

Linguaggi e paradigmi di programmazione

Luca Barra

Anno accademico 2023/2024

INDICE

CAPITOLO 1	INTRODUZIONE	PAGINA 1
1.1	Tipi di paradigmi di programmazione	1
1.2	I linguaggi funzionali	1
	Il λ -calcolo — 1 • LISP, FP e ML — 1 • I linguaggi Lazy e Haskell — 2	
CAPITOLO 2	IL λ-CALCOLO	PAGINA 3
2.1	Perchè studiarlo?	3
	Le funzioni — 3	
2.2	Sintassi	3
	Convenzioni sintattiche — 4	
2.3	Semantica	4
	α -conversione — 5 • β -riduzione — 5 • η -riduzione — 6	
2.4	Confluenze e strategie di riduzione	6
	Ordine applicativo — 7 • Ordine normale — 7 • Normalizzazione — 7	
CAPITOLO 3	PROGRAMMARE NEL λ-CALCOLO	PAGINA 8
3.1	Semantica	8
3.2	Operazioni sui numeri naturali	9
3.3	Sintassi delle λ -espressioni con booleani	10
	Regole di tipo — 11	
CAPITOLO 4	ALGORITMO DI INFERENZA	PAGINA 13
4.1	Sommario	13
	Costruzione dell'albero sintattico — 13 • Annotazione dell'albero e generazione dei vincoli — 14 • Sistemi di equazioni e soluzioni — 16	
4.2	Estensioni dell'algoritmo	18
CAPITOLO 5	DIMOSTRAZIONE DI PROPRIETÀ DI FUNZIONI SU NUMERI INTERI	PAGINA 20
5.1	Dimostrazioni	20
	Dimostrazione per casi — 21 • Induzione — 21	
5.2	Dimostrazioni sulle liste	23
5.3	Dimostrazioni sugli alberi	24

Capitolo 1

Introduzione

1.1 Tipi di paradigmi di programmazione

Paradigma	Un programma è	Esempi
Imperativo	Sequenza di azioni (esecuzione \Rightarrow nuovo stato)	C, C++, Pascal, Java, Scala, Python, Scheme
Object-oriented	Oggetti che comunicano (interazione \Rightarrow nuovo stato)	Smalltalk, C++, OCaml, Java, Scala, Python
Funzionale	Espressione (valutazione \Rightarrow risultato)	Haskell, OCaml, Scala, Erlang, Scheme

Per il paradigma *imperativo* un programma è una sequenza di azioni che modificano lo stato attuale del calcolatore. Per il paradigma *object-oriented* un programma è un insieme di oggetti che comunicano tra loro tramite uno scambio di messaggi. Per il paradigma *funzionale* un programma è una grande espressione in cui compaiono funzioni. Un programma funzionale si *valuta*, non si esegue. Quasi tutti i linguaggi attuali sono *multi-paradigma*, ossia hanno caratteristiche di due o più paradigmi.

1.2 I linguaggi funzionali

1.2.1 Il λ -calcolo

La programmazione *funzionale* risale agli anni '30, prima della costruzione dei primi calcolatori elettronici. Il λ -calcolo¹ è un piccolo linguaggio che parte dall'idea di calcolare con le funzioni come si calcola con i numeri. Le uniche cose che si possono scrivere sono espressioni di funzioni (tutto è funzione). Si possono definire funzioni senza dare loro un nome, per esempio, la funzione identità (accetta un argomento x e produce x come risultato):

$$\lambda x.x$$

Note:-

Tutte le funzioni sono a un solo argomento (*currying*), ma si possono avere funzioni di ordine superiori usando delle funzioni come argomento. Il λ -calcolo è un modello di calcolo computazionalmente completo, ossia è abbastanza potente da esprimere tutti i programmi concepibili.

1.2.2 LISP, FP e ML

Negli anni '50 viene sviluppato il primo linguaggio di programmazione funzionale (in parte imperativo), *LISP*², in cui le liste hanno un ruolo chiave. Inizialmente era concepito per l'elaborazione non numerica in cui era possibile definire funzioni anonime con notazione prefissa (abbondante uso di parentesi). Il LISP fu il primo *garbage collector*³.

¹Il " λ " nasce da un errore tipografico, doveva essere un accento circonflesso sull'argomento

²Dalla contrazione di LISP Processor

³La gestione della memoria non ricade sul programmatore

Negli anni '70 John Backus, ideatore del FORTRAN, vince il premio Turing. Nella sua lezione d'onore⁴ Backus critica il FORTRAN e il paradigma imperativo introducendo successivamente *FP*. In FP vengono incorporate le idee della programmazione funzionale (tuttavia non avrà mai successo).

*ML*⁵ fu il primo linguaggio funzionale moderno. Esso fu concepito da Robin Milner come "spin-off" di LCF⁶, ma diventò un linguaggio a sè stante (OCamel si fonda su ML). Si fonda su *type inference* (il programmatore poteva non specificare i tipi) e fu il primo con *polimorfismo parametrico*. Inoltre è possibile definire tipi e viene introdotto il *pattern matching* (per analizzare le strutture dati). Infine era dotato di un sistema di moduli per scomporre programmi di grandi dimensioni.

1.2.3 I linguaggi Lazy e Haskell

Negli anni '80 si svilupparono i linguaggi funzionali *lazy*, in cui gli argomenti non vengono valutati se la funzione non ne ha davvero bisogno. SASL introduce le guardie e il currying. KRC introduce un precursore delle liste comprehension. Miranda introduce le sezioni (ossia funzioni in cui si applica un'operazione n-aria a un solo operando).

Negli anni '90 si organizzò un comitato per standardizzare i linguaggi lazy. *Haskell* è un linguaggio di programmazione funzionale puro in cui si usano i tipi per separare I/O, stati, etc.. Si hanno classi di tipo per implementare l'overloading. Nel 2005 si stavano raggiungendo i limiti della velocità dei processori, per cui si sviluppano architetture multi-core. Il *calcolo parallelo* è difficile a causa dei linguaggi imperativi, ma Haskell, essendo puro, può facilmente essere usato.

⁴Lezione data da un vincitore del premio Turing in cui si racconta il perchè si è vinto il premio

⁵Meta language

⁶Logic for Computable Function

Capitolo 2

Il λ -calcolo

2.1 Perché studiarlo?

Il λ -calcolo definisce in modo preciso il processo di valutazione (riduzione) di un programma funzionale. Esso pone le basi per lo sviluppo di un sistema di tipi e il relativo algoritmo di inferenza.

2.1.1 Le funzioni

- **Punto di vista estensionale:** $f = \{(0, 1), (1, 2), (2, 5), (3, 10), \dots\}$, rappresenta un'elegante interpretazione insiemistica, ma non fornisce informazioni su come calcolare le funzioni e sul relativo costo;
- **Punto di vista intensionale:** $f(x) = x^2 + 1$, fornisce una "ricetta" per il calcolo, ma non tutte le funzioni hanno una ricetta finita. Su questo punto di vista si basa il λ -calcolo.

Note:-

Nel λ -calcolo i numeri non sono primitive, in Haskell sì

2.2 Sintassi

Definizione 2.2.1: Variabili e sintassi

Sia $\text{Var} = \{x, y, z, \dots\}$ un insieme finito di variabili, la sintassi è la seguente:

$$M, N ::= x \mid (\lambda x.M) \mid (MN)$$

Note:-

$\lambda x.M$ è un'astrazione o funzione con argomento x e corpo M

Note:-

(MN) è l'applicazione della funzione M all'argomento N

Esempio 2.2.1

- $(\lambda x.x)$;
- $((\lambda x.(xx))(\lambda y.(yy)))$;
- $(\lambda f.(\lambda x.(f(fx))))$.

2.2.1 Convenzioni sintattiche

Si può limitare l'uso delle parentesi:

- le parentesi più esterne sono omesse $MN = (MN)$;
- il corpo delle associazioni si estende il più possibile a destra $\lambda x.xx = (\lambda x(xx))$;
- l'applicazione è associativa a sinistra $M_1M_2M_3 = ((M_1M_2)M_3)$.

2.3 Semantica

Note:-

Diciamo che un'occorrenza di x in M è legata se compare in sotto-termine della forma $\lambda x.N$ in M , altrimenti è libera

Esempio 2.3.1

- $\lambda x.x$ non ha nessuna variabile libera;
- $x \ y \ z$ ha solo variabili libere;
- $(\lambda x.xy)x$ in cui x occorre sia libera che legata.

Definizione 2.3.1: Insieme delle variabili libere

L'insieme delle variabili libere di un termine M , denotato come $fv(M)$, è definito induttivamente sulla struttura di M come segue:

$$fv(x) = \{x\} \quad fv(\lambda x.M) = fv(M) \setminus \{x\} \quad fv(MN) = fv(M) \cup fv(N)$$

Definizione 2.3.2: Sostituzione

- $x\{N/y\} = \begin{cases} N & \text{se } x = y \\ x & \text{se } x \neq y \end{cases}$
- $(M_1M_2)\{N/y\} = M_1\{N/y\}M_2\{N/y\}$;
- $(\lambda x.M)\{N/y\} = \begin{cases} \lambda x.M & \text{se } x = y \\ \lambda x.M\{N/y\} & \text{se } x \neq y \text{ e } x \notin fv(N) \\ \lambda z.M\{z/x\}\{N/y\} & \text{se } x \neq y \text{ e } x \in fv(N) \text{ e } z \in Var - (fv(M) \cup fv(N)) \end{cases}$

Note:-

$M\{N/y\}$ è ottenuta sostituendo le occorrenze libere di y in M con N . Serve per evitare la cattura delle variabili libere di N per non alterarne il senso

Esempio 2.3.2

- $\lambda x.x\{y/x\} = \lambda x.x$ non avviene nessuna sostituzione, perchè non ci sono variabili libere;
- $((\lambda x.x)x)\{y/x\} = (\lambda x.x)y$ sono state sostituite le occorrenze libere;
- $(\lambda z.x)\{y/x\} = \lambda z.y$ $y \neq z$ quindi non viene catturata;
- $(\lambda y.xy)\{y/x\} = \lambda z.yz$ y verrebbe catturata, quindi viene cambiata con z ;
- $(\lambda x.y)\{\lambda x.x/y\} = \lambda x.\lambda x.x$ non c'è cattura;

- $(\lambda x.y)\{\lambda z.x/y\} = \lambda u.\lambda z.x$ perchè x verrebbe catturata.

Note:-

Il significato di una funzione è indipendente dal nome dell'argomento

2.3.1 α -conversione

Definizione 2.3.3: α -conversione

L' α -conversione \Leftrightarrow_α è la congruenza tra λ -espressioni tale che, se $y \notin fv(M)$, allora $\lambda x.M \Leftrightarrow_\alpha \lambda y.M\{y/x\}$

Note:-

$y \notin fv(M)$ serve a evitare che una variabile libera in M venga catturata dalla conversione

2.3.2 β -riduzione

Note:-

Applicare una funzione $\lambda x.M$ a un argomento N significa valutare il corpo della funzione (M) in cui ogni occorrenza libera dell'argomento (x) è stata sostituita da N

Definizione 2.3.4: β -riduzione

La β -riduzione è la relazione tra λ -espressioni tale che:

- $(\lambda x.M)N \rightarrow_\beta M\{N/y\}$;
- se $M \rightarrow_\beta M'$ allora $MN \rightarrow_\beta M'N$;
- se $M \rightarrow_\beta M'$ allora $MN \rightarrow_\beta NM'$;
- se $M \rightarrow_\beta M'$ allora $MN \rightarrow_\beta \lambda x.M'$.

Note:-

Nella β -riduzione:

$$(\lambda x.M)N \rightarrow_\beta M\{N/y\}$$

$(\lambda x.M)N$ è un β -redex^a.

$M\{N/y\}$ è il suo *ridotto*.

Ci possono essere più modi di ridurre la stessa λ -espressione. La riduzione di un β -redex può creare altri β -redex. La riduzione di un β -redex può cancellare altri β -redex. La riduzione può non terminare.

^aREDucible EXpression

Note:-

Ci sono esempi di espressioni che rappresentano la stessa espressione, ma che non possono essere ridotti. Per esempio:

$$(\lambda x.Mx)N \rightarrow_\beta (Mx)\{N/x\} = M\{N/x\}N = MN$$

M e $\lambda x.Mx$ producono lo stesso risultato se applicate allo stesso argomento, tuttavia nessuna delle due è β -riducibile nell'altra.

2.3.3 η -riduzione

Definizione 2.3.5: η -riduzione

La η -riduzione è la relazione tra λ -espressioni tale che:

- se $x \notin \text{fv}(M)$ allora $\lambda x.Mx \rightarrow_\eta M$;
- se $M \rightarrow_\eta M'$ allora $MN \rightarrow_\eta M'N$;
- se $M \rightarrow_\eta M'$ allora $MN \rightarrow_\eta NM'$;
- se $M \rightarrow_\eta M'$ allora $MN \rightarrow_\eta \lambda x.M'$.

Definizione 2.3.6: Riduzioni singole e multiple

Si scrive \rightarrow per indicare l'unione $\rightarrow_\beta \cup \rightarrow_\eta$ e \Rightarrow per indicare la chiusura riflessiva e transitiva di \rightarrow . Ovvero \Rightarrow è la più piccola relazione tale che:

- $M \Rightarrow M$;
- se $M \rightarrow N$ allora $M \Rightarrow N$;
- se $M \Rightarrow M'$ e $M' \Rightarrow N$ allora $M \Rightarrow N$.

Definizione 2.3.7: Convertibilità

Scriviamo $M \leftrightarrow N$ se $M \rightarrow N$ oppure $N \rightarrow M$ e scriviamo \Leftrightarrow per la chiusura riflessiva e transitiva di \leftrightarrow . Diciamo che M e N sono convertibili se $M \Leftrightarrow N$.

2.4 Confluenze e strategie di riduzione

Teorema 2.4.1 Confluenza

Se $M \Rightarrow N_1$ e $M \Rightarrow N_2$ allora esiste N tale che $N_1 \Rightarrow N$ e $N_2 \Rightarrow N$

Note:-

Ossia, indipendentemente dalla strada presa, si giunge allo stesso risultato

Definizione 2.4.1: Forma normale

Diciamo che M è in forma normale se non può più essere ridotto, ovvero se non esiste N tale che $M \rightarrow N$. In tal caso scriviamo $M \rightarrow$

Corollario 2.4.1

La forma normale di M , se esiste, è unica (a meno di α -conversioni)

Esempio 2.4.1 (Dimostrazione della forma normale)

Supponiamo che M abbia due forme normali N_1 e N_2 , ovvero $M \Rightarrow N_1 \rightarrow$ e $M \Rightarrow N_2 \rightarrow$. Per il teorema di confluenza esiste N tale che $N_1 \Rightarrow N$ e $N_2 \Rightarrow N$. Siccome N_1 e N_2 sono in forma normale, deve essere $N_1 = N = N_2$ (a meno di α -conversioni)

2.4.1 Ordine applicativo

Definizione 2.4.2: Ordine applicativo

Nell'ordine applicativo si sceglie il redesso più interno e più a sinistra

Note:-

Viene utilizzato dai linguaggi zelanti o eager

2.4.2 Ordine normale

Definizione 2.4.3: Ordine normale

Nell'ordine normale si sceglie il redesso più esterno e più a destra

Note:-

Viene utilizzato dai linguaggi pigri o lazy

2.4.3 Normalizzazione

Teorema 2.4.2 Normalizzazione

Se $M \Leftrightarrow N$ e N è in forma normale, allora c'è una riduzione in ordine normale $M \Rightarrow N$

Note:-

Questa proprietà non vale per l'ordine applicativo

Capitolo 3

Programmare nel λ -calcolo

3.1 Semantica

Definizione 3.1.1: Valori booleani

- $\text{TRUE} = \lambda x.\lambda y.x$;
- $\text{FALSE} = \lambda x.\lambda y.y$;
- $\text{IF} = \lambda z.z$

Proposizione 3.1.1

- $\text{IF TRUE } MN \Leftrightarrow M$;
- $\text{IF FALSE } MN \Leftrightarrow N$.

Definizione 3.1.2: Operatori logici

- $\text{AND} = \lambda x.\lambda y.\text{IF } xy \text{ FALSE}$;
- $\text{OR} = \lambda x.\lambda y.\text{IF } x \text{ TRUE } y$;
- $\text{NOT} = \lambda x.\text{IF } x \text{ FALSE TRUE}$.

Definizione 3.1.3: Coppie

- $\text{PAIR} = \lambda x.\lambda y.\lambda z.zxy$;
- $\text{FST} = \lambda p.p \text{ TRUE}$;
- $\text{SND} = \lambda p.p \text{ FALSE}$.

Proposizione 3.1.2

- $\text{FST (PAIR } MN) \Leftrightarrow M$;
- $\text{SND (PAIR } MN) \Leftrightarrow N$.

Definizione 3.1.4: Numeri naturali (codifica di Church)

Dato $k \in \mathbb{N}$ scriviamo $M^k N$ per $M(M(\dots(MN)))$ (k volte). In particolare:
 $M^0 N = N$.

- $\underline{n} = \lambda f. \lambda x. f^n x$ (codifica del numero naturale n);
- $\text{SUCC} = \lambda a. \lambda f. \lambda x. a f (f x)$ (funzione successore).

Note:-

Un numero naturale è un iteratore che itera una certa funzione n volte su un certo elemento

3.2 Operazioni sui numeri naturali

Definizione 3.2.1: ADD, MUL e EXP

- $\text{ADD} = \lambda a. \lambda b. b \text{SUCC} a$;
- $\text{MUL} = \lambda a. \lambda b. b (\text{ADDA} a) \underline{0}$;
- $\text{EXP} = \lambda a. \lambda b. b (\text{MULA} a) \underline{1}$.

Proposizione 3.2.1

- $\text{ADD } \underline{m} \underline{n} \Leftrightarrow \underline{m + n}$;
- $\text{MUL } \underline{m} \underline{n} \Leftrightarrow \underline{m * n}$;
- $\text{EXP } \underline{m} \underline{n} \Leftrightarrow \underline{m^n}$.

Definizione 3.2.2: NEXT e PRED

- $\text{NEXT} = \lambda p. \text{PAIR } (\text{SND } p) (\text{SUCC } (\text{SND } p))$;
- $\text{PRED} = \lambda a. \text{FST } (a \text{ NEXT } (\text{PAIR } \underline{0} \underline{0}))$.

Proposizione 3.2.2

- $\text{NEXT } (\text{PAIR } \underline{m} \underline{n}) \Leftrightarrow \text{PAIR } \underline{n} \underline{n+1}$;
- $\text{PRED } \underline{n} \Leftrightarrow \begin{cases} \underline{0} & \text{se } n = 0 \\ \underline{n-1} & \text{se } n > 0 \end{cases}$

Definizione 3.2.3: ISZERO

- $\text{ISZERO} = \lambda a. a (\lambda x. \text{FALSE } \text{TRUE})$.

Proposizione 3.2.3

- $\text{ISZERO } \underline{n} \Leftrightarrow \begin{cases} \text{TRUE} & \text{se } n = 0 \\ \text{FALSE} & \text{se } n \neq 0 \end{cases}$

Definizione 3.2.4: Punto fisso

x è un punto fisso di F se $x = F(X)$

Definizione 3.2.5: Operatore di un punto fisso

$$\text{FIX} = \lambda f. (f(x \ x))(\lambda x. f(x \ x))$$
Proposizione 3.2.4

$$\text{FIX } M \Leftrightarrow M(\text{FIX } M)$$
Note:-

FIX è utilizzato per definire funzioni ricorsive

Definizione 3.2.6: FACT

$\text{FACT} = \text{FIX } \text{AUX}$, dove $\text{AUX} = \lambda f. \lambda a. \text{IF } (\text{ISZERO } a) \ \underline{1} \ (\text{MUL } a \ (f \ (\text{PRED } a)))$

Note:-

AUX "butta via" il punto fisso quando a è zero (caso base), restituendo 1

Proposizione 3.2.5

$$\text{FACT} \Leftrightarrow \lambda a. \text{IF } (\text{ISZERO } a) \ \underline{1} \ (\text{MUL } a \ (\text{FACT } (\text{PRED } a)))$$

3.3 Sintassi delle λ -espressioni con booleani

Definizione 3.3.1: Estensione della sintassi

Espressioni $M, N ::=$

- x (variabile);
- c (costante);
- $\lambda x. M$ (astrazione);
- $M \ N$ (applicazione);
- $\text{if } M \ N_1 \ N_2$ (condizionale).

Costanti $c \in \{\text{False}, \text{True}\}$.

Riduzioni per if

- $\text{if true } M \ N \rightarrow M$;
- $\text{if false } M \ N \rightarrow N$.

Note:-

Quest'estensione introduce possibili errori. Per catturarli si introduce il concetto di *tipo*

Definizione 3.3.2: Sintassi dei tipi

Tipi $t, s ::=$

- Bool (booleani);
- $t \rightarrow s$ (funzioni).

Note:-

Per cui esistono due tipi: Bool e freccia (\rightarrow)

Definizione 3.3.3: Contesto

Un contesto Γ è una funzione parziale da variabili a tipi

Proposizione 3.3.1

- Scriviamo $dom(\Gamma)$ per il dominio di Γ ;
- Scriviamo $x : t$ per il contesto Γ tale che $dom(\Gamma) = \{x\}$ e $\Gamma(x) = t$;
- Scriviamo Γ, Γ' per l'unione di Γ e Γ' quando $dom(\Gamma) = \{x\} \cap dom(\Gamma') = \emptyset$

3.3.1 Regole di tipo

Definizione 3.3.4: Regole di tipo

Le regole di tipo hanno la forma:

$$\frac{\text{Premessa}_1 \dots \text{Premessa}_n}{\text{Conclusione}}$$

Se le premesse sono vere, allora la conclusione è vera

Note:-

Una regola senza premesse è detta *assioma* ed è vero

Definizione 3.3.5: Regole di tipo per il λ -calcolo con costanti

- $[t\text{-var}] = \frac{}{\Gamma, x:t \vdash x:t}$;
- $[t\text{-bool}] = \frac{}{\Gamma \vdash c: \text{Bool}}$;
- $[t\text{-lam}] = \frac{\Gamma, x:t \vdash M:s}{\Gamma \vdash \lambda x. M: t \rightarrow s}$;
- $[t\text{-if}] = \frac{\Gamma \vdash M: \text{Bool} \quad \Gamma \vdash N_1:t \quad \Gamma \vdash N_2:t}{\Gamma \vdash \text{if } M \text{ then } N_1 \text{ else } N_2:t}$;
- $t\text{-app} = \frac{\Gamma \vdash M:t \rightarrow s \quad \Gamma \vdash N:t}{\Gamma \vdash M N:s}$.

Note:-

Le regole vanno lette dalla conclusione fino alle premesse

Lemma 3.3.1 Subject reduction

Se $\Gamma \vdash M : t$ e $M \rightarrow N$, allora $\Gamma \vdash N : t$

Definizione 3.3.6: Valore

Diciamo che M è un *valore* se M è una costante o un'astrazione

Note:-

Un valore è un risultato

Teorema 3.3.1 Progresso

Se $\vdash M : t$ e $M \Rightarrow N \rightarrow$ allora N è un valore

Note:-

Il teorema del progresso enuncia che se M si riduce a N in un certo numero di passi e N non si può ridurre, allora N è ben tipato

Capitolo 4

Algoritmo di inferenza

4.1 Sommario

Definizione 4.1.1: Fasi dell'algoritmo

1. Si costruisce l'albero sintattico della λ -espressione;
2. Si annota l'albero e si generano i vincoli:
 - variabile di tipo: tipo sconosciuto;
 - espressione di tipo: tipo (parzialmente) sconosciuto;
 - vincolo: relazione di uguaglianza tra tipi espressa nelle regole di tipo.
3. Si risolvono i vincoli:
 - Si deve determinare se il sistema ammette almeno una soluzione;
 - Si deve calcolare la soluzione più generale da cui derivare tutte le altre.

4.1.1 Costruzione dell'albero sintattico

- Si rappresenta la λ -espressione come un albero;
- I nodi interni e le foglie sono opportunamente etichettati;
- Indichiamo con $T[M]$ l'albero corrispondente alla λ -espressione.

Definizione 4.1.2: Albero sintattico

- $T[x] = x$ (foglia);
- $T[c] = c$ (foglia);
- $T[\lambda x.M] =$

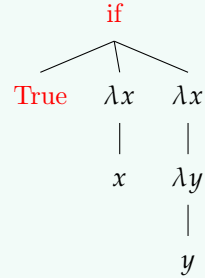
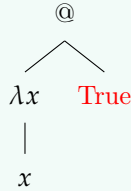
$$\begin{array}{c} \lambda x \\ | \\ T[M] \end{array}$$
- $T[M N] =$

$$\begin{array}{c} @ \\ / \quad \backslash \\ T[M] \quad T[N] \end{array}$$
- $T[\text{if } M \ N_1 \ N_2] =$

$$\begin{array}{c} \text{if} \\ / \quad | \quad \backslash \\ T[M] \quad T[N_1] \quad T[N_2] \end{array}$$

Esempio 4.1.1

- $(\lambda x.y) \text{ True}$
- $\text{if True } (\lambda x.x) (\lambda x.\lambda y.y)$



4.1.2 Annotazione dell'albero e generazione dei vincoli

- Ogni nodo dell'albero viene annotato con un'espressione di tipo;
- Si procede in modo bottom-up, dalle foglie verso la radice.

Definizione 4.1.3: Sintassi delle espressioni di tipo

Sia $TVar = \{\alpha, \beta, \gamma, \dots\}$ un insieme infinito di variabili di tipo e α un tipo sconosciuto^a, le espressioni di tipo $\tau, \sigma ::=$

α (variabile di tipo)

Bool (booleani)

$\tau \rightarrow \sigma$ (funzioni)

^aAncora da determinare

Note:-

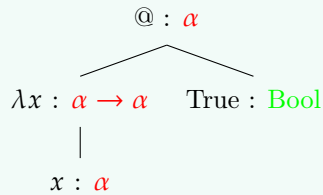
Un vincolo è una coppia di espressioni di tipo scritta come $\tau = \sigma$

Albero	Note
$x : \alpha$	α è nuova, avendo cura di usare la stessa α per tutte le occorrenze della stessa x
$c : \text{Bool}$	Altre costanti richiederanno tipi diversi
$\begin{array}{c} \lambda x : \alpha \rightarrow \tau \\ \\ T : \tau \end{array}$	α è la variabile di tipo usata per annotare x in T se x compare in T o è nuova altrimenti
$\begin{array}{c} @ : \alpha \\ / \quad \backslash \\ T_1 : \tau \quad T_2 : \sigma \end{array}$	α è nuova Generare il vincolo $\tau = \sigma \rightarrow \alpha$
$\begin{array}{c} @ : \tau_2 \\ / \quad \backslash \\ T_1 : \tau_1 \rightarrow \tau_2 \quad T_2 : \sigma \end{array}$	Ottimizzazione facoltativa del caso precedente che evita l'introduzione di una nuova α Generare il vincolo $\tau_1 = \sigma$
$\begin{array}{c} \text{if} : \tau_2 \\ / \quad \quad \backslash \\ T_1 : \tau_1 \quad T_2 : \tau_2 \quad T_3 : \tau_3 \end{array}$	Generare il vincolo $\tau_1 = \text{Bool}$ Generare il vincolo $\tau_2 = \tau_3$

Esempio 4.1.2

$\lambda x.x \text{ True}$

Albero annotato



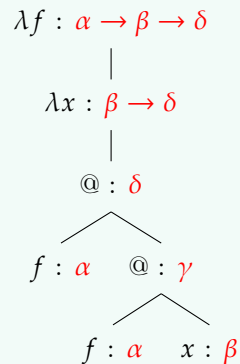
Vincoli generati

$\alpha = \text{Bool}$

Esempio 4.1.3

$\lambda f.\lambda x.f (f x)$

Albero annotato



Vincoli generati

$\alpha = \beta \rightarrow \gamma$

$\alpha = \gamma \rightarrow \delta$

Note:-

Nell'ultimo esempio entrambe le f hanno la stessa annotazione

4.1.3 Sistemi di equazioni e soluzioni

Definizione 4.1.4: Sostituzione

Una sostituzione θ è una funzione da variabili di tipo a espressioni di tipo. Scriviamo $\theta(\tau)$ per l'espressione ottenuta da τ sostituendo ogni α con $\theta(\alpha)$

Definizione 4.1.5: Soluzione

Dato un sistema di vincoli $\{\tau_i = \sigma_i\}_{1 \leq i \leq n}$ e una sostituzione θ diciamo che θ è soluzione (o unificatore) del sistema se $\theta(\tau_i) = \theta(\sigma_i)$ per ogni $1 \leq i \leq n$. Diciamo inoltre che θ è l'unificatore più generale del sistema se ogni soluzione del sistema è ottenibile componendo θ con un'altra sostituzione

Se c'è un vincolo	e	allora
$\tau = \tau$	—	eliminare il vincolo
$\tau = \alpha$	τ non è una variabile	rimpiazzare il vincolo con $\alpha = \tau$
$\tau \rightarrow \tau' = \sigma \rightarrow \sigma'$	—	rimpiazzare il vincolo con $\tau = \sigma$ e $\tau' = \sigma'$
$\tau \rightarrow \sigma = \text{Bool}$ o $\text{Bool} = \tau \rightarrow \sigma$	—	💀 l'algoritmo fallisce (type error)
$\alpha = \tau$	$\alpha \neq \tau$ ma α compare in τ	💀 l'algoritmo fallisce (occur check)
$\alpha = \tau$	α non compare in τ α compare altrove	sostituire α con τ in tutti gli altri vincoli ($\alpha = \tau$ rimane)

Note:-

L'ordine in cui si applicano le trasformazioni non è importante. Se non si può applicare nessuna trasformazione l'algoritmo ha avuto successo

Proposizione 4.1.1

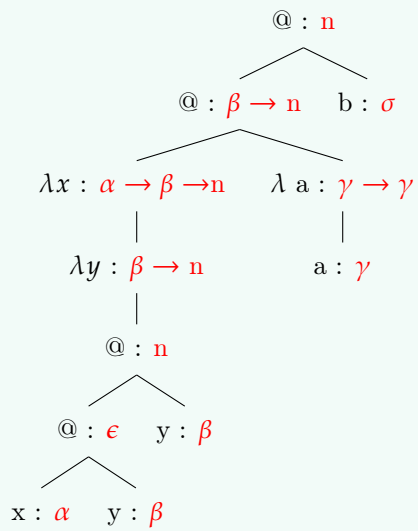
- In un numero finito di passi l'algoritmo ha successo o fallisce;
- Se l'algoritmo fallisce allora il sistema è insoddisfacibile;
- Se l'algoritmo ha successo:
 - il sistema ha forma $\{\alpha_i = p_i\}_{1 \leq i \leq m}$ in cui ciascuna α_i compare una sola volta nel sistema;
 - la sostituzione $\theta = \{\alpha_i \rightarrow p_i\}_{1 \leq i \leq m}$ è l'unificatore più generale del sistema iniziale, in particolare $\sigma(\tau_i) = \theta(\sigma_i)$ per ogni $i \leq m$.

Esempio 4.1.4

►	$\alpha = \beta \rightarrow \gamma$ $\alpha = \gamma \rightarrow \delta$	►	$\alpha = \beta \rightarrow \beta$ $\alpha = \text{Bool} \rightarrow \gamma$
►	$\alpha = \beta \rightarrow \gamma$ $\beta \rightarrow \gamma = \gamma \rightarrow \delta$	►	$\alpha = \beta \rightarrow \beta$ $\beta \rightarrow \beta = \text{Bool} \rightarrow \gamma$
►	$\alpha = \beta \rightarrow \gamma$ $\beta = \gamma$ $\gamma = \delta$	►	$\alpha = \beta \rightarrow \beta$ $\beta = \text{Bool}$ $\beta = \gamma$
►	$\alpha = \gamma \rightarrow \gamma$ $\beta = \gamma$ $\gamma = \delta$	►	$\alpha = \text{Bool} \rightarrow \text{Bool}$ $\beta = \text{Bool}$ $\text{Bool} = \gamma$
	$\alpha = \delta \rightarrow \delta$ $\beta = \delta$ $\gamma = \delta$		$\alpha = \text{Bool} \rightarrow \text{Bool}$ $\beta = \text{Bool}$ $\gamma = \text{Bool}$

Esempio 4.1.5 (Esercizio)

$(\lambda x. \lambda y. x \ y \ y)(\lambda a. a) b$



$\alpha = \beta \rightarrow \epsilon$
 $\epsilon = \beta \rightarrow n$
 $\alpha = \gamma \rightarrow \gamma$
 $\beta = \sigma$

Risoluzione:

$$\begin{cases} \alpha = \beta \rightarrow \epsilon \\ \epsilon = \beta \rightarrow n \\ \alpha = \gamma \rightarrow \gamma \\ \beta = \sigma \\ \alpha = \beta \rightarrow \epsilon \\ \epsilon = \beta \rightarrow n \\ \beta \rightarrow \epsilon = \gamma \rightarrow \gamma \\ \beta = \sigma \\ \alpha = \beta \rightarrow \epsilon \\ \epsilon = \beta \rightarrow n \\ \beta = \gamma \\ \epsilon = \gamma \\ \beta = \sigma \end{cases}$$

$$\begin{cases} \alpha = \gamma \rightarrow \epsilon \\ \epsilon = \gamma \rightarrow n \\ \beta = \gamma \\ \epsilon = \gamma \\ \gamma = \sigma \\ \alpha = \gamma \rightarrow \gamma \rightarrow n \\ \epsilon = \gamma \rightarrow n \\ \beta = \gamma \\ \gamma \rightarrow n = \gamma \\ \gamma = \sigma \\ \alpha = \gamma \rightarrow \gamma \rightarrow n \\ \epsilon = \gamma \rightarrow n \\ \beta = \gamma \\ \gamma = \gamma \rightarrow n \\ \gamma = \sigma \end{cases}$$

! OCCUR CHECK FAIL !

4.2 Estensioni dell'algoritmo

Definizione 4.2.1: Numeri interi

Le costanti includono i numeri interi

$$c \in \{\text{False}, \text{True}, 0, 1, \dots\}$$

Le espressioni di tipo sono arricchite con il tipo **Int**

Note:-

Se c'è un vincolo $\tau \rightarrow \sigma = \text{Int}$ o $\text{Int} = \text{Bool}$ o $\text{Bool} = \text{Int}$ l'algoritmo fallisce (**TYPE ERROR**)

Definizione 4.2.2: Liste

Le costanti includono i costruttori canonici

$$c \in \{\dots, [], (:)\}$$

Ogni occorrenza di un costruttore fa uso di nuove variabili di tipo

Note:-

- Se c'è un vincolo $[\tau] = [\sigma]$ rimpiazzarlo con $\tau = \sigma$;
- Se c'è un vincolo $[\tau] = \text{Bool}$ o $\text{Bool} = [\tau]$ o $[\tau] = \sigma_1 \rightarrow \sigma_2$ o ... l'algoritmo fallisce (**TYPE ERROR**)

Definizione 4.2.3: Funzioni di libreria

Le costanti includono le funzioni di libreria

$$c \in \{\dots, \text{id}, \text{head}, \text{tail}, \dots\}$$

Ogni occorrenza di una funzione di libreria fa uso di nuove variabili di tipo

Definizione 4.2.4: Definizioni ricorsive

$$f = M$$

dove f può comparire in M . Il nome f è trattato come ogni altra variabile. Alla fine dell'annotazione si genera il vincolo $\alpha = \tau$ dove α è la variabile di tipo associata a f e τ è l'annotazione di M

Capitolo 5

Dimostrazione di proprietà di funzioni su numeri interi

Domanda 1

Date una funzione e una specifica di ciò che la funzione dovrebbe calcolare, la funzione è corretta rispetto alla specifica?

Domanda 2

Date due funzioni (una corretta ma inefficiente e una efficiente ma più complessa da capire), sono equivalenti?

Test:

- facile (soprattutto se il linguaggio non è imperativo);
- non è esaustivo (possono esserci casi non considerati).

Dimostrazione:

- difficile (soprattutto se il linguaggio è imperativo);
- è esaustiva.

5.1 Dimostrazioni

```
1 foo :: Int -> Int -> Int -> Int
2 foo x y z | y < x      = foo y x z
3           | z < y      = foo x z y
4           | otherwise = z
```

Domanda 3

$\forall x, y, z = \max \{x, y, z\}$ è una proprietà vera?

Si possono fare dei test, ma saranno sempre in numero finito. Per cui è più conveniente cercare una dimostrazione.

5.1.1 Dimostrazione per casi

Note:-

I numeri sono infinite, per cui non si può verificare il comportamento per ogni combinazione. Ma l'ordine tra i numeri è totale, per cui possiamo considerare un numero finito di casi che è esaustivo

- 1 $x \leq y \leq z \Rightarrow \text{foo } x y z = z$
- 2 $x \leq z < y \Rightarrow \text{foo } x y z = \text{foo } x z y = y$
- 3 $y < x \leq z \Rightarrow \text{foo } x y z = \text{foo } y x z = z$
- 4 $y \leq z < x \Rightarrow \text{foo } x y z = \text{foo } y x z = \text{foo } y z x = x$
- 5 $z < x \leq y \Rightarrow \text{foo } x y z = \text{foo } x z y = \text{foo } z x y = y$
- 6 $z < y < x \Rightarrow \text{foo } x y z = \text{foo } y x z = \text{foo } y z x = \text{foo } z y x = x$

Note:-

Il codice è tutto ciò che serve per ragionare sui casi

5.1.2 Induzione

Note:-

L'approccio precedente è attuabile solo se il numero dei casi da prendere in considerazione è finito. Il principio di induzione permette di dimostrare una proprietà su un insieme infinito di casi

Definizione 5.1.1: Il principio di induzione

Data una proprietà $P(n)$ dei numeri naturali, se:

- $P(0)$;
- $P(n)$ implica $P(n + 1)$ per ogni $n \in \mathbb{N}$.

allora $P(n)$ per ogni $n \in \mathbb{N}$

```
1 exp :: Int -> Int -> Int -> Int
2 exp _ 0 = 1
3 exp x n = x * exp x (n - 1)
```

Esempio 5.1.1 (Esponenziale)

Si vuole dimostrare che:

1. $\forall x, m \geq 0, n \geq 0 : \exp x (m + n) = \exp x m * \exp x n$;
2. $\forall x, n : \exp (x * x) n = \exp x n * \exp x n$.

Prima dimostrazione:

$$\begin{aligned}
 P(m) &\stackrel{\text{def}}{=} \forall x, n \geq 0 : \exp x (m + n) = \exp x m * \exp x n \\
 P(0) & \text{ lato sinistro} \\
 \exp x (0 + n) & \\
 = \exp x n & \text{ (proprietà di +)} \\
 P(0) & \text{ lato destro} \\
 \exp x 0 * \exp x n & \\
 = 1 * \exp x n & \text{ (exp. 1)} \\
 = \exp x n & \text{ (proprietà di *)} \\
 P(m - 1) \Rightarrow P(m) \text{ per ogni } m > 0 & \text{ lato sinistro} \\
 \exp x (m + n) & \\
 = x * \exp x ((m + n) - 1) & \text{ (exp. 2)} \\
 = x * \exp x ((m - 1) + n) & \text{ (proprietà di + e -)} \\
 = x * (\exp x (m - 1) * \exp x n) & \text{ (ipotesi induttiva)} \\
 P(m - 1) \Rightarrow P(m) \text{ per ogni } m > 0 & \text{ lato destro} \\
 \exp x m * \exp x n & \\
 = (x * \exp x (m - 1)) * \exp x n & \text{ (exp. 2)} \\
 = x * (\exp x (m - 1) * \exp x n) & \text{ (proprietà di *)}
 \end{aligned}$$

Seconda dimostrazione:

$$\begin{aligned}
 P(n) &\stackrel{\text{def}}{=} \forall x : \exp (x * x) n = \exp x n * \exp x n \\
 P(0) & \text{ lato sinistro} \\
 \exp (x * x) 0 = 1 & \text{ (exp. 1)} \\
 P(0) & \text{ lato destro} \\
 \exp x 0 * \exp x 0 & \\
 = 1 * 1 & \text{ (exp. 1)} \\
 = 1 & \text{ (proprietà di *)} \\
 P(n - 1) \Rightarrow P(n) \text{ per ogni } n > 0 & \text{ lato sinistro} \\
 \exp (x * x) n & \\
 = (x * x) * \exp (x * x) (n - 1) & \text{ (exp. 2)} \\
 = (x * x) * (\exp x (n - 1) * \exp x (n - 1)) & \text{ (ipotesi induttiva)} \\
 P(n - 1) \Rightarrow P(n) \text{ per ogni } n > 0 & \text{ lato destro} \\
 \exp x n * \exp x n & \\
 = (x * \exp x (n - 1)) * (x * \exp x (n - 1)) & \text{ (exp. 2)} \\
 = (x * x) * (\exp x (n - 1) * \exp x (n - 1)) & \text{ (proprietà di *)}
 \end{aligned}$$

Definizione 5.1.2: Principio di induzione forte

Data una proprietà $P(n)$ dei numeri naturali, se:

- $(\forall m < n : P(m)) \Rightarrow P(n)$, per ogni $n \in \mathbb{N}$.

allora $P(n)$ per ogni $n \in \mathbb{N}$

Note:-

Il principio di induzione forte è equivalente al principio di induzione

5.2 Dimostrazioni sulle liste

Definizione 5.2.1: Principio di induzione sulle liste finite

Data una proprietà $P(xs)$ delle liste, se:

- $P([])$;
- $P(xs)$ implica $P(x : xs)$ per ogni x e xs .

Allora $P(xs)$ per ogni lista finita xs .

Esempio 5.2.1 (Length)

$$P(n) \stackrel{\text{def}}{=} \forall x : \text{exp } (x * x) \ n = \text{exp } x \ n * \text{exp } x \ n$$

$$P(0)$$

$$\text{exp } (x * x) \ 0 = 1$$

lato sinistro

(exp.1)

$$P(0)$$

$$\text{exp } x \ 0 * \text{exp } x \ 0$$

$$= 1 * 1$$

$$= 1$$

lato destro

(exp.1)

(proprietà di *)

$$P(n-1) \Rightarrow P(n) \text{ per ogni } n > 0$$

$$\text{exp } (x * x) \ n$$

$$= (x * x) * \text{exp } (x * x) \ (n-1)$$

$$= (x * x) * (\text{exp } x \ (n-1) * \text{exp } x \ (n-1))$$

lato sinistro

(exp.2)

(ipotesi induttiva)

$$P(n-1) \Rightarrow P(n) \text{ per ogni } n > 0$$

$$\text{exp } x \ n * \text{exp } x \ n$$

$$= (x * \text{exp } x \ (n-1)) * (x * \text{exp } x \ (n-1))$$

$$= (x * x) * (\text{exp } x \ (n-1) * \text{exp } x \ (n-1))$$

lato destro

(exp.2)

(proprietà di *)

Note:-

Può capitare, durante una dimostrazione, di osservare passaggi intuitivi di cui non si ha una prova. Per cui si possono assumere e poi dimostrare in seguito

5.3 Dimostrazioni sugli alberi

Definizione 5.3.1: Principio di induzione sugli alberi

Data una proprietà $P(t)$, se:

- $P(Leaf)$;
- $P(t_1)P(t_2)$ implica $P(Branch\ t_1t_2)$ per ogni x , t_1 e t_2 .

Allora $P(t)$ per ogni albero (finito) t .