INTRODUZIONE ALLA TEORIA COSTRUTTIVA DEGLI INSIEMI

LAURA CROSILLA

Appunti per le lezioni tenute in occasione del seminario
Logica e Informazione
Seconda Parte
Prof. A. Cantini, Prof. P. Minari
Università degli Studi di Firenze
Dipartimento di Filosofia
A.A. 2003 - 04, Secondo semestre[1]

[1]Questi appunti sono editi in LaTeX 2_ε

Indice

1. Introduzione

1.1. **Prologo.** In questi appunti intendiamo esplorare la nozione di insieme da un punto di vista costruttivo cercando al contempo di restare il più vicino possibile alla tradizione classica, conservando di essa il linguaggio formale, le intuizioni di base e la terminologia.

È a tutti noto il concetto informale di insieme, ovvero di una collezione di oggetti in cui si astrae dalle particolari caratteristiche degli oggetti stessi, così come sono a tutti note le più semplici operazioni di manipoalzione su insiemi, quali l'intersezione, l'unione, la somma disgiunta etc.

Si vuole qui presentare una versione costruttiva, ovvero basata sulla logica intuizionistica e inoltre predicativa, di **ZF** (Zermelo Fraenkel), il più noto sistema formale introdotto allo scopo di caratterizzare ed esattamente comprendere la nozione classica di insieme.

Il concetto di insieme qui rappresentato ha forti connessioni con la nozione di insieme propria della teoria dei tipi di Martin Löf che è stata affrontata nel semestre scorso. Vedremo infatti che esiste una traduzione del tutto naturale della teoria costruttiva degli inisiemi in una particolare versione di teoria dei tipi.

Vi sono tuttavia anche notevoli differenze, che cercheremo di indicare e chiarire per quanto possibile.

Data la limitatezza di spazio, ci accontenteremo in questi appunti di introdurre e spiegare gli assiomi, mostrare qualche esempio di principio incompatibile con la logica intuizionistica, fornire i rudimenti della formalizzazione di familiari nozioni insiemistiche, per infine schizzare l'interpretazione di **CZF** nella teoria dei tipi di Martin Löf. Si spera in questo modo di convenire un'impressione del significato della teoria, del modo in cui in essa si opera ma anche di presentare un esempio di tecnica di interpretazione tra distinte teorie.

Si osservi che sebbene la familiarità con gli argomenti delle lezioni del primo semestre sia di supporto per quanto verrà qui esposto, le prime sezioni non richiedono di fatto la conoscenza della teoria dei tipi. Per le sezioni relative all'interpretazione della teoria costruttiva **CZF** nella teoria dei tipi, tali nozioni sono tuttavia necessarie. Sotto richiesta potrà essere offerta una sezione supplettiva di riepilogo delle principali idee della teoria dei tipi.

Nel corso dell'esposizione verranno proposti vari esercizi di difficoltà disparata. Indicheremo con $\star$ quelli ritenuti più complessi.

1.2. **Accenni storici.**

1.3. **La teoria classica degli insiemi.** Non vi è qui modo di presentare una panoramica seppure sommaria della nascita e dello sviluppo della teoria degli insiemi da G. Cantor ai nostri giorni. Un breve accenno si trova per esempio nell'introduzione al classico "Foundations of set theory" di A. Fraenkel and Y. Bar-Hillel [9].

Se si desidera consultare una trattazione formale della teoria classica degli insiemi, i testi di riferimento sono innumerevoli e di varia difficoltà. Tra i più recenti si consiglia il volume di Moschovakis [15]. Per lettori con una discreta familiarità con le nozioni di base della teoria classica degli insiemi e che intendano avvicinarsi a tematiche più avanzate o semplicemente coglierne il significato generale, si consigliano i classici Jech ([12]) e Kunen ([13]).

1.4. **La teoria costruttiva.** Interesse principale di queste note è come accennato una versione costruttiva della teoria **ZF**.

Sebbene la pratica matematica, essendo essenzialmente informale, non faccia di fatto uso degli assiomi di **ZF** (o **ZFC**)[2], si ritiene in genere che **ZFC** (oppure una sua appropriata estensione) costituisca un sistema in cui tale pratica possa essere interamente espressa e formalmente rappresentata.

La teoria costruttiva degli insiemi, e in particolare il sistema **CZF**, fa propria questa idea e si propone come fondazione per la matematica *costruttiva.*

È tuttavia essenziale osservare che sistemi come **CZF** rappresentano un radicale mutamento di prospettiva rispetto a **ZF**: la logica di base non è più quella classica ma quella intuizionistica. Viene dunque bandito il principio del terzo escluso che consente di effettuare argomentazioni per assurdo e viene conseguentemente richiesto che ogni asserzione di esistenza sia corroborata dal poter (almeno in linea di principio) produrre un oggetto che soddisfa tale asserzione (un witness). Vedremo che questo cambiamento di prospettiva ha un forte impatto su quanto può essere di fatto dimostrato sulla base di tali sistemi.

1.5. **Alcuni punti di riferimento.** Ripercorriamo ora i fondamentali eventi nello sviluppo della teoria **CZF**. Ci aiuteremo con il ricordare alcuni testi e articoli che ne sono alle origini.[3]

(*i*) E. Bishop: “Foundations of constructive analysis”, 1967 ([6]).

Con questo testo Bishop dà vita ad una nuova era per la matematica basata sulla logica intuizionistica. Invece di accentuarne i limiti rispetto alla matematica classica, indicando quanto di essa *non* si possa dimostrare sulla base della logica intuizionistica, e piuttosto che accogliere come principi fondamentali delle asserzioni in palese contraddizione con la tradizione classica (giustificate da una diversa ontologia delle entità matematiche), Bishop, con spirito pragmatico, propone una matematica costruttiva del tutto compatibile con la logica classica e assai più simile ad essa di qualsiasi contributo fino ad allora apportato alla tradizione intuizionistica.

Si ricordi inoltre che la necessità di garantire un valore computazionale ai risultati matematici è una costante del suo pensiero, ed è sufficiente a giustificare il passaggio alla logica intuizionistica, indipendentemente da specifiche e più profonde posizioni filosofiche relative all'essenza delle entità matematiche.

[2]**ZFC** indica la teoria **ZF** più Assioma di scelta, **AC**.

[3]Si veda anche l'introduzione alle dispense del primo semestre.

Presto sorge una *Bishop school*, cui principale rappresentante è tuttora D. Bridges, e che fa proprio lo spirito pragmatico e l'urgenza di sviluppare in vena costruttiva porzioni sempre più ampie e sofisticate della matematica.

(*ii*) J. Myhill: "Constructive set theory", 1975 ([16]).

Il testo di Bishop stimola un nuovo fermento tra i logici che si propongno di individuare sistemi formali che enucleino le nozioni di fatto utilizzate da Bishop ma dall'autore non del tutto esplicitate.

Ci si interroga prima di tutto su quali siano gli strumenti necessari per esprimere la matematica costruttiva di recente nascita, e in alcuni casi si cerca inoltre di limitare i principi utilizzati nella formalizzazione alle sole nozioni sufficienti.

Tra i vari tentativi, degno di menzione è quello di Myhill e Goodman di formalizzazione della matematica costruttiva in sistemi tipati quali Gödel's T. Gli autori pervengono presto alla convinzione che la formalizzazione risultante sia troppo faticosa e artificiale.[4]

Vi sono inoltre numerosi esperimenti da parte di Myhill e Friedman volti a produrre versioni intuizionistiche degli assiomi di **ZF**. Il sistema più noto è **IZF** che risulta essere impredicativo ed estremamente forte da un punto di vista di teoria della dimostrazione.[5]

Myhill [16] propone un formalismo che si avvicini il più possibile alla teoria informale degli insiemi utilizzata da Bishop nella sua opera di elaborazione dell'analisi costruttiva.[6] Per esempio il sistema ha una nozione primitiva di funzione ed evita l'uso di Powerset e di Separazione piena, risultando quindi predicativo[7].

(*iii*) P. Aczel: "The type theoretic interpretation of constructive set theory", 1978 ([1], si vedano anche [2], [3] e [4]).

Aczel riprende il sistema di Myhill e lo modifica formulandolo in un linguaggio puramente insiemistico così da ottenere una teoria del tutto compatibile con **ZF** (per esempio una funzione è ora un insieme di coppie ordinate). Il sistema risultante viene battezzato **CZF**, Constructive Zermelo Fraenkel, a ragione della sua somiglianza con **ZF**.

---

[4]Si veda l'introduzione a Myhill [16]. La lettura di tale articolo è vivamente consigliata.

[5]**IZF** risulta della stessa forza di **ZF**, come dimostrato da Friedman per mezzo di un'interpretazione via doppia negazione. Si noti, tuttavia, che Friedman propone anche sistemi essenzialmente deboli, persino sistemi della forza dell'aritmetica di Peano.

[6]Si veda per esempio il capitolo 3 in Bishop e Bridges [7].

[7]Ad oggi sono state presentate varie nozioni di predicatività. Alcuni autori, soprattutto S. Feferman e K. Schütte hanno indicato nell'ordinale Γ_0 una sorta di limite invalicabile per la predicatività di una teoria. Ovvero una teoria è predicativa qualora possiamo attribuirle l'ordinale proof teoretico Γ_0. Tale scelta ha radici nelle tecniche utilizzate nell'assegnazione dell'ordinale stesso. Altri autori, tra cui Myhill, Aczel, e ultimamente anche Martin Löf, hanno abbracciato invece un cosiddetto predicativismo liberale, che classifica come predicative anche teorie in cui si possano esprimere definizioni induttive. Da un punto di vista dell'analisi ordinale, tali teorie richiedono, tuttavia, tecniche più raffinate e sono caratterizzate da ordinali maggiori di Γ_0.

L'autore fornisce al contempo un'interpretazione di **CZF** nella teoria dei tipi di Martin Löf, che si rende necessaria, come vedremo in seguito, allo scopo di garantire un genuino significato alla nozione di insieme così formalizzata. Egli rafforza infine due principi, collezione ed esponenziazione, a seguito dell'osservazione che le versioni così ottenute sono valide nell'interpretazione nella teoria dei tipi.

1.6. **Un confronto (I).** Volendo grossolanamente comparare la teoria costruttiva degli insiemi con la teoria classica, si osserva prima di tutto che la prima si evidenzia per la varietà di interpretazioni o modelli. Caratteristico inoltre il suo consentire lo studio di concetti familiari della tradizione classica in modo estremamente sottile. In genere, infatti, ad un concetto classico corrispondono in ambito costruttivo numerosi concetti distinti. Ponendoci nella prospettiva costruttiva otteniamo dunque una visione più profonda e chiara del significato di quelle che classicamente ci appaiono semplicemente come leggere sfumature, del tutto incapaci di modificare in essenza il concetto stabilito.

D'altro canto, abbracciando un approccio costruttivo dobbiamo di necessità rinunciare a tanti dei risultati della matematica classica, alcuni dei quali tra i più noti e familiari. Questa sembra essere la fonte della gran parte dei pregiudizi che accompagnano costantemente la diffusione dell'impresa costruttiva.

Si deve tuttavia osservare che le teorie costruttive vantano un chiaro contenuto computazionale per i loro enunciati, e questo è a nostro giudizio un fondamentale argomento a loro favore, anche qualora non si intenda prendere una posizione specifica di carattere più propriamente filosofico relativamente allo stato di esistenza delle entità matematiche. Riteniamo che se si intende lavorare all'interno di una matematica di rilevanza computazionale, non è di fatto realistico attenersi alla matematica classica il cui sviluppo e processo storico è stato motivato da ben altri stimoli creativi. La pratica computazionale ci appare anzi assai più restrittiva di qualsiasi interpretazione costruttiva, limitando le nostre computazioni e asserzioni con vincoli sia di carattere temporale che spaziale e fisico.

1.7. **Un confronto (II).** Nei primi anni settanta vengono introdotti altri sistemi formali che si propongono come fondazione per la matematica costruttiva alla Bishop, per esempio:

- la *matematica esplicita* di S. Feferman,
- la *teoria costruttiva dei tipi* di P. Martin Löf,
- e la *teoria intuizionistica degli insiemi* di H. Friedman e J. Myhill.

Rispetto alla teoria dei tipi o alla matematica esplicita, **CZF** offre al logico di formazione classica, abituato a lavorare in teoria degli insiemi, un ambito di lavoro più confortevole[8]. Rispetto ad altri sistemi alla Zermelo Fraenkel, sia quelli più forti, come per esempio **IZF**, che quelli più deboli, come la versione intuizionistica della teoria **KP** (Kripke Platek), **CZF** presenta un chiaro vantaggio per il suo combinare una notevole capacità espressiva matematica con una limitata forza proof teoretica. Essa risponde dunque ad una richiesta di parsimonia dei principi che le altre teorie non condividono.

Avendo di fronte un pluralità di possibili formalismi, e per ciascuno di essi una varietà di sistemi distinti, ci si può interrogare su quali criteri possano aiutarci a sceglierne uno in cui operare e su cui concentrare le nostre ricerche. Oppure, come più facilmente si opera di fatto, trovandoci a lavorare per motivi diversi entro un sistema particolare ci si può chiedere se esso sia di fatto adatto agli scopi che ci si era prefissati. Naturalmente svariati sono i criteri che consentono di stabilire se un sistema è un "buon" sistema formale costruttivo. I seguenti sono a nostro avviso di particolare rilevanza:

(i) costruttività della nozione di insieme risultante,
(ii) adeguatezza nel rappresentare la matematica costruttiva,
(iii) semplicità della formalizzazione,
(iv) predicatività.

Si può inoltre richiedere (o meno) la compatibilità con la tradizione classica.

La teoria **CZF** soddisfa tutti questi requisiti, sebbene il primo solo in modo indiretto. Le teorie costruttive degli insiemi possono infatti essere viste come il risultato della seguente procedura:

(a) Si consideri la teoria classica **ZF** e si sostituisca la logica classica del primo ordine con il suo sottosistema intuizionistico.
(b) Si osservi che alcuni assiomi (per es. fondazione) producono, sulla base della logica intuizionistica e di altri principi di **ZF**, istanze del principio del terzo escluso. Li si rimpiazzi dunque con schemi ad essi classicamente equivalenti ma che risultino "innocui" da un punto di vista costruttivo.
(c) Si limitino in modo essenziale quei principi che possono produrre forme di impredicatività (quali lo schema di separazione piena, e l'assioma dell'insieme potenza).[9]

Seguendo questa procedura si perde di fatto il senso della costruttività della nozione di insieme caratterizzata dagli assiomi. Per questo Aczel ha ritenuto necessario presentare la teoria **CZF** congiuntamente alla sua interpretazione nella teoria dei tipi di Martin Löf, quest'ultima essendo ritenuta

[8]Si osservi tuttavia che sempre più ampio è il numero di logici che non provengono dalla tradizione classica di teoria degli insiemi, e che trovano quindi più agevole la teoria dei tipi.

[9]Si osservi che in questo modo si può pervenire ad una pluralità di sistemi. Come osservato **CZF** aggiunge al vantaggio di soddisfare tutti i criteri appena elencati anche una limitata forza proof teoretica.

dall'autore genuinamente costruttiva. La costruttività della nozione di insieme risulta dunque indiretta, mutata dalla costruttività della stessa nozione nella teoria dei tipi.

2. Il sistema **CZF**

Giungiamo ora alla presentazione delle caratteristiche formali di **CZF**. Introdurremo prima di tutto il linguaggio della teoria, e successivamente gli assiomi e schemi.

Importante rilevare che contrariamente alla teoria dei tipi, in cui la logica predicativa del primo ordine sorge come conseguenza degli assiomi attraverso la corrispondenza Curry-Howard, la teoria degli insiemi si basa su una formalizzazione standard della logica, di cui accoglie assiomi e regole, per poi imporre su di essa ulteriori principi che caratterizzano la nozione di insieme.

2.1. **Il linguaggio.** Il linguaggio di **CZF**, qui indicato con LST, è ottenuto dall'usuale linguaggio del calcolo dei predicati intuizionistico con uguaglianza (quindi con simboli primitivi $\bot$, $\wedge$, $\vee$, $\rightarrow$, $\exists$, $\forall$ ed $=$) aggiungendo un predicato binario $\in$ (rappresentante la relazione di appartenenza).

Come al solito scriviamo $\neg\varphi$ in luogo di $\varphi \rightarrow \bot$ e $\varphi \leftrightarrow \psi$ come abbreviazione di $\varphi \rightarrow \psi \wedge \psi \rightarrow \varphi$.

Per comodità considereremo come primitivi i quantificatori limitati, ossia della forma $\exists x \in y$ e $\forall x \in y$.

Una formula di LST è detta essere Δ_0 o *limitata* se e solo se tutti i quantificatori che occorrono in essa sono limitati.

2.2. **Insiemi e classi.** Nella teoria classica degli insiemi è prassi distinguere tra insiemi e classi. Anche in **CZF** possiamo condividere questa abitudine di riferirci a classi. Queste non fanno di fatto parte dell'ontologia della teoria degli insiemi, ma forniscono un comodo strumento per riferirsi all'estensione di una formula arbitraria come ad una collezione di oggetti che soddisfano tale formula.

Useremo la notazione $\{x : \varphi(x)\}$ anche per classi e designeremo le lettere maiuscole dell'alfabeto per indicarle. Ogni riferimento a classi può essere tuttavia eliminato. Per esempio, se $A = \{x : \varphi(x)\}$, $y \in A$ è da considerarsi meramente come un'informale notazione per $\varphi(y)$.

2.3. **Gli assiomi.** Prima di tutto riportiamo di seguito gli assiomi per poi darne una breve informale descrizione.

(1) Assiomi e regole della **logica intuizionistica del primo ordine** con uguaglianza
(2) **Estensionalità**

$$\forall y\, (y \in a \leftrightarrow y \in b) \rightarrow a = b$$

(3) **Coppia**

$$\exists x\, \forall y\, (y \in x \leftrightarrow y = a \vee y = b)$$

(4) **Unione**

$$\exists x \, \forall y \, (y \in x \leftrightarrow \exists z \in a \, y \in z)$$

(5) **Schema di Δ_0 - Separazione**
Per ogni Δ_0 formula $\varphi(y)$,

$$\exists x \, \forall y \, (y \in x \leftrightarrow y \in a \wedge \varphi(y))$$

(6) **Schema di sottocollezione**
Per ogni formula $\varphi(x, y, u)$,

$$\exists c \, \forall u \, \big(\forall x \in a \, \exists y \in b \, \varphi(x, y, u) \\ \rightarrow \exists d \in c \, (\forall x \in a \, \exists y \in d \, \varphi(x, y, u) \wedge \forall y \in d \, \exists x \in a \, \varphi(x, y, u))\big)$$

(7) **Schema di collezione forte**
Per ogni formula $\varphi(x, y)$,

$$\forall x \in a \, \exists y \, \varphi(x, y) \\ \rightarrow \exists b \, (\forall x \in a \, \exists y \in b \, \varphi(x, y) \wedge \forall y \in b \, \exists x \in a \, \varphi(x, y))$$

(8) **Assioma dell'infinito**

$$\exists x \, \big(0 \in x \wedge \forall y \, (y \in x \rightarrow suc(y) \in x)\big)$$

con $suc(y) = y \cup \{y\}$ e $0 = \emptyset$, definito nel modo usuale

(9) **Schema di $\in$ - Induzione**
Per ogni formula $\varphi(a)$,

$$\forall a \, (\forall y \in a \, \varphi(y) \rightarrow \varphi(a)) \rightarrow \forall a \, \varphi(a).$$

Osserviamo anzitutto che i primi 3 assiomi e l'assioma dell'infinito sono esattamente gli stessi assiomi che si trovano in presentazioni standard della classica **ZF**.

Come di prassi possiamo distinguere principi che consentono di formare insiemi a partire da insiemi dati (coppia etc.), assiomi asserenti l'esistenza di un nuovo insieme (infinito), assiomi che relazionano tra di loro gli insiemi (estensionalità) e schemi che consentono di dimostrare proprietà di insiemi ($\in$ - induzione).

(1) Con l'assioma di *estensionalità* prescindiamo dalle modalità di formazione degli insiemi, in quanto identifichiamo tutti gli insiemi che contengono gli stessi elementi.
(2) L'assioma di *coppia* consente, dati due insiemi qualsiasi a e b, di formare un nuovo insieme che contiene esattamente a e b. Esso è unico per estensionalità, così che lo indicheremo con $\{a, b\}$.
(3) L'assioma di *unione* ci permette di raccogliere in un nuovo insieme gli elementi di ciascun elemento di un insieme dato, a. Anch'esso è unico per estensionalità e verrà indicato con $\bigcup a$.
(4) Dato un insieme a l'assioma di Δ_0-*separazione* permette di selezionare un suo sottoinsieme costituito esattamente dagli elementi di a che soddisfano una certa Δ_0 formula φ. Lo indichiamo con $\{x \in a : \varphi(x)\}$.

Si osservi la restrizione a formule di tipo Δ_0, che aderisce ad una richiesta di predicatività. Si vuole infatti limitare la quantificazione ai soli insiemi precedentemente formati, così evitando definizioni impredicative.

Come prima applicazione dell'assioma di separazione (e di estensionalità), definiamo l'insieme vuoto come $\{x \in a : \neg x = x\}$ con a un qualsiasi insieme.[10]

(5) Lo *schema di sottocollezione* è di difficile lettura e comprensione. Per comodità possiamo pensarlo come un rafforzamento di un assioma noto con il nome di esponenziazione di Myhill. Quest'ultimo stabilisce che dati due insiemi a e b la classe di tutte le funzioni da a a b costituisce un insieme.

Esponenziazione

$$\exists x \forall f\, (f \in x \leftrightarrow (fun(f) \wedge dom(f) = a \wedge ran(f) \subseteq b)).$$

Con fun, dom e ran indichiamo formule che esprimono le nozioni di funzione, dominio e codominio. Vedremo in seguito come possono essere espresse in **CZF**.

Si osservi che lo schema di sottocollezione prende il posto in **CZF** dell'assioma dell'insieme potenza che caratterizza **ZF**. L'assioma dell'insieme potenza consente di formare l'insieme di tutti i sottoinsiemi di un insieme dato. Postulare l'esistenza di un tale insieme dà luogo a impredicatività e sembra in contrasto con una nozione costruttiva di insieme. Non è infatti per nulla chiaro come formare l'insieme potenza persino di una collezione così fondamentale come l'insieme dei naturali.

È importante sottolineare che classicamente assioma dell'insieme potenza, sottocollezione ed esponenziazione sono equivalenti. In contesti costruttivi, tuttavia, l'assioma dell'insieme potenza è decisamente più forte degli altri due principi.

(6) Lo schema di *collezione forte* è un rafforzamento naturale del principio di collezione che troviamo in genere nelle presentazioni della teoria classica degli insiemi.[11] Siano dati un insieme a, una proprietà φ e supponiamo che per ogni elemento x di a si possa produrre un insieme y tale che $\varphi(x, y)$ valga. Lo schema di collezione consente

[10] L'esistenza di almeno un insieme è giustificata in teorie degli insiemi per la validità del principio logico $\exists x\, x = x$.

[11] Si osservi che spesso la teoria classica degli insiemi è formulata con lo schema di rimpiazzamento in luogo di quello di collezione. Tipicamente l'antecedente del rimpiazzamento richiede sia soddisfatta un'ulteriore condizione di unicità e asserisce essenzialmente che il codominio di una funzione con dominio un insieme è anch'esso un insieme. Collezione e rimpiazzamento sono dimostrabilmente equivalenti in teorie classiche con assioma di fondazione. Non lo sono però in genere sulla base di teorie costruttive o sfondate.

Si noti infine che il principio di rimpiazzamento (o collezione) non era presente nella formulazione originaria della teoria degli insiemi dovuta a Zermelo, e la sua introduzione si deve a Fraenkel.

di formare un nuovo insieme b che raccoglie tali y. Collezione forte assicura addizionalmente che per ogni $x \in a$ vi sia un $y \in b$ tale che $\varphi(x, y)$ ed anche il viceversa, ovvero che per ogni $y \in b$ esista un $x \in a$ per cui $\varphi(x, y)$.

(7) L'assioma dell'*infinito* è necessario per assicurare che la teoria non tratti meramente oggetti finiti. Con questo principio asseriamo l'esistenza di un insieme infinito. La forma qui scelta asserisce di fatto che esiste un insieme che raccoglie i numeri naturali, ovvero un insieme che contiene lo 0 (l'insieme vuoto) e che è chiuso rispetto all'operazione di successore. Utilizzando lo schema di $\in$ - induzione ed estensionalità si può dimostrare che esiste il più piccolo insieme che soddisfa questa proprietà, che chiameremo ω (o insieme dei numeri naturali).

(8) Lo schema di $\in$ - *induzione* consente di ragionare per induzione sulla relazione di appartenenza. Con esso asseriamo che dato un insieme arbitrario a, se una proprietà φ si trasmette da elementi di a ad a stesso, allora la proprietà vale di ogni insieme.

Si osservi che classicamente $\in$ - *induzione* è equivalente all'assioma di fondazione, asserente che ogni insieme abitato ha un elemento minimo rispetto alla relazione di appartenenza. Intuizionisticamente, tuttavia, lo schema di induzione non è equivalente alla fondazione; quest'ultima implica infatti in combinazione con altri assiomi di **CZF** il principio del terzo escluso per Δ_0 formule (**REM**, Restriced Excluded Middle).

Vediamo ora in dettaglio l'argomento. Nel seguito scriviamo $x \notin y$ per $\neg\, x \in y$.

Proposizione 2.1. **CZF** + *Assioma di fondazione* $\Longrightarrow$ **REM**.

Dimostrazione. Sia ψ una qualsiasi Δ_0 formula e si assuma l'assioma di fondazione. Vogliamo dimostrare che $\psi \vee \neg\psi$ vale, così che data la scelta arbitraria di ψ si ottenga **REM**.

Formiamo dunque l'insieme

$$a = \{x \in \omega : x = 1 \vee (x = 0 \wedge \psi)\}.$$

Utilizzando fondazione si ottiene un elemento x di a tale che $\forall z \in x\, z \notin a$. Essendo $x \in a$ si ha chiaramente $x = 1 \vee (x = 0 \wedge \psi)$. Se $x = 1$ allora per la minimalità di x, $0 \notin a$, per cui $\neg\psi$, mentre se $x = 0 \wedge \psi$ allora ψ.

In entrambi i casi otteniamo dunque $\psi \vee \neg\psi$. □

Concludiamo questa sezione con una Proposizione fondamentale. Di seguito **EM** indica il principio del terzo escluso (per formule arbitrarie).

Proposizione 2.2. *(Aczel)* **CZF** + **EM** = **ZF**.

Dimostrazione. Esercizio. □

Esercizio 2.3. *(1) Sia dato il seguente schema di comprensione:*

$$\exists x\, \forall y\, (y \in x \leftrightarrow \varphi(y)),$$

con φ formula Δ_0. Si derivi l'esistenza di un insieme r tale che $r \in r \leftrightarrow r \notin r$ (Paradosso di Russell).

(2) *Si verifichi (usando $\in$ - induzione) che per ogni insieme a, $a \notin a$.*
(3) *Si verifichi: $\neg \exists a \, \forall y \, (y \in a)$.*
(4) * *Si verifichi Proposizione 2.2.*

3. Conseguenze degli assiomi: esempi di formalizzazione

Vediamo ora di derivare semplici conseguenze dagli assiomi di **CZF**. Vogliamo formare le usuali unione e intersezione di due insiemi, definire le nozioni di coppia ordinata e prodotto cartesiano. Possiamo poi con questi ultimi introdurre i concetti di relazione, funzione, dominio, codominio.

Elencheremo inoltre alcune proprietà dei numeri naturali, che evidenziano che il loro comportamento è del tutto analogo a quello che si ha nella teoria classica degli insiemi.

Nel caso dei numeri reali e degli ordinali, ci attendono invece delle sorprese rispetto alla tradizione classica.

3.1. **Rimpiazzamento.** Prima di tutto osserviamo che lo schema di collezione forte implica sia lo schema di collezione che quello di rimpiazzamento (Esercizio). Questi sono i seguenti schemi, per formule arbitrarie $\varphi(x, y)$:

Collezione

$$\forall x \in a \, \exists y \, \varphi(x, y) \;\rightarrow\; \exists b \, \forall x \in a \, \exists y \in b \, \varphi(x, y)$$

Rimpiazzamento

$$\forall x \in a \, \exists! y \, \varphi(x, y) \;\rightarrow\; \exists b \, \forall y \, (y \in b \leftrightarrow \exists x \in a \, \varphi(x, y))$$

Poichè non possiamo assumere nel nostro contesto che questi siano equivalenti a collezione forte e tra loro, è importante sottolineare ogni volta quale assioma sia sufficiente.

Esercizio 3.1. (1) *Si dimostri che lo schema di collezione forte implica il rimpiazzamento.*

3.2. **I: Unione e intersezione binarie, coppia ordinata, prodotto cartesiano.** Di seguito a e b indicano insiemi.

(i) Unione binaria: Vogliamo poter formare l'insieme

$$a \cup b := \{x : x \in a \vee x \in b\}$$

Osserviamo che utilizzando gli assiomi di coppia e di unione, $\bigcup\{a, b\}$ è un insieme e soddisfa la definizione di unione binaria. Utilizzando l'assioma di estensionalità, l'unione binaria risulta univocamente caratterizzata, così da giustificare la notazione $a \cup b$.

(ii) Intersezione binaria: desideriamo mostrare che la classe

$$a \cap b := \{x : x \in a \wedge x \in b\}$$

è un insieme. Possiamo così definirla: $a \cap b = \{x \in a : x \in b\}$ ed osservare che è un insieme per Δ_0 - separazione.

(iii) L'usuale definizione (Kuratowski-Mostowski) di coppia ordinata può chiaramente essere utilizzata anche in teorie costruttive. Definiamo $\langle a, b\rangle := \{\{a\}, \{a, b\}\}$, con $\{a\} := \{a, a\}$. È un utile esercizio dimostrare che questa nozione di coppia ordinata è ben definita, ovvero che: $\langle a, b\rangle = \langle c, d\rangle \leftrightarrow a = c \wedge b = d$.

(iv) Si intende ora formare un insieme prodotto cartesiano di due insiemi a e b:

$$a \times b := \{\langle x, y\rangle : x \in a \wedge y \in b\}$$

Osserviamo dunque che per un qualsiasi insieme y, $\forall x \in a\, \exists! z\, (z = \langle x, y\rangle)$. Usando rimpiazzamento possiamo quindi formare un insieme $c_y = \{z : \exists x \in a\, (z = \langle x, y\rangle)\}$. Notiamo dunque che $\forall y \in b\, \exists! c_y\, (c_y = \{z : \exists x \in a\, (z = \langle x, y\rangle)\})$. Usando nuovamente rimpiazzamento otteniamo un insieme $c = \{c_y : y \in b\}$. Utilizzando unione formiamo infine l'insieme $\bigcup c$ che rappresenta chiaramente il prodotto cartesiano di a per b ed è unico per estensionalità.

Esercizio 3.2. *(1) Si verifichi:* $(a \cup b) \cup c = a \cup (b \cup c)$.

(2) Si verifichi: $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$.

(3) Si dimostri che la nozione di coppia ordinata di Kuratowski Moskowski è adeguata, ovvero per insiemi a, b, c, d*:*

$$\langle a, b\rangle = \langle c, d\rangle \rightarrow a = c \wedge b = d.$$

(4) Si definisca $(a, b) := \{\{a, 0\}, \{y, \{0\}\}$. *Si dimostri l'adeguatezza di questa seconda nozione di coppia ordinata.*

3.3. **II: Relazione, funzione, dominio, codominio.** In teoria degli insiemi le nozioni di relazione e funzione vengono rappresentate mediante l'insieme delle coppie ordinate che soddisfano la relazione e, rispettivamente, le coppie ordinate di argomenti e valori della funzione.

Come al solito usiamo la notazione $a \subseteq b$ per $\forall x \in a\, (x \in b)$.

(i) Una relazione è semplicemente rappresentata da un insieme di coppie ordinate.[12] Dati due insiemi a e b, una relazione tra di essi costituisce dunque un sottoinsieme del prodotto cartesiano di a per b. Scriviamo:

$$rel(r) := \forall a \in r\, (a \text{ “è una coppia ordinata”})$$

dove a “è una coppia ordinata” può essere così espressa:

$$\exists c \in a\, \exists d \in a\, \exists x \in d\, \exists y \in d\, (c = \{x\} \wedge d = \{x, y\} \wedge a = \{c, d\})$$

con $w = \{u, v\}$ la formula:

$$u \in w \wedge v \in w \wedge \forall z \in w\, (z = u \vee z = v)$$

Si osservi che la nozione di relazione è Δ_0.

[12] Si osservi che dobbiamo assicurarci che ciascuna specifica collezione di coppie ordinate davvero costituisca un insieme per poter parlare di relazione, e allo scopo dobbiamo utilizzare solo gli assiomi propri di **CZF**.

(ii) Il dominio di una relazione r è così definito:

$$dom(r) := \{x : \exists y \, \langle x, y\rangle \in r\}.$$

Il dominio costituisce un insieme grazie agli assiomi di Δ_0 - separazione e unione, poichè

$$dom(r) = \{x \in c : \exists y \in c \, (\langle x, y\rangle \in r)\},$$

con $c = \bigcup\bigcup r$.

(iii) Il codominio (ovvero range) di r è così definito:

$$ran(r) := \{y : \exists x \, \langle x, y\rangle \in r\}.$$

Anche il codominio di una relazione è un insieme, infatti

$$ran(r) = \{y \in c : \exists x \in c \, (\langle x, y\rangle \in r)\},$$

con $c = \bigcup\bigcup r$.

(iv) Una funzione è rappresentata da una relazione che soddisfa un'ulteriore condizione di unicità per cui ad ogni x corrisponde esattamente un y tali che $\langle x, y\rangle \in f$. Ovvero

$$fun(f) := rel(f) \wedge \forall x \in dom(f) \, \exists! y \in ran(f) \, (\langle x, y\rangle \in f).$$

Useremo la notazione $f : a \to b$ per indicare una funzione f da a a b, ovvero $fun(f) \wedge dom(f) = a \wedge ran(f) \subseteq b$. Con $f(x)$ indichiamo l'unico y tale che $\langle x, y\rangle \in f$.

Esercizio 3.3. *(1) Dimostrare che se $\forall x \in a \, \exists! y \, \varphi(x, y)$ allora esiste un'unica funzione f con $dom(f) = a$ e tale che $\forall x \in a \, \varphi(x, f(x))$. [Suggerimento: si osservi che $\forall x \in a \, \exists! z \, \psi(x, z)$, con $\psi(x, z)$ la formula $\exists y \, (z = \langle x, y\rangle \wedge \varphi(x, y))$.]*

(2) * Sia dato il seguente schema (Union-Replacement):

$$\forall x \in a \, \exists b \, \forall y \, (y \in b \leftrightarrow \varphi(x, y)) \to \exists c \, \forall y \, (y \in c \leftrightarrow \exists x \in a \, \varphi(x, y)).$$

Si dimostri che Union-Replacement è equivalente (sulla base di **CZF** *meno unione e collezione forte) alla combinazione dell'assioma di unione e dello schema di rimpiazzamento.*

3.4. **III: I numeri naturali.** I numeri naturali sono rappresentati dagli elementi dell'insieme ω postulato dall'assioma dell'infinito. Usiamo le lettere $n, m, k, \ldots$ per indicare i numeri naturali.

Definiamo una relazione d'ordine $< \subseteq \omega \times \omega$ sui naturali ponendo:

$$n < m := n \in m.$$

Proposizione 3.4 (Alcune proprietà dei naturali)**.** *(i) $\forall n \, (0 \neq suc(n))$,*

(ii) $\forall n, m \, (n + 1 = m + 1 \to n = m)$,

(iii) $\forall n, m \, (n < m \vee n = m \vee m < n)$,

(iv) $\forall m, n \, (m < n \vee m \not< n)$,

(v) $\forall m, n \, (m = n \vee m \neq n)$,

(vi) $\varphi(0) \wedge \forall n \in \omega \, (\varphi(n) \to \varphi(suc(n))) \to \forall n \, \varphi(n)$.

Dimostrazione. Esercizio. □

Una volta introdotti i numeri naturali, possiamo definire come al solito operazioni di addizione e moltiplicazione sui naturali grazie ad un teorema di recursione (insiemistica) per **CZF** dimostrabile facendo uso di istanze di $\in$ - induzione.[13]

Esercizio 3.5. (1) *Dimostrare usando $\in$ - induzione l'esistenza del più piccolo insieme che soddisfa l'assioma dell'infinito; ossia dimostrare che vi è un insieme, ω, che soddisfa l'assioma e tale che per ogni altro insieme y che contine* 0 *come elemento e che è chiuso rispetto a successore si dia $\omega \subseteq y$.*

(2) *Si scrivano per intero i primi 7 numeri naturali.*
Si dimostri che per ogni numero naturale n, $n \in suc(n)$.

(3) *Diciamo che un insieme a è* **transitivo** *se ogni suo elemento è un suo sottoinsieme, ovvero, $Tran(a) := \forall x \in a\,(x \subseteq a)$. Si dimostri che i numeri naturali sono transitivi.*

(4) * *Un numero* **ordinale** *è un insieme transitivo i cui elementi sono a loro volta transitivi. Indichiamo con $\alpha, \beta, \ldots$ i numeri ordinali. La relazione $<$ viene estesa alla classe dei numeri ordinali ponendo $\alpha < \beta := \alpha \in \beta$. Si usi un argomento simile a Proposizione 2.1 per dimostrare che la relazione $<$ sugli ordinali non soddisfa la linearità; in altri termini si dimostri che qualora si assuma che per ogni α, β si dia $\alpha < \beta \vee \alpha = \beta \vee \beta < \alpha$, si ottiene così la derivabilità di istanze di* **REM**.

4. Assioma di scelta

Uno dei più discussi e noti principi utilizzati oggi nella matematica (classica) è il principio di scelta. Nella teoria degli insiemi esso prende la forma di Assioma di scelta, **AC**, ed è stato dimostrato consistente con **ZF** (Gödel), sebbene sia da essa indipendente (Choen).

L'assioma di scelta, non è però compatibile con **CZF**: si può infatti osservare che l'aggiunta di **AC** a **CZF** comporta la derivabilità di **REM**. Di conseguenza se si desidera operare all'interno di una teoria degli insiemi genuinamente intuizionistica si deve rinunciare all'assioma di scelta. Si noti tuttavia che è possibile optare per principi di scelta più deboli, come scelta denumerabile, **CC**, e scelta dipendente, **DC**, che sono invece compatibili con la teoria costruttiva. Aczel [2] ha infatti mostrato la loro validità nell'interpretazione di **CZF** nella teoria dei tipi di Martin Löf.

Si osservi che l'assioma di scelta è derivabile nella teoria dei tipi, a causa dell'identificazione di proposizioni e tipi.

AC è la seguente proposizione:

$$(\forall x \in a)\,(\exists y \in b)\,\psi(x, y) \to (\exists f : a \to b)\,(\forall x \in a)\,\psi(x, f(x)).$$

[13] Si veda Aczel e Rathjen [4].

Vediamo ora l'argomento che dimostra che **AC** insieme agli assiomi di **CZF** implica **REM**. Vi sono chiare somiglianze con Proposizione 2.1.

Proposizione 4.1. $\mathbf{CZF} + \mathbf{AC} \implies \mathbf{REM}$.

Dimostrazione. Si assuma la validità di **AC**. Sia φ una Δ_0 formula e si definiscano

$$a = \{n \in \omega : n = 0 \vee (n = 1 \wedge \varphi)\},$$

$$b = \{n \in \omega : n = 1 \vee (n = 0 \wedge \varphi)\}.$$

Questi sono insiemi per Δ_0 separazione. Osserviamo che

$$(\forall z \in \{a, b\})(\exists n \in \omega)(n \in z).$$

Utilizzando ora **AC** abbiamo una funzione di scelta $f : \{a, b\} \to \omega$, tale che $f(a) \in a$ and $f(b) \in b$.

Poichè i valori di f sono numeri naturali, abbiamo $f(a) = f(b)$ oppure $f(a) \neq f(b)$.

- se $f(a) = f(b)$, allora φ, e quindi $\varphi \vee \neg\varphi$;
- se $f(a) \neq f(b)$, allora $\neg\varphi$, ovvero $\varphi \to \bot$. Infatti, supponiamo che φ valga. Per estensionalità $a = b$ così che $f(a) = f(b)$. Quindi $\neg\varphi$, e dunque $\varphi \vee \neg\varphi$.

In entrambi i casi $\varphi \vee \neg\varphi$. □

Esercizio 4.2. *(1) Dimostrare la validità in* **CZF** *del seguente principio:*

$$(\forall x \in a)\,(\exists! y \in b)\,\psi(x, y) \to (\exists f : a \to b)\,(\forall x \in a)\,\psi(x, f(x)).$$

Tale enunciato è spesso indicato con il nome di principio di scelta unica. Myhill ([16]*) lo ha caratteristicamente battezzato principio di non scelta.*

(2) L'assioma di scelta denumerabile, **CC**, *è il seguente principio, per $\psi(x, y)$ arbitraria:*

$$(\forall x \in \omega)\,(\exists y \in \omega)\,\psi(x, y) \to (\exists f : \omega \to \omega)\,(\forall x \in \omega)\,\psi(x, f(x)).$$

L'assioma di scelta dipendente, **DC**, *è il seguente schema, per formula $\psi(x, y)$ arbitraria: se*

$$\forall x \in a\, \exists y \in a\, \psi(x, y)$$

e se $b \in a$, allora $\exists f : \omega \to a$ tale che

$$f(0) = b,$$
$$\forall n \in \omega\, \psi(f(n), f(n + 1)).$$

Si dimostri che sulla base degli assiomi di **CZF**, **DC** *implica* **CC**.

(3) $\star$ Si dimostri che **AC** *implica* **DC**.

5. L'interpretazione di **CZF** nella teoria dei tipi di Martin Löf

Preliminarmente all'esposizione dell'interpretazione di Aczel di **CZF** nella teoria dei tipi di Martin Löf dobbiamo estendere la teoria dei tipi introdotta nel primo semestre con un tipo "large" noto con l'appellativo di Universo. Su tale universo verremo costruendo un nuovo tipo "large", il tipo degli insiemi iterati, **V**, che ha la funzione di rappresentare all'interno della teoria dei tipi la nozione di insieme caratteristica di **CZF**. Gli insiemi di **CZF** saranno cioè rappresentati nella teoria dei tipi dagli elementi del tipo **V**.

5.1. **Un principio di riflessione per la teoria costruttiva dei tipi: il primo universo.** Nel primo semestre è stata introdotta la nozione di insieme caratteristica della teoria dei tipi: un insieme è o l'insieme dei numeri naturali, **N**, o un insieme finito, $\mathbf{N_k}$, oppure un insieme ottenuto da questi per applicazione di un costruttore di tipi, quale **I**, Σ, Π etc. Questo processo dà luogo ad una struttura di insiemi finiti.

Si intende ora introdurre un nuovo tipo che non è un insieme in questo senso, ovvero non ha una delle forme appena descritte, ma che può essere pensato come la collezione di tutti gli insiemi fino ad ora introdotti. L'universo **U**, conterrà dunque un codice come rappresentante di ciascun insieme. Per semplicità lavoreremo qui senza distinguere tra i codici e gli insiemi mediante essi rappresentati.[14]

Si osservi che onde evitare di ricadere in un paradosso, non possiamo assumere che l'universo sia dello stesso "livello" degli insiemi precedenti, nè tantomeno che appartenga a sè stesso.

Sarà quindi un tipo o insieme "large" contenente tipi o insiemi "small".

L'universo può essere visto da un punto di vista logico come un principio di riflessione.

Le regole che specificano l'universo possono o meno includere una regola di eliminazione. Questa non è di fatto necessaria, e per questo verrà qui omessa. Si noti, tuttavia, che una tale regola avrebbe l'effetto di fissare i costrutti rispetto a cui l'universo è chiuso, mentre si preferisce qui postulare un universo aperto e passibile di ampliamento.

- **U** - Formazione

$$\mathbf{U}\ \mathbf{set} \qquad\qquad \frac{A \in \mathbf{U}}{A\ \mathbf{set}}$$

[14]Martin Löf [14] distingue tra universo alla Tarski e alla Russell, quest'ultimo essendo quello qui trattato. Il primo è un insieme "large" che contiene codici per gli insiemi di livello inferiore e richiede quindi anche la postulazione di una funzione di decodifica che ad un elemento dell'universo fa corrispondere un insieme "small". È questa da considerarsi la corretta formulazione dell'universo. Il nome è dovuto alla somiglianza tra l'operatore di decodifica e la nozione di verità tarskiana: l'operatore assomiglia infatti ad un predicato di verità. La seconda formulazione, qui presentata esclusivamente per questioni di semplicità notazionale, introduce invece un tipo i cui elementi sono direttamente insiemi. Deriva il nome dalla somiglianza con la teoria dei tipi ramificati di Russell.

- $\mathbf{U}$ - Introduzione

$$\frac{A \in \mathbf{U} \qquad \begin{matrix}(x \in A)\\ B(x) \in \mathbf{U}\end{matrix}}{\Pi(A,B) \in \mathbf{U}} \qquad \frac{A \in \mathbf{U} \qquad \begin{matrix}(x \in A)\\ B(x) \in \mathbf{U}\end{matrix}}{\Sigma(A,B) \in \mathbf{U}}$$

$$\frac{A \in \mathbf{U} \qquad B \in \mathbf{U}}{A{+}B \in \mathbf{U}} \qquad \frac{A \in \mathbf{U} \qquad x,y \in A}{\mathbf{I}(A,x,y) \in \mathbf{U}}$$

$$\mathbf{N}_0 \in \mathbf{U} \qquad \mathbf{N}_1 \in \mathbf{U} \qquad \ldots \qquad \mathbf{N} \in \mathbf{U}$$

5.2. **La gerarchia degli universi.** Possiamo ora ripetere l'operazione di costruzione appena compiuta postulando un nuovo universo che contiene non solo gli insiemi di base ma anche l'universo appena costruito.

E possiamo poi proseguire nel costruire una gerarchia di universi, ciascuno riflettente i livelli precedenti: $\mathbf{U}_1, \mathbf{U}_2, \mathbf{U}_3, \ldots$.

Anche in questo caso dovremo evitare di richiedere che un universo sia elemento di sè stesso, e inoltre che vi sia un universo che contenga ogni insieme (o tipo).

Si osservi che per l'interpretazione di **CZF** *nella teoria dei tipi è sufficiente postulare l'esistenza di un solo universo.*

Esercizio 5.1. *(1) Dimostrare il quarto assioma di Peano.*

5.3. **L'estensione di ML mediante un tipo, V, degli insiemi iterati.** Vogliamo ora estendere $\mathbf{ML}_1$ mediante un nuovo tipo, $\mathbf{V}$, costruito su $\mathbf{U}$ e rappresentante la nozione di *insieme iterato* propria di **CZF**. Il sistema risultante verrà chiamato $\mathbf{ML_1V}$.

Si può comprendere la necessità di introdurre un nuovo tipo $\mathbf{V}$ che adeguatamente rappresenti all'interno dellea teoria dei tipi la nozione di insieme propria di **CZF** tenendo conto della diversa natura della nozione di insieme delle due teorie. Esempio paradigmatico sono i numeri naturali: nella teoria assiomatica degli insiemi i numeri naturali sono transitivi; si ha per esempio $0 \in 1$, $1 \in 2$, $0 \in 2$ etc. Nella teori dei tipi questo non può verificarsi, essendo i numeri naturali elementi di un insieme, $\mathbf{N}$, ma non insiemi essi stessi. Se si intende ora fornire un'interpretazione di **CZF** nella teoria dei tipi si deve quindi introdurre un nuovo tipo i cui elementi possano rappresentare la concezione iterativa di insieme che caratterizza **CZF**.

Il nuovo tipo, $\mathbf{V}$, verrà introdotto sulla base dell'universo $\mathbf{U}$. L'idea di fondo è infatti di utilizzare un elemento A dell'universo come insieme di indici che ci consenta di "enumerare" gli elementi di un nuovo insieme a in $\mathbf{V}$.

Possiamo pensare al processo di indicizzazione come ad una funzione $f : A \to \mathbf{V}$; otterremo a, intuitivamente, raccogliendo in un tutto gli $f(x)$ per $x \in A$. Per analogia con la nozione di ordinale, l'insieme a è stato da Aczel indicato con la notazione $\sup(A, f)$. In altri termini, a sorge attraverso un processo di collezione di elementi prodotti "precedentemente" ed "enumerati" da A. È quindi evidente il carattere induttivo di $\mathbf{V}$.

5.4. **Le regole.** ($\mathbf{V}$- Formazione)

$$\mathbf{V} \ \mathbf{set}$$

($\mathbf{V}$- Introduzione)

$$\frac{A \in \mathbf{U} \qquad\qquad f \in A \to \mathbf{V}}{\sup(A, f) \in \mathbf{V}}$$

($\mathbf{V}$- Eliminazione)

$$\frac{c \in \mathbf{V} \qquad\qquad \begin{array}{c}\big(A \in \mathbf{U}, f \in A \to \mathbf{V}, g \in (\Pi v \in A)C(f(v))\big) \\ \\ d(A, f, g) \in C(\sup(A, f))\end{array}}{Rec(c, d) \in C(c)}$$

Come accennato, gli elementi di $\mathbf{V}$ rappresenteranno gli insiemi di **CZF**.

Indichiamo con $A, B, \ldots$ gli elementi di $\mathbf{U}$, mentre con $a, b \ldots$ quelli di $\mathbf{V}$.

Gli elementi di $\mathbf{V}$ possono essere anche visti come alberi i cui nodi sono prodotti da elementi dell'universo, mentre la connessione tra nodi esprime la relazione di appartenenza.

Definiremo ora una relazione di equivalenza tra elementi di $\mathbf{V}$ che adeguatamente rappresenti l'uguaglianza estensionale della teoria assiomatica degli insiemi. La relazione è una naturale equivalenza tra alberi: due alberi sono equivalenti se ad ogni nodo dell'uno corrisponde un nodo dell'altro al primo equivalente e viceversa.

5.5. **La relazione di equivalenza su V e l'analogo dell'appartenenza.** Siano $A \in \mathbf{U}$, $f \in A \to \mathbf{V}$ ed $a = \sup(A, f)$. Scriviamo $\bar{a}$ per A e $\tilde{a}$ per f.

Definiamo $a \doteq b$ come segue:

$$\Sigma(\Pi(\bar{a}, (u).\Sigma(\bar{b}, (v).\tilde{a}(u) \doteq \tilde{b}(v))),\ (x).\,\Pi(\bar{b}, (v).\Sigma(\bar{a}, (u)\tilde{a}(u) \doteq \tilde{b}(v)))),$$

mentre $b \,\dot{\in}\, a$ è:

$$\Sigma(\bar{a}, (u).\, b \doteq \tilde{a}(u)).$$

Usando l'isomorfismo di Curry-Howard otteniamo la formula:

$$a \doteq b \ := \ \forall u \in \bar{a}\, \exists v \in \bar{b}\ (\tilde{a}(u) \doteq \tilde{b}(v)) \ \wedge\ \forall v \in \bar{b}\, \exists u \in \bar{a}\ (\tilde{a}(u) \doteq \tilde{b}(v)),$$

inoltre:

$$b \,\dot{\in}\, a \ := \ \exists u \in \bar{a}\, (b \doteq \tilde{a}(u)).$$

L'esistenza di $a \doteq b$ per $a, b \in \mathbf{V}$ si dimostra attraverso una doppia recursione su $\mathbf{V}$ (facendo quindi uso di $\mathbf{V}$- eliminazione).

Si dimostra così anche che per a e b in $\mathbf{V}$, $a \doteq b \in \mathbf{U}$ e quindi anche $b \dot{\in} a \in \mathbf{U}$.

5.6. **L'interpretazione.** Le variabili di LST sono interpretate da elementi di $\mathbf{V}$ (per comodità qui non distingueremo tra le variabili di LST e la loro interpretazione).

Per ogni formula φ di LST definiamo un tipo $||\varphi||$ che ne rappresenta l'interpretazione nella teoria di Martin Löf.

$$
\begin{array}{ccc}
||a = b|| & := & a \doteq b \\
||a \in b|| & := & a \dot{\in} b \\
||a \wedge b|| & := & \Sigma(a, (x).b) \\
||a \vee b|| & := & +(a, (x).b) \\
||a \rightarrow b|| & := & \Pi(a, (x).b) \\
||\forall x \in a\, \varphi|| & := & \Pi(a, (x).||\varphi||) \\
||\exists x \in a\, \varphi|| & := & \Sigma(a, (x).||\varphi||) \\
||\forall x\, \varphi|| & := & \Pi(\mathbf{V}, (x).||\varphi||) \\
||\exists x\, \varphi|| & := & \Sigma(\mathbf{V}, (x).||\varphi||)
\end{array}
$$

Si osservi che se ψ è Δ_0, allora $||\psi|| \in \mathbf{U}$. Questo consegue (per induzione sulla costruzione della formula ψ) dal fatto che per $a, b \in \mathbf{V}$ si ha $a \doteq b \in \mathbf{U}$ e $a \dot{\in} b \in \mathbf{U}$.

D'altro canto, se ψ contiene quantificatori illimitati, la sua interpretazione risulta essere un tipo "large", essendo $\mathbf{V}$ "large".

5.7. **Verifica dell'interpretazione.** Diamo di seguito un'intuizione di come si procede nel verificare l'interpretazione di **CZF** in $\mathbf{ML_1V}$. Si vedano gli articoli [1] e [2] di Aczel oppure il testo [17] per i dettagli.

- Si dovrà verificare prima di tutto la validità della logica dei predicati e degli assiomi di uguaglianza.
- Dovremo poi controllare la validità dell'assioma di estensionalità.
- Per ciascun assioma che postuli l'esistenza di un insieme dovremo costruire un elemento di $\mathbf{V}$ che lo interpreti o rappresenti.
- La $\in$ - induzione segue direttamente dalla regola di $\mathbf{V}$- eliminazione.

(1) *Assiomi e regole del calcolo dei predicati intuizionistico*
Si utilizzi la definizione di $||\varphi||$.
Esercizio

(2) *Assiomi di uguaglianza*
Si deve dimostrare che per ogni $a, b, c \in \mathbf{V}$:
$a \doteq a$,
$a \doteq b \rightarrow b \doteq a$,
$a \doteq b \wedge b \doteq c \rightarrow a \doteq c$.
Dimostrazione: mediante $\in$ - induzione.

Per esempio, per dimostrare la validità del primo assioma, si assuma la validità della riflessività per elementi di a e si derivi la sua validità per a. Mediante $\in$ - induzione si potrà quindi concludere che la riflessività vale per ogni $a \in \mathbf{V}$.

(3) *Estensionalità*
Esercizio

(4) *Coppia*
Siano $a, b \in \mathbf{V}$ e si ponga

$$c := \sup(\mathbf{N}_2, (z).\mathbf{R}_2(z, a, b)).$$

Si dimostra quindi facilmente che $c \in \mathbf{V}$ e si può inoltre facilmente verificare che c rappresenta adeguatamente la nozione di coppia di a e b.

(5) *Unione*
Sia $a \in \mathbf{V}$ e sia

$$c := \sup\big(\Sigma(\bar{a}, (x).\,\overline{\tilde{a}(x)}), (y).\,\widetilde{\tilde{a}(\pi_0 y)}(\pi_1(y))\big).$$

Anche in questo caso si verifica facilmente che $c \in \mathbf{V}$ e che rappresenta $\bigcup a$.

(6) Δ_0 - *Separazione*
Sia $a \in \mathbf{V}$ e $||\varphi||$ l'interpretazione in $\mathbf{ML_1V}$ di una Δ_0 formula, φ, di **CZF**.
Si pongano

$$A := \Sigma(\bar{a}, (x).\,||\varphi(\tilde{a}(x))||)$$

e

$$c := \sup\big(A, (z).(\tilde{a}(\pi_0(z)))\big).$$

Ricordando che per φ Δ_0 si ha $||\varphi|| \in \mathbf{U}$, otteniamo facilmente $c \in \mathbf{V}$ e c rappresenta l'insieme $\{y \in a : \varphi y\}$.

(7) *Collezione forte*
Sia $a \in V$ e supponiamo che $\forall x \in \bar{a}\, \exists y \in \mathbf{V}\, ||\varphi(\tilde{a}(x), y)||$ (ovvero che il tipo corrispondente sia abitato).
Si usi *l'assioma di scelta* in $\mathbf{U}$ così da ottenere $g \in \bar{a} \to \mathbf{V}$ tale che $(\forall x \in \bar{a})\, ||\varphi(\tilde{a}(x), g(x))||$. Si osservi che l'assioma di scelta vale nell'universo, sebbene non valga in $\mathbf{V}$.
Sia $b := \sup(\bar{a}, g)$.
Chiaramente $b \in \mathbf{V}$ e si può mostrare che b rappresenta di fatto l'insieme postulato da collezione forte.

(8) *Esponenziazione*
Dati $a, b \in \mathbf{V}$ si ponga

$$c := \sup\big(\bar{a} \to \bar{b}, (z).\,\sup(\bar{a}, (x).\,\tilde{b}(z(x)))\big).$$

Risulta quindi $c \in \mathbf{V}$.

(9) *Infinito*
Sia
$$\dot{\emptyset} := \sup(\mathbf{N}_0, \mathbf{R}_0).$$
Dato $a \in \mathbf{V}$, sia
$$suc(a) := \sup(\bar{a} + \mathbf{N}_1, (x).\, \mathbf{D}(x, \tilde{a}, (y).a)).$$
Si osservi:
- $\dot{\emptyset} \in \mathbf{V}$,
- se $a \in \mathbf{V}$ allora $suc(a) \in \mathbf{V}$, e $c \in suc(a) \leftrightarrow (c \mathrel{\dot{\in}} a \vee c \doteq a)$,
- se $a \in \mathbf{V}$ allora $(suc(a) \doteq \dot{\emptyset}) \to \perp$,
- se $a, b \in \mathbf{V}$ allora $suc(a) \doteq suc(b) \to a \doteq b$.

Dato $n \in \mathbf{N}$ si ponga
$$\Delta(n) := \mathbf{R}(n, \emptyset, (x, y).\, suc(y)).$$
Si dimostra che per $n \in \mathbf{N}$, $\Delta(n) \in \mathbf{V}$.
Si ponga infine
$$\dot{\omega} := \sup(\mathbf{N}, (n).\, \Delta(n))$$
Chiaramente $\dot{\omega} \in \mathbf{V}$ e $\dot{\omega}$ rappresenta adeguatamente l'insieme ω di **CZF** ottenuto dall'assioma dell'infinito e dai principi di $\in$ - induzione ed estensionalità.

(10) $\in$ - *induzione*
Lo schema consegue facilmente da **V** - eliminazione.

Esercizio 5.2. *(1) ⋆ Completare la dimostrazione della validità di assiomi e schemi di* **CZF** *nell'interpretazione in* $\mathbf{ML_1V}$.

Riferimenti bibliografici

[1] P. Aczel: *The Type Theoretic Interpretation of Constructive Set Theory*, in: A. MacIntyre, L. Pacholski, J. Paris (eds.), *Logic Colloquium '77* (North–Holland, Amsterdam-New York, 1978) pp. 55–66.
[2] P. Aczel: *The type-theoretic interpretation c of constructive set theory: choice principles*, in: A. S. Troelstra, D. Van Dalen (eds)., *The L.E.J. Brouwer Centenary Symposium* (North–Holland, Amsterdam, 1982) pp. 1–40.
[3] P. Aczel: *The type-theoretic interpretation of constructive set theory: inductive definitions*, in: R. B. Marcus et al. (eds.), *Logic, Methodology, and Philosophy of Science VII* (North-Holland, Amsterdam, 1986) pp. 17–49.
[4] P. Aczel, M. Rathjen: *Notes on Constructive Set Theory*, Draft available from the Internet at the address: http://www.cs.man.ac.uk/ petera/.
[5] M. Beeson: *Foundations of Constructive Mathematics*, (Springer Verlag, Berlin 1985).
[6] E. Bishop: *Foundations of constructive analysis* (McGraw-Hill, New York, 1967).
[7] E. Bishop, D. Bridges: *Constructive Analysis* (Springer, Berlin Heidelberg, 1985).
[8] S. Feferman: *A language and axioms for explicit mathematics* in: J. Crossley (ed.), *Algebra and Logic*, *Lecture Notes in Mathematics*, vol 450, (Springer, Berlin 1975), pp. 87–139.
[9] A. Fraenkel, Y. Bar-Hillel: *Foundations of set theory*, (North–Holland, Amsterdam, 1958), pp. 415.

[10] H. Friedman: *Set theoretic foundations for constructive analysis*, Annals of Math. 105 (1977), pp. 1–28.
[11] N. Goodman, J. Myhill: *Choice implies excluded middle*, Z. Math. Logik Grundlag. Math. 24 (1978), no. 5, 461.
[12] T. Jech: *Set theory*, (Academic Press, New York-London, 1978).
[13] K. Kunen: *Set theory, an introduction to independence proofs*, (North–Holland, Amsterdam, 1980)
[14] P. Martin-Löf: *Intuitionistic Type Theory*, (Bibliopolis, Naples, 1984).
[15] Y. Moskovakis: *Notes on set theory*, (Springer-Verlag, New York, 1994).
[16] J. Myhill: *Constructive Set Theory*, Journal of Symbolic Logic, 40 (1975), pp. 347–382.
[17] A. S. Troelstra and D. van Dalen: *Constructivism in Mathematics: an Introduction*, volumes I and II (North–Holland, Amsterdam 1988).

Indice analitico

Dipartimento di Filosofia, Università degli Studi di Firenze, Via Bolognese, 52, 50139 Firenze, Italia, E-mail: Laura.Crosilla@unifi.it