



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



DIPARTIMENTO
MATEMATICA

Università degli Studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Laurea Magistrale in Informatica

Esame di Teoria dei Tipi

Teoria dei Tipi
Elaborato scritto - Settembre 2020
Eleonora Signor, 1237581

Indice

1	Introduzione	5
1.1	La triplice faccia della teoria dei tipi	5
1.2	Come nasce la teoria dei tipi	5
1.3	Il Paradosso di Russell	6
1.4	Idee principali nelle teorie di tipo moderne	7
1.4.1	Richiamo della teoria del λ -calcolo di <i>Church</i>	7
1.5	Che cosa è un tipo?	8
1.6	Esempi di tipi	10
1.6.1	I tipi dipendenti	10
1.7	Regole paradigmatiche per caratterizzare la teoria dei tipi	11
1.7.1	Simbolo \in	11
1.7.2	Uguaglianza definizionale vs uguaglianza proposizionale	12
1.7.3	Generazione di contesti	12
2	Regole della teoria dei tipi	13
2.1	Regole strutturali	13
2.1.1	Regole di formazione dei contesti	13
2.1.2	Regole di assunzione delle variabili	14
2.1.3	Regole strutturali addizionali sull'uguaglianza	14
2.1.4	Regole di conversione dell'uguaglianza per tipi uguali	14
2.1.5	Regole di indebolimento e di sostituzione	14
2.1.6	Regole proprie e derivabili	15
2.1.7	Nozione di contesto telescopico	16
2.1.8	Esempi di applicazione	16
2.1.9	Regole di tipaggio	17
2.2	Il tipo singoletto	17
2.2.1	Regola di formazione	17
2.2.2	Regole di Introduzione	18
2.2.3	Regole di Eliminazione	18
2.2.4	Regole di Conversione	18
2.2.5	Osservazioni sul tipo singoletto	19
2.3	Sanitary checks rules	19
2.4	Esercizi	20
3	Naturali, Somma disgiunta e liste	21
4	Uguaglianza proposizionale	23

5	Somma indicata forte e prodotto cartesiano	25
---	--	----

6	Tipo delle funzioni e tipo prodotto dipendente	27
---	--	----

7	La logica della teoria dei tipi di <i>Martin-Löf</i>	29
---	--	----

A	Tabelle	31
---	---------	----

Capitolo 1

Introduzione

1.1 La triplice faccia della teoria dei tipi

La teoria dei tipi offre una base teorica a fondamento dello sviluppo di:

- **Matematica:** nella teoria degli insiemi;
- **Logica:** come fondamento dei connettivi logici e dei quantificatori, con trattazione mediate tecniche di *proof-theory* per dimostrarne la non falsità o non contraddittorietà;
- **Informatica:** per la correttezza dei programmi, da una semantica operativa a un certo tipo di operazioni.
Con riferimento alla teoria degli insiemi, visto come linguaggio di programmazione funzionale, è possibile specificare con formule l'obiettivo di un programma e dimostrarne la correttezza attraverso la specifica.

La teoria dei tipi nasce per garantire la *Certified Proof Correctness*. Ovvero la correttezza dei programmi, volta a costruire gli assistenti automatici per le formalizzazioni.

1.2 Come nasce la teoria dei tipi

Gli errori di programmazione sono stati preponderanti alla nascita di metodi automatici, che assicurassero la correttezza del *software*. Alcuni di questi, degni di nota, sono stati:

- Incidente nel lancio dell'Apollo 11;
- Tragedie sanitarie: incidenti avvenuti tra il 1985-1987, in cui dei pazienti ricevettero una massiccia *overdose* di radiazioni e per la quali alcuni morirono;
- Errori di vita civile: riserva di solo due cifre per il campo età all'interno dei *database*. Ecco che una signora danese ricevette per il suo 107-esimo compleanno, una mail dalle autorità della scuola locale per iscriversi alla prima elementare.

Per la matematica la correttezza delle dimostrazioni è irrilevante solo quando la soluzione è certa (come accade con il cubo di *Rubik*, dove so che la soluzione è corretta quando ognuno dei lati è uniformemente colorato); e in generale questo è difficile che accada.

Un'esempio di problema, dove la soluzione non è certa, è il Teorema dei Quattro Colori, risolto da un *computer* e la cui prova di correttezza della dimostrazione fu data dal *proof assistant* Coq. Quest'ultimo basato sulla teoria dei tipi e in-
tellegibile dall'essere umano.

Una citazione importante va al matematico Russo V.V. *Voevodsky*, vincitore della medaglia *Fields*. Esso si battè per la creazione di un *proof assistant*, per rendere le dimostrazioni da informali, per problemi complessi, a completamente formalizzate, con l'impiego della teoria dei tipi. I suoi studi trovano principale applicazione in campo algebrico e geometrico; ma i concetti emersi assunsero delle connotazioni più ampie. *Voevodsky*, difatti, si rese conto che formalizzare equivale a programmare. Ciò significa che la teoria dei tipi permette di vedere una dimostrazione come un programma.

Esiste la certezza assoluta per una certa teoria, esclusivamente, quando ha un numero di assiomi, accettati per fede, molto limitato. In quanto assiomalizzabile da un calcolatore.

In conclusione formalizzare in una teoria dei tipi (come quella degli insiemi) equivale a programmare un programma.

1.3 Il Paradosso di Russell

La base della teoria dei tipi, compresa quella di *Martin-Löf*, si deve a B. *Russell*. Siamo nel 1907 quando nasce la teoria dei tipi, sviluppata nei *Principia Mathematica* da B. *Russel* assieme ad A.N. *Whitehead*. Tale teoria, intesa come logica e non informatica, nasce come soluzione alternativa alla teoria degli insiemi, di allora, con lo scopo di fondare la matematica su un sistema formale accettabile e non contraddittorio.

Di seguito espongo un sistema contraddittorio della teoria degli insiemi.

Linguaggio L di una teoria degli insiemi F

- L linguaggio del primo ordine ($=, \&, \rightarrow, \vee, \forall x, \exists x$), con l'aggiunta del predicato \in "appartiene"
- variabili $\text{VAR} \ni \{x, y, z, w, \dots\}$

dove x, y, z sono da intendersi come insiemi e $x \in y =$ "x appartiene a y".

All'interno di L c'è una teoria degli insiemi. Tra cui prende posto l'**assioma di comprensione di Frege**, definito nel modo seguente:

Per ogni formula $\phi(x)$ vale che $\exists z \forall y (y \in z \Leftrightarrow \phi(y)) [\equiv \exists z z = \{x \mid \phi(x)\}]$

Teorema (o Paradosso) di Russell: la teoria F è contraddittoria.

Dimostrazione:

$$\phi(x) = x \notin x \ (\equiv \neg (x \in x))$$

Per l'assioma di comprensione $\exists z \ z = \{x \mid x \notin x\}$ ($\exists z \ \forall y \ (y \in z \Leftrightarrow y \notin y)$)

Ponendo $y=z$ ottengo che $z \in z \Leftrightarrow z \notin z$, risulta una **contraddizione**.

L'assioma di comprensione è contraddittorio perchè permette di formare insiemi che non appartengono a se stessi.

Come correggere la contraddizione?

La soluzione accettabile è porre agli insiemi una **gerarchia di tipi**. In questo modo l'assioma di comprensione diventa:

$$\exists z \ \forall y \ (y \in a \rightarrow (y \in z \Leftrightarrow \phi(y))) \equiv z = \{x \in a \mid \phi(x)\}$$

In questo modo non posso più creare il Paradosso di *Russell*.

Al momento questa teoria dei tipi non è utilizzata. Una sua evoluzione diretta è la teoria dei tipi di *Martin-Löf*.

L'idea di *Russell* fu dunque quella di costruire insiemi partendo da una gerarchia.

1.4 Idee principali nelle teorie di tipo moderne

Le teorie di tipo moderne (chiamate λ -calcolo tipato) nascono, nel corso degli anni '30, dalla combinazione della teoria di tipo di *Russell* con il λ -calcolo di *Church*.

1.4.1 Richiamo della teoria del λ -calcolo di *Church*

Ha origine dalla logica, è un linguaggio in grado di trattare le funzioni e rivolto alla loro formalizzazione. Consiste in un linguaggio formale, le cui componenti principali sono programmi chiamati termini (pensati come funzioni).

La grammatica è la seguente:

$$t := x \mid b_1(b_2) \mid \lambda x.t$$

Esempio di applicazione: $tg(x) \equiv \lambda x.tg(x)$

Regole di computazione di base

$$(\lambda x.t)(b) \rightarrow t\left[\frac{x}{b}\right] \quad \frac{b_1 \rightarrow b_2 \quad a_1 \rightarrow a_2}{b_1(a_1) \rightarrow b_2(a_2)} \quad \frac{b_1 \rightarrow b_2}{\lambda x.b_1 \rightarrow \lambda x.b_2}$$

Si dice che un programma si riduca a un altro, cioè converge, solo se c'è una sequenza di riduzioni (applicazione di regole e/o assiomi), che connettono il primo programma con l'ultimo. Si parla, in questo modo, di **chiusura transitiva e simmetrica**, che si conclude quando il programma non è più riducibile. Quanto appena descritto può venire espresso nel seguente modo:

$t \rightarrow t'$ sse esiste un numero finito di passi per cui t si riduce a t' , ovvero esiste

$b_1 \dots b_m$ t.c. $t \rightarrow b_1 \rightarrow b_2 \dots \rightarrow b_m \rightarrow t'$.

Il λ calcolo permette di codificare qualsiasi programma scritto in qualunque linguaggio (imperativo, dichiarativo, Java, C++, BASIC, ...). Tuttavia tale linguaggio non codifica solo programmi che terminano, ma anche programmi che non lo fanno. Un esempio di applicazione, per quest'ultima categoria, è un programma con computazione infinita: $\lambda x.x(x)$

$\lambda x.x(x)$ lo applichiamo a se stesso. Perciò diventa $\Lambda \equiv (\lambda x.x(x))(\lambda x.x(x))$ che seguendo la computazione si riduce a:

$$x(x)\left[\frac{x}{\lambda x.x(x)}\right] \equiv (\lambda x.x(x))(\lambda x.x(x))$$

Dunque esiste una catena di $(t_i)_{i \in \mathbb{N}}$ di termini $t_i \rightarrow t_{i+1}$. Ciò significa che Λ non termina in qualunque linguaggio sia interpretato.

Λ risulta un buon metodo per rappresentare le funzioni, ma non è completo, rispetto all'intuizione matematica di funzione. È necessario, per questo, tipare le variabili; ovvero $\lambda x.x \in A \rightarrow B(x \in A)$.

Il λ -calcolo tipato, nato dal λ -calcolo "puro", è anch'esso un linguaggio di programmazione. Essendo tipato può essere trattato come una teoria degli insiemi.

1.5 Che cosa è un tipo?

Per rispondere a questa domanda è necessario fornire la semantica intuitiva di tipo. Per farlo è utile pensare alla teoria dei tipi come paradigma di fondazione sia logico che matematico che informatico.

Sintassi in teoria dei tipi moderna	Sintassi in teoria degli insiemi	Sintassi in un linguaggio logico/per una logica (anche predicativo)	Sintassi in un linguaggio di programmazione
A type	A set	A prop	A data type
$a \in A$	$a \in A$ set	$a \in A$	$a \in A$

Tabella 1.1: Sintassi per i diversi paradigmi funzionali.

Per la sintassi:

- nella **teoria dei tipi moderna** a rappresenta un termine e A un tipo;
- nella sintassi in una **teoria degli insiemi** a è un elemento e A un insieme. Coincidendo con la corrispondenza originale in mente da *Russell*.
- nella sintassi in un **linguaggio logico** a rappresenta una proposizione di A , inteso come insieme di tipo delle sue dimostrazioni. Perciò un *proof-term* affermatore come la proposizione di A sia vera.

- nella teoria in una sintassi di un **linguaggio di programmazione** a rappresenta un programma e A una specifica.

Dunque quando parliamo di tipo ci riferiamo a un insieme, una proposizione o *data type*, a seconda dell'applicazione di tipo che si ha in mente.

Dal punto di vista logico non si hanno solo proposizioni, ma anche predicati. Parlare solo di tipo non risulta quindi sufficiente. Per questo se si vuole rappresentare non una proposizione, ma un predicato $A(x)$ si usa la seguente sintassi: **$A(x)$ prop[$x \in D$]**.

Dalla logica si sa che i predicati $\phi(x)$ hanno x senza un dominio specifico, perchè la sintassi non determina che cosa è in x . Al seguito di tutto questo i predicati hanno una variabile che deve essere tipata come **$\phi(x)$ prop[$x \in D$]**.

Dunque (definizione di predicato)

$$\exists \mathbf{z} \quad \mathbf{z} = \{x \in \mathbf{a} \mid \phi(x)\} \quad \equiv \quad \phi(x) \text{prop}[x \in \mathbf{a}]$$

Quanto appena definito da origine al concetto di **tipo dipendente**, nel quale vengono tipate tutte le variabili che appartengono ad una **famiglia di tipo**.

Le famiglie di tipo sono indispensabili per rappresentare il concetto di predicato. Di seguito ho riassunto in forma tabellare le diverse famiglie.

di tipo	negli insiemi	in logica	dati dipendenti
$A(x)$ prop[$x \in D$]	$A(x)$ set[$x \in D$]	$A(x)$ prop[$x \in D$]	$A(x)$ datatype[$x \in D$]

Tabella 1.2: Famiglia di tipi.

Il concetto di tipo dipendente è stato introdotto per la prima volta da *Martin-Löf*. *Russell* si era limitato a definire esclusivamente il concetto di funzione proposizionale dipendente da un tipo.

1.6 Esempi di tipi

A type	A set	A prop	A data type
N_1 singoletto	l'insieme singoletto	tt costante vero	tipo Unit
N_0 vuoto	l'insieme vuoto	\perp costante falso	vuoto come data-type
$B \times C$ (tipo prodotto)	l'insieme prodotto cartesiano dell'insieme B con l'insieme C	$B \& C$ congiunzione della proposizione B e della proposizione C	tipo prodotto cartesiano (come in <i>set theory</i>)
$B + C$ (tipo somma binaria)	l'insieme unione disgiunta dell'insieme B con l'insieme C	$B \vee C$ disgiunzione della proposizione B e della proposizione C	tipo unione disgiunta con codifica
$B \rightarrow C$	l'insieme delle funzioni dall'insieme B verso l'insieme C: $A \rightarrow B \equiv \{f \mid f: B \rightarrow C\}$	$B \rightarrow C$, implicazione della proposizione B e della proposizione C	insieme delle funzioni dal <i>datatype</i> B al <i>datatype</i> C

Tabella 1.3: Famiglia di tipi.

1.6.1 I tipi dipendenti

$A(x)\text{type}[x \in B]$
tipo indicato
$\prod_{x \in B} C(x)$
tipo somma disgiunta indicata
$\sum_{x \in B} C(x)$

$A(x)\text{set}[x \in B]$	$A(x)\text{prop}[x \in B]$	$A(x)\text{datatype}[x \in B]$
$\{f : B \rightarrow \prod_{x \in B} C(x)\}$	$\forall x \in B \quad C(x)$	tipo prodotto indicato come in <i>set theory</i> (non esiste un <i>data-type</i> specifico)
$\prod_{x \in B} C(x) = \{b, c \mid b \in B \quad c \in C(b)\}$		
$\bigcup_{x \in B} C(x)$	$\exists x \in B \quad C(x)$	non è primitivo deriva sempre dalla <i>set theory</i>
$\prod_{x \in B} C(x) = \{b, c \mid b \in B \quad c \in C(b)\}$		

Tabella 1.4: Tipi dipendenti.

1.7. REGOLE PARADIGMATICHE PER CARATTERIZZARE LA TEORIA DEI TIPI¹¹

Lo slogan principale della teoria dei tipi è quello di tipare le variabili in un linguaggio formale set teorico/computazionale.

Esiste anche il **tipo uguaglianza**:

- intensionale: $\text{Id}(B, c, d)$;
- estensionale: $\text{Eq}(B, c, d)$.

Introdotta da *Martin-Löf*.

E i costrutti degli **universi**, in cui U è universo di proposizioni e di insiemi.

1.7 Regole paradigmatiche per caratterizzare la teoria dei tipi

La teoria dei tipi è stata formalizzata usando la nozione di **giudizio**, dove si asserisce qualcosa come vero.

Ci sono quattro forme di giudizio (nelle quali Γ identifica il contesto):

- **$A \text{ type}[\Gamma]$** : A è un tipo, possibilmente indicato da variabili nel contesto Γ , dipendente da Γ stesso. Rappresenta il giudizio di tipo.
- **$A = B \text{ type}[\Gamma]$** : il tipo A dipendente da Γ è uguale al tipo B dipendente da Γ . Rappresenta il giudizio di uguaglianza di tipo.
- **$a \in A \text{ type}[\Gamma]$** : a è un elemento del tipo A , possibilmente indicato, ovvero dipendente da Γ e dalle sue variabili di contesto. Un esempio di tipo dipendente è l'array, che ha termini di funzioni che dipendono da Γ . Invece il termine non è dipendente quando si parla di funzione costante senza variabili.
- **$a = b \in A \text{ type}[\Gamma]$** : a come elemento del tipo A dipende da Γ ed è uguale in modo definizionale/computazionale al termine b . Quest'ultimo, difatti, è elemento del tipo A dipendente da Γ .

All'interno di ogni singolo giudizio si lavora con la teoria dei tipi.

I giudizi solo esclusivamente asserzioni, dicono solo qualcosa quando è vero (non si usano i quantificatori). Essi limitano le frasi che si possono fare per codificare la logica intuizionistica.

1.7.1 Simbolo \in

Il significato di $a \in A$ in teoria dei tipi è differente da quello insiemistico. Espongo il concetto con un esempio trattato a lezione:

$$1 \in \text{Nat} \tag{1.1}$$

- In *set theory* usuale \in è tra insiemi. Nell'equazione 1.1, 1 rappresenta lui stesso un'insieme e Nat l'insieme dei numeri Naturali. Risulta vero che $1 \equiv \{\emptyset\}$, poichè $0 \equiv \emptyset$.
- Invece in **teoria dei tipi** (di *Martin-Löf* come di *Russell*) 1 rappresenta un elemento ma non un tipo e Nat il tipo dei Naturali. Vi è dunque la distinzione tra elemento e tipo (come esiste quella tra programmi e tipi).

1.7.2 Uguaglianza definizionale vs uguaglianza proposizionale

Specifico $\mathbf{a} = \mathbf{b} \in \mathbf{A}[\Gamma]$ come l'uguaglianza computazionale/definizionale, che viene data come primitiva e non va confusa con l'uguaglianza proposizionale/estensionale tra a e b .

L'uguaglianza proposizionale $a = b$ è rappresentata non da un giudizio, che asserisce solo ciò che è vero, ma bensì da un tipo $\text{Eq}(A, a, b)$ che può anche essere senza termini e/o essere falso, dal punto di vista logico.

Visti come programmi, a e b rappresentano lo stesso programma. In λ -calcolo $a \rightarrow b$ oppure $b \rightarrow a$ (si riducono). Inoltre a e b possono essere sia termini finali che trovarsi in mezzo alla computazione.

1.7.3 Generazione di contesti

Esiste anche un quinto giudizio ausiliario (§ 2.1.1) $F\text{-}C$, che permette di generare i contesti. Tale giudizio, a differenza dei primi quattro, rimane immutato in ogni teoria dei tipi.

Capitolo 2

Regole della teoria dei tipi

Lo scopo della teoria dei tipi è offrire un sistema formale in cui derivare, tramite regole e assiomi, giudizi nella forma:

$$\begin{array}{l} A \text{ type}[\Gamma] \quad A = B \text{ type}[\Gamma] \quad a \in A \text{ type}[\Gamma] \quad a = b \in A \text{ type}[\Gamma] \\ + \text{ ausiliaria } \Gamma \text{ cont} \end{array}$$

L'ultimo giudizio non è necessario, serve esclusivamente per imparare. Quando si formula una nuova teoria dei tipi è bene impiegare il minor numero possibile di regole strutturali e di formazione di tipi e termini. Tali regole devono essere rivolte all'ottimizzazione e correttezza della teoria. Alcune di queste, come quelle di indebolimento e sostituzione in §2.1.5, sono irrinunciabili, la cui validità è sempre garantita e utilizzate nella derivazione di ogni teoria.

Se la teoria dei tipi è dipendente si ha bisogno di tutti i giudizi. Invece in una teoria dei tipi non dipendente, come quella dei tipi semplici, il giudizio $A = B \text{ type}[\Gamma]$ può venire omissa.

2.1 Regole strutturali

Assioma unico: $[\] \text{ cont}$

Nel calcolo dei sequenti, in logica classica, le derivazioni di giudizio, valide in una teoria dei tipi con solo le regole singoletto, diventano derivazioni di sequenti nella forma $\Gamma \multimap A$ e unico assioma $\varphi \multimap \varphi$.

Di seguito illustro le principali regole di contesto comuni a tutte le teorie dei tipi.

2.1.1 Regole di formazione dei contesti

$$[\] \text{ cont} \quad \text{dove } [\] = \emptyset$$

$$\text{F-C)} \frac{A \text{ type}[\Gamma]}{\Gamma, x \in A} \quad x \in A \notin \Gamma$$

2.1.2 Regole di assunzione delle variabili

$$\text{var-ass)} \frac{\Gamma, x \in A, \Delta \quad \text{cont}}{x \in \text{type}[\Gamma, x \in A, \Delta]}$$

2.1.3 Regole strutturali aggiuntive sull'uguaglianza

L'uguaglianza, in una teoria dei tipi, consiste in una relazione di equivalenza sia fra tipi che fra termini. Sono perciò valide le seguenti regole di uguaglianza tra tipi:

$$\begin{aligned} \text{ref)} \quad & \frac{A \text{ type}[\Gamma]}{A = A \text{ type}[\Gamma]} & \text{sym)} \quad & \frac{A = B \text{ type}[\Gamma]}{B = A \text{ type}[\Gamma]} \\ \text{tra)} \quad & \frac{A = B \text{ type}[\Gamma] \quad B = C \text{ type}[\Gamma]}{A = C \text{ type}[\Gamma]} \end{aligned}$$

E allo stesso modo anche le regole di uguaglianza definizionale/computazionale tra termini:

$$\begin{aligned} \text{ref)} \quad & \frac{a \in A \text{ type}[\Gamma]}{a = a \in A \text{ type}[\Gamma]} & \text{sym)} \quad & \frac{a = b \in A \text{ type}[\Gamma]}{b = a \in A \text{ type}[\Gamma]} \\ \text{tra)} \quad & \frac{a = b \in A \text{ type}[\Gamma] \quad b = c \in A \text{ type}[\Gamma]}{a = c \in A \text{ type}[\Gamma]} \end{aligned}$$

2.1.4 Regole di conversione dell'uguaglianza per tipi uguali

L'appartenenza si conserva con l'uguaglianza di termini e tipi. Le regole da aggiungere, in una teoria dei tipi, per garantirlo sono:

$$\begin{aligned} \text{conv)} \quad & \frac{a \in A \text{ type}[\Gamma] \quad A = B \text{ type}[\Gamma]}{a \in B \text{ type}[\Gamma]} \\ \text{conv - eq)} \quad & \frac{a = b \in A \text{ type}[\Gamma] \quad A = B \text{ type}[\Gamma]}{a = b \in B \text{ type}[\Gamma]} \end{aligned}$$

2.1.5 Regole di indebolimento e di sostituzione

Indebolimento

$$\begin{aligned} \text{ind - ty)} \quad & \frac{A \text{ type}[\Gamma] \quad \Gamma, \Delta \text{ cont}}{A \text{ type}[\Gamma, \Delta]} & \text{ind - ty - eq)} \quad & \frac{A = B \text{ type}[\Gamma] \quad \Gamma, \Delta \text{ cont}}{A = B \text{ type}[\Gamma, \Delta]} \\ \text{ind - te)} \quad & \frac{a \in A \text{ type}[\Gamma] \quad \Gamma, \Delta \text{ cont}}{a \in A \text{ type}[\Gamma, \Delta]} & \text{ind - te)} \quad & \frac{a = b \in A \text{ type}[\Gamma] \quad \Gamma, \Delta \text{ cont}}{a = b \in A \text{ type}[\Gamma, \Delta]} \end{aligned}$$

Sostituzione

$$\text{sub - typ)} \quad \frac{C(x_1, \dots, x_n) \text{ type}[\Gamma, x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})] \quad a_1 \in A_1 \text{ type}[\Gamma] \dots a_n \in A_n(a_1, \dots, a_{n-1}) \text{ type}[\Gamma]}{C(a_1, \dots, a_n) \text{ type}[\Gamma]} \quad (2.1)$$

$$\text{sub} - \text{eq} - \text{typ}) \quad \frac{C(x_1, \dots, x_n) \text{ type}[\Gamma, x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})] \quad a_1 = b_1 \in A_1 \text{ type}[\Gamma] \dots a_n = b_n \in A_n(a_1, \dots, a_{n-1}) \text{ type}[\Gamma]}{C(a_1, \dots, a_n) = C(b_1, \dots, b_n) \text{ type}[\Gamma]} \quad (2.2)$$

$$\text{sub} - \text{Eqtyp}) \quad \frac{C(x_1, \dots, x_n) = D(x_1, \dots, x_n) \text{ type}[\Gamma, x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})] \quad a_1 \in A_1 \text{ type}[\Gamma] \dots a_n \in A_n(a_1, \dots, a_{n-1}) \text{ type}[\Gamma]}{C(a_1, \dots, a_n) = D(a_1, \dots, a_n) \text{ type}[\Gamma]} \quad (2.3)$$

$$\text{sub} - \text{eq} - \text{Eqtyp}) \quad \frac{C(x_1, \dots, x_n) = D(x_1, \dots, x_n) \text{ type}[\Gamma, x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})] \quad a_1 = b_1 \in A_1 \text{ type}[\Gamma] \dots a_n = b_n \in A_n(a_1, \dots, a_{n-1}) \text{ type}[\Gamma]}{C(a_1, \dots, a_n) = D(a_1, \dots, a_n) \text{ type}[\Gamma]} \quad (2.4)$$

$$\text{sub} - \text{ter}) \quad \frac{c(x_1, \dots, x_n) \in C(x_1, \dots, x_n) \text{ type}[\Gamma, x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})] \quad a_1 \text{ in } A_1 \text{ type}[\Gamma] \dots a_n \in A_n(a_1, \dots, a_{n-1}) \text{ type}[\Gamma]}{c(a_1, \dots, a_n) \in C(a_1, \dots, a_n) \text{ type}[\Gamma]} \quad (2.5)$$

$$\text{sub} - \text{eqter}) \quad \frac{c(x_1, \dots, x_n) = d(x_1, \dots, x_n) \in C(x_1, \dots, x_n) \text{ type}[\Gamma, x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})] \quad a_1 \in A_1 \text{ type}[\Gamma] \dots a_n \in A_n(a_1, \dots, a_{n-1}) \text{ type}[\Gamma]}{c(a_1, \dots, a_n) = d(a_1, \dots, a_n) \in C(a_1, \dots, a_n) \text{ type}[\Gamma]} \quad (2.6)$$

$$\text{sub} - \text{eq} - \text{ter}) \quad \frac{c(x_1, \dots, x_n) \in C(x_1, \dots, x_n) \text{ type}[\Gamma, x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})] \quad a_1 = b_1 \in A_1 \text{ type}[\Gamma] \dots a_n = b_n \in A_n(a_1, \dots, a_{n-1}) \text{ type}[\Gamma]}{c(a_1, \dots, a_n) = c(b_1, \dots, b_n) \in C(a_1, \dots, a_n) \text{ type}[\Gamma]} \quad (2.7)$$

$$\text{sub} - \text{eq} - \text{eqter}) \quad \frac{c(x_1, \dots, x_n) = d(x_1, \dots, x_n) \in C(x_1, \dots, x_n) \text{ type}[\Gamma, x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})] \quad a_1 = b_1 \in A_1 \text{ type}[\Gamma] \dots a_n = b_n \in A_n(a_1, \dots, a_{n-1}) \text{ type}[\Gamma]}{c(a_1, \dots, a_n) = d(b_1, \dots, b_n) \in C(a_1, \dots, a_n) \text{ type}[\Gamma]} \quad (2.8)$$

2.1.6 Regole proprie e derivabili

In una teoria formale ci sono due tipi di regole:

- **regole proprie del calcolo**, come lo sono le regole strutturali e quelle del singoletto;
- **regole derivabili**, come le regole di sostituzione, utili per abbreviare le derivazioni.

Una regola $r \frac{J_1, \dots, J_n}{J}$ è ammissibile in un calcolo t sse i giudizi derivabili in $t + r$ sono gli stessi dei giudizi derivabili in t . Ciò comporta che l'aggiunta di una regola r non cambia i giudizi che ne possono derivare.

Quando un assioma è ammissibile e derivabile questo coincide con un giudizio derivabile.

2.1.7 Nozione di contesto telescopico

Un giudizio, in teoria dei tipi dipendenti si esprime nella forma

$$A(x_1, \dots, x_n)[x_1 \in B_1, \dots, x_n \in B_n]$$

e prende il nome di **contesto telescopico**. Questi presenta una dipendenza continua, esemplificata nel seguente giudizio

$$A(x_1, x_2, x_3) \text{ type}[x \in C_1, x_2 \in C(x_1), x_3 \in C(x_1 x_2)..)$$

Inoltre si parla di contesti rigidi, ovvero senza possibilità di scambio. Come appare dall'esempio sotto.

$$[x \in Nat, y \in Nat, z \in Mat(x, y)] \text{ cont} \Rightarrow \text{è derivabile}$$

$$[y \in Nat, x \in Nat, z \in Mat(x, y)] \text{ cont} \Rightarrow \text{è derivabile}$$

$$[y \in Nat, z \in Mat(x, y), x \in Nat] \Rightarrow \text{non è un contesto.}$$

Perciù non esiste lo scambio arbitrario, si deve porre attenzione alle dipendenze delle assunzioni, che provoca una sostituzione rigida.

2.1.8 Esempi di applicazione

Attenzione all'ordine di sostituzione si deve partire sempre da quello con meno dipendenze.

$$\frac{c \in [C, \Gamma] \quad b \in [B(c), \Gamma] \quad A(x, y) \text{ type}[x \in C, y \in B(x)]}{A(c, b) \text{ type}[\Gamma]}$$

$$\frac{c \in [C, \Gamma] \quad b \in [B(c), \Gamma] \quad A(x, y) \text{ type}[x \in C, y \in B(x)]}{a(c, b) \in A(c, b) \text{ type}[\Gamma]}$$

Se si ha un tipo può venire usato il giudizio di uguaglianza tra termini e la sostituzione.

$$\frac{A(x) \text{ type}[\Gamma, x \in C] \quad c = e \in C[\Gamma]}{A(c) = A(e) \text{ type}[\Gamma]}$$

È dunque fondamentale il concetto di uguaglianza fra tipi. Se considero che ci sia un elemento

$$\frac{a(x) \in A(x) \text{ type}[\Gamma, x \in C] \quad c = e \in C[\Gamma]}{a(c) = a(e) \in A(c) \text{ type}[\Gamma]}$$

Per poter affermare che $A(e) = A(c)$ devo poterlo dedurre. Per farlo mi sono indispensabili le **regole di conversione dell'uguaglianza del tipaggio** (§2.1.9).

2.1.9 Regole di tipaggio

Regole di conversione

$$\frac{c \in C[\Gamma] \quad C = D \text{ type}[\Gamma]}{C \in D \text{ type}[\Gamma]}$$

Se due tipi sono uguali allora hanno gli stessi termini: $C = D \Rightarrow (c \in C \Leftrightarrow c \in D)$. L'uguaglianza fra tipi è per questo simmetrica.

Tuttavia non sempre l'unicità del tipaggio di un termine (il \Leftrightarrow) è garantito per ogni teoria. Nei casi trattati dal corso sì, in quanto verrà inteso che $C = D \text{ type}[\Gamma]$ sse due tipi hanno gli stessi elementi (come già accade in *set theory*), ma può non essere sempre vero.

Regole di conversione dell'uguaglianza

$$\frac{c = d \in C[\Gamma] \quad C = D \text{ type}[\Gamma]}{c = d \in D \text{ type}[\Gamma]}$$

Questa regola permette di convertire le uguaglianze nel tipaggio di un termine.

2.2 Il tipo singoletto

Il tipo singoletto risulta essere paradigmatico per gli altri tipi. Per definirlo impiegherò i giudizi nella forma $A \text{ type}[\Gamma]$, $a \in A \text{ type}[\Gamma]$ e $a = b \in A \text{ type}[\Gamma]$. L'uguaglianza, invece, non verrà coinvolta, in quanto non può essere impiegata per definire un nuovo tipo, è difatti usata solo nelle derivazioni.

Innanzitutto come già visto in §2.1.1 ogni derivazione parte sempre dal contesto vuoto (\emptyset).

$$\text{F-C)} \frac{A \text{ type}[\Gamma]}{\Gamma, x \in A} x \in A \notin \Gamma$$

2.2.1 Regola di formazione

$$\text{F-S)} \frac{[\Gamma] \text{ cont}}{N_1 \text{ type}[\Gamma] \text{ cont}}$$

La regola F-S Permette di derivare vari giudizi e di dire che cosa è un tipo.

Con l'impiego solo delle regole F-C e F-S si possono derivare $[x_1 \in N_1 \dots x_n \in N_1] \text{ cont}$ e ottenere, così, contesti di una lista arbitraria di variabili diverse appartenenti a N_1 , come si vede dall'esempio seguente.

$$\begin{array}{c} \text{F-C)} \frac{[\] \text{ cont}}{[x_1 \in N_1] \text{ cont}} \quad x_1 \in N_1 \notin \emptyset \\ \text{F-S)} \frac{[x_1 \in N_1] \text{ cont}}{N_1 \text{ type} [x_1 \in N_1]} \\ \text{F-C)} \frac{N_1 \text{ type} [x_1 \in N_1]}{[x_1 \in N_1, x_2 \in N_1] \text{ cont}} \quad x_2 \in N_1 \notin x_1 \in N_1 \end{array}$$

2.2.2 Regole di Introduzione

$$\text{I-S)} \frac{[\Gamma] \text{ cont}}{* \in N_1 \text{ type}[\Gamma] \text{ cont}}$$

Sia N_1 in ogni contesto Γ , partendo da contesto \emptyset , la regola I-S permette di formare i termini, per mezzo dell'introduzione di un elemento costante $*$ in N_1 .

Un esempio diretto della sua applicazione è

$$\text{I-S)} \frac{[] \text{ cont}}{* \in N_1 (x_1 \in N_1 \dots x_n \in N_1)}$$

2.2.3 Regole di Eliminazione

$$\text{E-S)} \frac{t \in N_1 \text{ type}[\Gamma] \quad M(z) \text{ type}[\Gamma, z \in N_1] \quad c \in M(*) \text{ type}[\Gamma]}{El_{N_1}(t, c) \in M(*) \text{ type}[\Gamma]}$$

El trattasi di costruttore di funzioni e $M[t] = M(z)[\frac{z}{t}]$.

La regola di eliminazione si può equivalentemente scrivere in un altro modo

$$\text{E-S)}_{dip} \frac{M(z) \text{ type}[\Gamma, z \in N_1] \quad c \in M(*) \text{ type}[\Gamma]}{El_{N_1}(z, c) \in M(z) \text{ type}[\Gamma, z \in N_1]}$$

Le regole E-S)_{dip} + la regole di sostituzione + F-S + I-S permettono di verificare la validità di E-S.

$$\text{sost)} \frac{t \in N_1 \text{ type}[\Gamma] \quad \text{E-S)}_{dip} \frac{M(z) \text{ type}[\Gamma, z \in N_1] \quad c \in M(*) \text{ type}[\Gamma]}{El_{N_1}(z, c) \in M(z) \text{ type}[\Gamma]}}{El_{N_1}(t, c) \in M(t) \text{ type}[\Gamma]}$$

Inoltre vale anche il viceversa, da E-S si riesce a ottenere E-S)_{dip} .

2.2.4 Regole di Conversione

$$\text{C-S)} \frac{M(z) \text{ type}[\Gamma, z \in N_1] \quad c \in M(*) \text{ type}[\Gamma]}{El_{N_1}(*, c) = c \in M(*) \text{ type}[\Gamma]}$$

La conversione rende possibile l'applicazione della regola di eliminazione introducendo delle uguaglianze.

Le regole (S), (I-S), (E-S) e (C-S) hanno una spiegazione computazionale, e riguardano la compatibilità tra tipi, ma non da caratterizzare il tipo dei tipi. Inoltre il tipo singoletto non è dipendente.

2.2.5 Osservazioni sul tipo singoletto

L'eliminatore $\text{El}_{N_1}(z, c)$ rappresenta una funzione definita per ricorsione su N_1 , difatti in $C\text{-}S$ si ha che $\text{El}_{N_1}(z, c)[\frac{z}{*}] = \text{El}_{N_1}(*, c)$.

Supposto che se $* \in N_1[\Gamma]$ in $E\text{-}S$, allora per la singola conversione vale che $\text{El}_{N_1} = c \in M(*)$. Dunque $\text{El}_{N_1}(z, c)$ rappresenta un programma funzionale per ricorsione. Questi è definito su N_1 , a partire da $c \in M(*)$, perciò $\text{El}_{N_1}(*, c) = c$.

La regola di eliminazione permette di definire un programma funzionale da N_1 a $M(z)$ esclusivamente con $c \in M(*)$, ovvero definendo $*$ come **elemento canonico**.

In

$$\frac{t \in N_1[\Gamma]}{t = * \in N_1[\Gamma]}$$

risulta vera l'uguaglianza definizionale?

No, non è vera. La regola di eliminazione consente di dare un valore al termine canonico, permettendo così di attribuire un valore a tutti i possibili termini del singoletto. Ma in generale questo non vale all'interno della teoria. Difatti l'uguaglianza definizionale è diversa da quella matematica e va intesa come computazionale e non proposizionale (come definito in §1.7.2).

2.3 Sanitary checks rules

Le *Sanitary checks* sono regole strutturali utili per abbreviare le derivazioni. Queste sono derivabili solo se la teoria dei tipi è corretta.

Assunto T , come una teoria dei tipi di riferimento, le *sanitary checks* sono le seguenti:

$$\frac{[\Gamma, \Delta] \text{ cont}}{\Gamma \text{ cont}}$$

Se $[\Gamma, \Delta] \text{ cont}$ è derivabile in T allora anche $[\Gamma] \text{ cont}$ è derivabile in T .

$$\frac{J_1, \dots, J_n}{J}$$

Se J_i con $i = 1, \dots, n$ in T sono derivabili allora anche J è derivabile in T .

$$\frac{A \text{ type } [\Gamma]}{\Gamma \text{ cont}}$$

Se $A \text{ type } [\Gamma]$ è derivabile in T allora anche $\Gamma \text{ cont}$ è derivabile in T .

$$\frac{A = B \text{ type } [\Gamma]}{A \text{ type } [\Gamma]} \quad \frac{A = B \text{ type } [\Gamma]}{B \text{ type } [\Gamma]}$$

Se $A = B \text{ type } [\Gamma]$ è derivabile in T allora anche $A \text{ type } [\Gamma]$ e $B \text{ type } [\Gamma]$ sono derivabili in T .

$$\frac{a \in A \text{ type } [\Gamma]}{A \text{ type}[\Gamma]}$$

Se $a \in A \text{ type } [\Gamma]$ è derivabile in T allora anche $A \text{ type}[\Gamma]$ è derivabile in T .

$$\frac{a = b \in A \text{ type } [\Gamma]}{a \in A \text{ type}[\Gamma]} \quad \frac{a = b \in A \text{ type } [\Gamma]}{b \in A \text{ type}[\Gamma]}$$

Se $a = b \in A \text{ type } [\Gamma]$ è derivabile in T allora anche $a \in A \text{ type}[\Gamma]$ e $b \in A \text{ type}[\Gamma]$ sono derivabili in T .

2.4 Esercizi

Dimostrare che da $E-S$ si riesce a ottenere $E-S_{dip}$ usando le derivazioni.

Dimostrare che la regola $E-S$ è derivabile in una teoria dei tipi T_1 , rimpiazzando la regola di eliminazione $E-S$ con la regola $E-N_{1prog}$, con aggiunta delle regole di indebolimento, sostituzione e di *sanitary checks*.

$$E-N_{1prog}) \frac{M(w) \text{ type } [\Gamma, w \in N_1] \quad d \in D(*) \text{ type}[\Gamma]}{EL_{N1}(w, d) \in M(w) \text{ type}[\Gamma, w \in N_1]}$$

$$E-S) \frac{t' \in N_1 \text{ type}[\Sigma] \quad M(w) \text{ type } [\Gamma, w \in N_1] \quad d' \in M(*) \text{ type}[\Sigma]}{El_{N1}(t', d') \in M(t') \text{ type}[\Gamma]}$$

Svolgimento

Capitolo 3

Naturali, Somma disgiunta e liste

Capitolo 4

Uguaglianza proposizionale

Capitolo 5

Somma indicata forte e prodotto cartesiano

Capitolo 6

Tipo delle funzioni e tipo prodotto dipendente

Capitolo 7

La logica della teoria dei tipi di *Martin-Löf*

Appendice A

Tabelle