemma 2.4 (Lemma di Inversione)**.**

1. *Se* $\Gamma \vdash \mathsf{true} : T$ *è derivabile, allora* $T = \mathsf{Bool}$.
2. *Se* $\Gamma \vdash \mathsf{false} : T$ *è derivabile, allora* $T = \mathsf{Bool}$.
3. *Se* $\Gamma \vdash n : T$ *è derivabile, allora* $T = \mathsf{Nat}$.
4. *Se* $\Gamma \vdash M + N : T$ *è derivabile, allora* $T = \mathsf{Nat}$ *e* $\Gamma \vdash M : \mathsf{Nat}$ *e* $\Gamma \vdash N : \mathsf{Nat}$.
5. *Se* $\Gamma \vdash M - N : T$ *è derivabile, allora* $T = \mathsf{Nat}$ *e* $\Gamma \vdash M : \mathsf{Nat}$ *e* $\Gamma \vdash N : \mathsf{Nat}$.
6. *Se* $\Gamma \vdash \mathsf{if}\ M_1\ \mathsf{then}\ M_2\ \mathsf{else}\ M_3 : T$ *è derivabile, allora* $\Gamma \vdash M_1 : \mathsf{Bool}$ *e* $\Gamma \vdash M_2, M_3 : T$.
7. *Se* $\Gamma \vdash x : T$ *è derivabile, allora* $x : T \in \Gamma$.
8. *Se* $\Gamma \vdash \mathsf{fn}\, x{:}T_1.M : T$ *è derivabile, allora* $T = T_1 \to T_2$ *per qualche* T_2 *tale che* $\Gamma, x : T_1 \vdash M : T_2$.
9. *Se* $\Gamma \vdash M\ N : T$ *è derivabile, allora* $\exists T_1$ *tale che* $\Gamma \vdash M : T_1 \to T$ *e* $\Gamma \vdash N : T_1$.

Proof. Immmediata dalla definizione delle regole di tipo, poiché in questo sistema di regole per ogni termine c'è al più una sola regola di tipo applicabile. □

Si noti che il lemma di inversione indica un algoritmo ricorsivo per calcolare il tipo dei termini: ci dice infatti, dato un qualsiasi termine, come calcolare il suo tipo (se un tale tipo esiste) partendo dai tipi dei suoi sottotermini.

EXERCISE 2.5. Provare che ogni sottotermine di un termine ben tipato è ben tipato. □

Theorem 2.6 (Unicità dei tipi)**.** *Dato un contesto* Γ*, se un termine è tipabile in* Γ*, allora il suo tipo è unico, e la derivazione di questo tipo è unica.* □

Ricordiamo che vogliamo dimostrare la proprietà di safety: un termine ben tipato non evolve in un termine stuck. Abbiamo assegnato ad un termine M il tipo T se M evolve ad un valore di tipo T. Dobbiamo però dimostrare che le regole di typing sono corrette. Innanzitutto diamo il seguente lemma, che dice come sono fatti i valori dei diversi tipi.

Lemma 2.7 (Forme canoniche)**.**

- *Se* v *è un valore di tipo* Bool *allora* v *è* true *oppure* false*.*
- *Se* v *è un valore di tipo* Nat *allora* v *è una costante intera* n*.*
- *Se* v *è un valore di tipo* $T_1 \to T_2$ *allora* v *è della forma* $\mathsf{fn}\, x{:}T_1.M$*.*

Proof. immediata. □

Il seguente torema di progressione è definito per i termini chiusi, che rappresentano i veri programmi. Per i termini con variabili libere il teorema di progressione non vale: e.g., il termine $f\ \mathsf{true}$ non si valuta a nulla, ma non è un valore.

Theorem 2.8 (Progressione)**.** *Sia M un termine chiuso e ben tipato, i.e. $\varnothing \vdash M : T$, allora o M è un valore, oppure esiste un termine M' tale che $M \longrightarrow M'$.*

Proof. Per induzione sull'altezza della derivazione del giudizio $\varnothing \vdash M : T$. Iniziamo dai casi base, che corrispondono al caso in cui il giudizio $\varnothing \vdash M : T$ è stato derivato con una prova di altezza 1 cioè con uno degli assiomi delle regole di typing. Distinguiamo i vari casi:

- Il giudizio è $\varnothing \vdash \mathsf{true} : \mathsf{Bool}$, ed in questo caso il termine true è un valore;
- Il giudizio è $\varnothing \vdash \mathsf{false} : \mathsf{Bool}$ oppure $\varnothing \vdash n : \mathsf{Nat}$, e anche in questi casi il termine è un valore.
- Nota che il caso in cui il giudizio in ipotesi è $\Gamma \vdash x : T$ non si applica, perché il teorema parla solo di termini chiusi.

Dimostriamo ora il teorema per i casi induttivi, assumiamo cioè che sia vero per i giudizi con derivazione di altezza k e proviamolo per i giudizi con derivazione di altezza $k+1$. In altri termini, l'ipotesi induttiva dice che "se $\varnothing \vdash N : T'$ è un giudizio derivabile con una prova di altezza minore o uguale a k allora N è un valore oppure $\exists N'.N \longrightarrow N'$". Assumiamo ora che valga l'ipotesi $\varnothing \vdash M : T$, derivata con un giudizio di altezza $k+1$, e procediamo per casi a seconda dell'ultima regola usata nella derivazione di altezza $k+1$:

- caso (T-SUM). In questo caso $M = M_1 + M_2$ e il giudizio in ipotesi è $\varnothing \vdash M_1 + M_2 : \mathsf{Nat}$, che è stato derivato da $\varnothing \vdash M_1 : \mathsf{Nat}$ e $\varnothing \vdash M_2 : \mathsf{Nat}$, ed entrambi questi giudizi hanno una derivazione di altezza k. Per ipotesi induttiva quindi sappiamo che M_1 è un valore oppure $\exists M_1'$ tale che $M_1 \longrightarrow M_1'$ e analogamente M_2 è un valore oppure $\exists M_2'$ tale che $M_2 \longrightarrow M_2'$. Se M_1, risp. M_2, è un valore, per il lemma delle forme canoniche si tratta di una costante intera m_1, risp. m_2. Abbiamo quindi i seguenti casi:
  - $M_1 = m_1$ e $M_2 = m_2$, ma allora $M \longrightarrow m$ (per la regola (SUM) della valutazione) dove m è la somma degli interi m_1 e m_2.
  - $M_1 = m_1$ e $M_2 \longrightarrow M_2'$, ma allora $M = m_1 + M_2 \longrightarrow m_1 + M_2'$ per la regola (SUM RIGHT) della valutazione.
  - $M_1 \longrightarrow M_1'$, ma allora $M = M_1 + M_2 \longrightarrow M_1' + M_2$ per la regola (SUM LEFT) della valutazione. Nota che in questo caso non occorre distinguere se M_2 è un valore oppure no.

  In tutti e tre i casi quindi abbiamo dimostrato che M fa un passo di riduzione, il che dimostra la tesi del teorema.
- caso (T-MINUS) del tutto analogo al precedente.
- caso (T-IFTHENELSE). In questo caso $M = \mathsf{if}\ M_1\ \mathsf{then}\ M_2\ \mathsf{else}\ M_3$ e il giudizio in ipoetsi è $\varnothing \vdash \mathsf{if}\ M_1\ \mathsf{then}\ M_2\ \mathsf{else}\ M_3 : T$, che è stato derivato da $\varnothing \vdash M_1 : \mathsf{Bool}$, $\varnothing \vdash M_2 : T$ e $\varnothing \vdash M_3 : T$, che hanno una derivazione di altezza minore o uguale a k. Per ipotesi induttiva quindi sappiamo che M_1 è un valore oppure $\exists M_1'$ tale che $M_1 \longrightarrow M_1'$. Se M_1 è un valore, per il lemma delle forme canoniche sappiamo che M_1 è true oppure false. Nel primo caso allora $M \longrightarrow M_2$ per la regola (IF-TRUE) della valutazione, nel secondo caso $M \longrightarrow M_3$ per la regola (IF-FALSE). Se invece $M_1 \longrightarrow M_1'$, allora $M \longrightarrow \mathsf{if}\ M_1'\ \mathsf{then}\ M_2\ \mathsf{else}\ M_3$ per la regola (IF) della valutazione. In tutti e tre i casi quindi abbiamo dimostrato che M fa un passo di riduzione, il che dimostra la tesi del teorema.
- caso (T-FUN). In questo caso $M = \mathsf{fn}\, x{:}T_1.M_1$ e il giudizio in ipotesi è $\varnothing \vdash \mathsf{fn}\, x{:}T_1.M_1 : T_1 \to T_2$. In questo caso già abbiamo che M è un valore, in accordo quindi con la tesi del teorema.
- caso (T-APP). In questo caso $M = M_1\ M_2$ e il giudizio in ipotesi è $\varnothing \vdash M_1\ M_2 : T_2$, che è stato derivato da $\varnothing \vdash M_1 : T_1 \to T_2$ e $\varnothing \vdash M_2 : T_1$, che hanno una derivazione di altezza minore o uguale a k. Per ipotesi induttiva quindi sappiamo che M_1, è un valore oppure $\exists M_1'$ tale che $M_1 \longrightarrow M_1'$, quindi:

- 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.

□