Circolarità

Minor Thesis

Dott. Marco Giovanni Benini

Dottorato di Ricerca XI Ciclo
Dipartimento di Scienze dell'Informazione
Università degli Studi di Milano

Sommario

In questo lavoro analizzeremo il concetto di circolarità, ovvero come sia possibile definire una teoria matematica generale in cui dare definizioni autoreferenziali, garantendo l'esistenza ed unicità del definendo.

L'esempio più semplice é dato dalle definizioni induttive, ma, in questo lavoro intendiamo analizzare metodi più generali di individuazione di oggetti che non siano riducibili al caso di definizione per induzione.

Per fare ciò, descriveremo la teoria degli insiemi non ben fondati, ed in essa svilupperemo alcuni esempi particolarmente significativi, tratti dall'Informatica e dalla Matematica.

Mostreremo come la teoria generale di cui trattiamo sia al contempo sufficentemente potente da fornire per ognuno degli esempi una soluzione esatta, con tutte le proprietà che ragionevolmente possiamo attenderci da essa, ma anche come tale teoria generale sia naturale, ovvero il tipo di formalizzazione che daremo per ogni esempio rispecchia fedelmente, e semplicemente, l'idea intuitiva soggiacente.

15 marzo 1998

Indice

1 Introduzione

In questo lavoro intendiamo analizzare il concetto di circolarità ed illustrare un insieme di strumenti e tecniche per modellare fenomeni circolari.

Il concetto di circolarità é facilmente definibile in termini matematici:

Definizione 1 *Una relazione binaria R si dice* non ben fondata *se esiste una sequenza infinita $b_0, \ldots, b_n, \ldots$ tale che, per ogni $n \in \mathbb{N}$, b_{n+1} R b_n.*

Definizione 2 *Una relazione binaria R si dice* circolare *se esiste una sequenza finita $b_0, \ldots, b_k$ con $b_0 \equiv b_k$ tale che b_{n+1} R b_n, per ogni n, $0 \leq n < k$.*

Il punto di partenza per la nostra analisi é dato dalla osservazione:

Proposizione 3 *Una relazione circolare é non ben fondata.*

Lo scopo di questa introduzione é triplice:

- mostrare come l'idea di circolarità ricorra frequentemente in molti campi della Matematica e dell'Informatica;
- illustrare i problemi che, storicamente, questa nozione ha introdotto;
- discutere brevemente, e tecnicamente, il significato che una teoria della circolarità induce nell'usuale pratica matematico/informatica.

Per quanto il taglio di questo lavoro sia teorico, da alcuni anni, specialmente nelle discipline legate all'Intelligenza Artificiale, molte applicazioni pratiche dei concetti che illustreremo sono state efficacemente usate per risolvere problemi *difficili* [Pau92,Pau93,Bar89].

1.1 Fenomeni Circolari

In questa prima sezione, illustreremo alcuni fenomeni che, in modo più o meno diretto, danno il sapore del concetto di circolarità.

Prima di addentrarci nei dettagli, vorremmo dare giustificazione del modo in cui presenteremo tali esempi. Innanzitutto useremo la parola *circolare* in modo molto informale, cercando, prima di affrontare un'analisi matematica precisa, di "costruire" una intuizione del concetto.

In secondo luogo, cercheremo di definire qual'é un'attesa ragionevole per una teoria della circolarità.

In modo informale sempre, cercheremo di suggerire che, in un certo senso, la descrizione di un fenomeno circolare si riduce a dare una definizione matematica di cui occorre garantire la *bontà*, ovvero che il definendo esista e sia univocamente determinato.

Questa sarà la chiave che consentirà, con una generalizzazione verso strutture non ben fondate, come già accennato in precedenza, di costruire una teoria che permetta di trattare i fenomeni che stiamo per descrivere soddisfacendo tutti i requisiti che andremo a delineare.

1.1.1 Sequenze

Alcune strutture dati concrete sono difficili da caratterizzare in forma di un modello matematico astratto [AHU83].

Un esempio comune é il file: esso é descrivibile come una sequenza di dati aventi tutti lo stesso tipo. L'idea chiave di sequenza pone qualche difficoltà.

Ciò che vorremmo catturare é una definizione formale che esprima una sequenza come una lista potenzialmente infinita.

Una lista (il tipo di dato lista) é descritto come:

- **Nil** é una lista di α;
- se a é un oggetto di tipo α, e l é una lista di α, allora **Cons** a l é una lista di α;
- niente altro é una lista di α.

Questa definizione é circolare, ma la clausola finale forza ad una definizione induttiva, quindi la definizione é *ben data*.

Vorremmo poter definire in modo analogo una sequenza di α, con la possibilità di dimostrare le proprietà rilevanti di questa struttura dati, quali quelle che la distinguono dalle liste: l'equazione

$$x = \textbf{Cons}\ a\ x$$

non ammette soluzioni se x é una lista, mentre ammette come soluzione la stringa di lunghezza infinita composta di sole a, se x é una sequenza.

Questo esempio ci dice che una teoria della circolarità "accettabile", deve contenere l'induzione (per poter trattare le liste), ma non deve limitarsi ad essa: in particolare deve permettere di definire strutture dati infinitarie come le sequenze.

1.1.2 Chiusure

Una costruzione algebrica [MB65,Lan65] spesso utilizza lo strumento della chiusura: data una relazione τ, si definisce la relazione τ^c come la più piccola relazione contenente τ che sia chiusa rispetto ad una o più operazioni e/o proprietà.

Un esempio é la chiusura riflessiva e transitiva: se τ é una relazione su $\mathbb{S}$, τ^* é la più piccola relazione su $\mathbb{S}$ tale che:

- $\tau \subseteq \tau^*$,
- $\forall x \in \mathbb{S}.\ x\ \tau^*\ x$,
- $\forall x, y, z \in \mathbb{S}.\ x\ \tau^*\ y \wedge y\ \tau^*\ z \rightarrow x\ \tau^*\ z$.

Una definizione *per chiusura* é circolare: formalizzando il concetto di "più piccola relazione tale che", otteniamo, nel caso dell'esempio

$$\forall \rho.\ \rho \subseteq \tau \wedge (\forall x \in \mathbb{S}.\ x\ \rho\ x) \wedge (\forall x, y, z \in \mathbb{S}.\ x\ \rho\ y \wedge y\ \rho\ z \rightarrow x\ \rho\ z) \rightarrow \tau^* \subseteq \rho\ .$$

La circolarità é dovuta al fatto che "per ogni ρ" significa "anche per τ^*". Questa forma di circolarità é nota come *impredicatività* [Bar84,JH56].

Il concetto di chiusura suggerisce naturalmente una costruzione duale: data una relazione τ, si definisce la relazione τ_c come la più grande relazione contenuta in τ che sia chiusa rispetto ad una o più operazioni e/o proprietà. Converremo di chiamare questa costruzione *co-chiusura*, sfruttando il modo di dare nomi ai concetti duali tipico della Teoria delle Categorie [Mac71].

Queste considerazioni ci portano a desiderare una teoria della circolarità che descriva i fenomeni di impredicatività, ma che permetta anche di identificare, in modo uniforme, costruzioni duali.

1.1.3 Auto-Applicazione

Una delle caratteristiche salienti del λ-Calcolo [Bar84] e della Logica Combinatoria [HS86,CF58] é la possibilità di applicare un operatore a se stesso. La possibilità é ampiamente sfruttabile per codificare, ad esempio, la ricorsione [Tur37]. Tuttavia possono presentarsi fenomeni di natura patologica, che sono oggetto di studio in queste discipline.

Consideriamo i combinatori:

$$I = S\,K\,K$$

e

$$\omega = \lambda x.\ x\, x$$

dove, al solito,

$$S = \lambda x\, y\, z.(x\, z)(y\, z)$$

e

$$K = \lambda x\, y.\ x\ \ .$$

Sfruttando le regole di riduzione dei rispettivi sistemi, possiamo dedurre che:

- $I\, I = S\, K\, K\, I = K\, I\, (K\, I) = I$,
- $\omega\, \omega = (\lambda x.\ x\, x)\, \omega = \omega\, \omega = \ldots$,
- $I\, \omega = S\, K\, K\, \omega = K\, \omega\, (K\, \omega) = \omega$,
- $\omega\, I = (\lambda x.\ x\, x)\, I = I\, I = I$.

Come vediamo $I\, I$,$I\, \omega$ e $\omega\, I$ ammettono una forma normale, mentre $\omega\, \omega$ non é riducibile che a se stesso.

Se, come consuetudine quando si usi il λ-Calcolo per modellare qualche altro sistema, immaginiamo un termine come una "definizione" per (l'unico) "valore" costituito dalla sua forma normale, $\Omega = \omega\, \omega$ é una definizione circolare che non individua alcun elemento.

L'accento in questi esempi é posto sulla *convergenza* della definizione circolare: $I\, I$ *converge* ad I, mentre $\omega\, \omega$ *diverge*. indexdivergenza

Un criterio che ci aspettiamo emergere dalla teoria della circolarità, é una descrizione/discriminazione tra criteri "convergenti" e "divergenti". I primi permetteranno di definire un oggetto, i secondi saranno utili per un'analisi astratta della struttura matematica sottostante al mondo in considerazione.

1.1.4 Concorrenza

Il problema basilare nell'Algebra dei Processi [Mil73] consiste nell'identificazione, ovvero quando due espressioni sintatticamente differenti designano lo stesso fenomeno. A questo scopo viene introdotta la nozione di *bisimulazione*.

Supponiamo di usare l'algebra dei CCS [Mil89]; un processo P bisimula un processo Q ($P \approx Q$) se e solo se:

$$\forall \alpha, P'.\ P \xrightarrow{\alpha} P' \rightarrow \exists Q'.\ Q \xrightarrow{\alpha} Q' \wedge P' \approx Q' \qquad (1)$$

e

$$\forall \alpha, Q'.\ Q \xrightarrow{\alpha} Q' \rightarrow \exists P'.\ P \xrightarrow{\alpha} P' \wedge P' \approx Q' \tag{2}$$

In parole, se, ogni volta che P effettua una azione, riducendosi a P', Q può effettuare la stessa azione, riducendosi ad un Q' tale che P' bisimuli Q'; la stessa cosa avviene per Q.

É immediato provare che la relazione $\approx$ é di equivalenza, quindi essa può essere usata come uguaglianza. Si può provare [Mil89] che $\approx$ é una congruenza, per cui é un concetto che ben si adatta all'identificazione di termini.

É anche evidente la circolarità della definizione, ma é facile convincersi che non si tratta di una definizione *per induzione*, potendo P' essere uguale (sintatticamente) a P:

$$\alpha\ .\ \mu X\ .\ \alpha\ .\ X \approx \mu X\ .\ \alpha\ .\ X\ \ .$$

Modificando la definizione base si ottengono altre forme utili di bisimulazione: se nel conseguente di (1) e (2) si sostituisce a $\xrightarrow{\alpha}$, la riduzione osservazionale $\stackrel{\hat{\alpha}}{\Longrightarrow}$ [Mil80], otteniamo la bisimulazione debole, che identifica processi che hanno lo stesso comportamento sulle azioni *osservabili*.

Si possono introdurre parecchie modifiche nello schema base di bisimulazione [Mil80], ottenendo un modo di confrontare processi, anche infiniti, che ne espleti l'aspetto "comportamentale" rispetto a quello "strutturale".

Il problema che riveste maggiore interesse dal punto di vista della circolarità é: quando, e perché, una bisimulazione é ben definita ? Ovvero, come é possibile garantire che esista una, ed una sola, relazione soddisfacente alle condizioni (o a varianti di) (1) e (2) ?

1.2 Paradossi

Qualsiasi forma una teoria della circolarità possa assumere, é necessario che essa faccia fronte ad un insieme di problemi che sono dati dai paradossi.

Presentiamo ora di seguito una piccola selezione di paradossi; in alcuni vedremo come la nozione di circolarità é solo la porta che permette il passaggio dell'inconsistenza, ma in altri casi, la circolarità é il supporto principale su cui il paradosso poggia.

É evidente che ogni teoria soddisfacente della circolarità debba fornire una soluzione ai paradossi di cui stiamo per parlare.

1.2.1 Russell

Forse il più noto paradosso della matematica é il paradosso di Russell [Rus06]. Consideriamo l'insieme $R = \{x \mid x \notin x\}$; se $R \notin R$ allora deve essere $R \in R$; se $R \in R$ allora, per definizione, $R \notin R$. In entrambi i casi otteniamo una contraddizione.

Come é noto, questo paradosso ammette una semplice soluzione: abbiamo assunto, erroneamente, che R sia un insieme. Se R non é un insieme, R non può essere elemento di un insieme, quindi le espressioni $R \in R$ e $R \notin R$ sono sintatticamente errate, poichè la relazione di appartenenza $\in$ é definita tra insiemi e classi. Il paradosso dice che R é una classe che non é un insieme.

Dal punto di vista della circolarità, vale la pena sottolineare che il paradosso NON nasce dall'autoriferimento. Se modifichiamo lievemente l'enunciato, questo fatto risulta evidente:

$$R_b = \{x \in b \mid x \notin x\} \ .$$

Quanto ci dice la costruzione di Russell é, semplicemente, che $R_b \notin b$.

1.2.2 Mentitore

Un paradosso classico che riguarda le asserzioni circolari é il paradosso del mentitore [Kri75,Mar84]: la sua forma più semplice é

io sto dicendo il falso. (3)

Se assumiamo l'asserzione (3) vera, allora (3) deve essere falsa, ottenendo un assurdo. Se (3) é falsa, allora deve essere vera, assurdo.

Una formulazione equivalente é: *questa asserzione é falsa.*

Come noto dal Teorema di Gödel [Göd31], questo paradosso può essere formulato in numerose teorie matematiche, ad esempio l'Aritmetica di Peano, con la conseguenza che esse sono incomplete, ovvero che esistono enunciati indecidibili. Di più, esse sono incompletabili, ovvero é sempre possibile estendere tali teorie, ma, in ogni possibile estensione *sensata* (effettivamente assiomatizzabile), é possibile riformulare il paradosso del mentitore, costruendo, di fatto, un enunciato indecidibile [Tar39].

La chiave di volta che genera il paradosso, ancora una volta, non é la circolarità, ma la nostra interpretazione di *questa asserzione* e di *falso*: il fatto che "questa" sia formalmente costruibile induce la circolarità nel sistema formale, ma ciò che effettivamente genera il paradosso, come il Teorema di Gödel prova, é che noi assumiamo, arbitrariamente, che ogni asserto sia dimostrabilmente vero oppure dimostrabilmente falso.

1.2.3 Ipergioco

Il paradosso dell'ipergioco [Zwi87] ha una natura lievemente diversa dai precedenti. La sua formulazione é la seguente: sia G una qualsiasi gioco che si svolga fra due contendenti. Chiameremo *regolare* un gioco che, dopo un numero finito di mosse, permetta sempre di designare un vincitore; chiameremo *irregolare* un gioco che non goda di questa proprietà. Consideriamo l'ipergioco siffatto: se A e B sono i due antagonisti, A sceglie un gioco regolare, B effettua la prima mossa, e, se A vince, allora é anche il vincitore dell'ipergioco, viceversa se B vince, allora B é il vincitore dell'ipergioco.

Apparentemente questo gioco é regolare: dovendo A scegliere un gioco regolare, esso termina dopo un numero finito di mosse con un vincitore, quindi anche l'ipergioco termina con il medesimo vincitore.

Tuttavia se l'ipergioco é regolare, allora A può scegliere l'ipergioco. Ma se sia A che B scelgono alternativamente l'ipergioco, esso non terminerà dopo un numero finito di mosse, quindi l'ipergioco é irregolare. Se l'ipergioco é irregolare, allora é facile convincersi che terminerà sempre dopo un numero finito di mosse, e, per di più, con un vincitore, quindi é regolare.

In questo caso, la soluzione più semplice per rimuovere il paradosso, consiste nel notare che la classe dei giochi regolari é *grande*, ovvero non é un insieme, e quindi non esiste un ipergioco, nel senso che la sua definizione é mal fondata.

Questa soluzione é insoddisfacente: non insegna qualcosa, come invece accade per il paradosso di Russell o per il paradosso del mentitore. Invece sembra che debba esistere una soluzione più profonda, che mostri come la costruzione di un ipergioco sia impossibile in virtù di una caratteristica strutturale del concetto di circolarità.

2 Teoria degli Insiemi Non Ben Fondati

In questa parte del lavoro intendiamo introdurre la teoria degli insiemi non ben fondati. Svilupperemo dapprima una estensione della teoria classica degli insiemi, e quindi, useremo questa per derivare alcuni risultati sui concetti di punto fisso e di bisimulazione.

Avendo queste basi, nella parte successiva ci occuperemo di applicare la teoria ai fenomeni circolari per analizzarli e formalizzarli.

2.1 ZF

Lo scopo che ci prefiggiamo in questa sezione é dare le basi su cui fondare una teoria degli insiemi che contenga gli strumenti per parlare, in generale, di insiemi non ben fondati, ed in particolare, di concetti circolari.

Noi estenderemo nel prosieguo la teoria degli insiemi di Zermelo e Frænkel (**ZF**) [Sho77,Hal60,Kun80]. Per chiarezza e semplicità di rifermento riportiamo una tra le possibili formulazioni:

- Estensionalità (**Ext**)

$$\forall x, y.\ (\forall z.\ z \in x \leftrightarrow z \in y) \rightarrow x = y\ .$$

- Fondazione (**FA**)

$$\forall x.\ (\exists y.\ y \in x) \rightarrow \exists y.\ y \in x \wedge \neg\exists z.\ z \in x \wedge z \in y\ .$$

- Comprensione (**Compr**)
  Per ogni formula ψ con variabili libere in x, z, w_1, $\ldots$, w_n,

$$\forall z, w_1, \ldots, w_n.\ \exists y.\ \forall x.\ x \in y \leftrightarrow x \in z \wedge \psi\ .$$

- Coppia (**Pair**)

$$\forall x, y.\ \exists z.\ x \in z \wedge y \in z\ .$$

- Unione (**Un**)

$$\forall F.\ \exists A.\ \forall x, y.\ x \in y \wedge y \in F \rightarrow x \in A\ .$$

- Rimpiazzamento (**Repl**)
  Per ogni formula ψ con variabili libere in x, y, A, w_1, $\ldots$, w_n,

$$\forall A, w_1, \ldots, w_n.\ (\forall x.\ x \in A \rightarrow \exists! y.\ \psi) \rightarrow$$
$$(\exists Y.\ \forall x.\ x \in A \rightarrow \exists y.\ y \in Y \wedge \psi)\ .$$

Nel modo usuale [Kun80], con questi assiomi, é possibile definire $\subseteq$ (sottoinsieme), $\emptyset$ (insieme vuoto), S (successore ordinale, $S(X) = X \cup \{X\}$), $\cup$ (unione), e la nozione di buon ordinamento.

Quindi i seguenti assiomi completano la presentazione di **ZF**:

- Infinito (**Inf**)

$$\exists x.\ \emptyset \in x \wedge \forall y.\ y \in x \rightarrow S(y) \in x\ .$$

- Potenza (**Pow**)

$$\forall x.\ \exists y.\ \forall z.\ z \subseteq x \rightarrow z \in y\ .$$

- Scelta (**Ch**)

$$\forall A.\ \exists R.\ R \text{ bene ordina } A\ .$$

Gli assiomi importanti dal punto di vista di una estensione come quella che ci apprestiamo a fare sono l'Assioma di Fondazione e l'Assioma di Estensionalitá.

Il significato intuitivo dell'Assioma di Estensionalità é caratterizzare gli insiemi come raggruppamenti di elementi; un insieme é univocamente determinato dai suoi elementi [Sho77].

L'Assioma di Fondazione é l'assioma che serve per caratterizzare il modo *lecito* di costruire insiemi al fine di evitare i paradossi quali quello di Russell. Esso afferma che un insieme deve contenere un elemento più *semplice* dell'insieme stesso. Si può facilmente provare [Sho77,BM91] che questo é equivalente a postulare che ogni insieme é ben fondato, secondo la definizione formale data nell'introduzione.

2.2 ZFA

La nostra euristica [Acz88], per estendere **ZF**, come accennato nell'introduzione, consiste nel costruire un sistema che consenta di modellare insiemi non ben fondati. Per fare ciò sostituiremo l'Assioma di Fondazione con un nuovo assioma [BM96,BM91], generando la teoria **ZFA** (Zermelo-Frænkel con Antifondazione).

Sebbene questa sia l'unica modifica necessaria per poter costruire la nostra teoria, per facilitarne l'esposizione e per non appesantire la trattazione con condizioni accessorie, supporremo che l'universo del discorso sia partizionato in due classi: *insiemi* e *atomi*.

Per evitare ambiguità, scriveremo "insieme" intendendo un oggetto della classe degli insiemi di **ZFA**, ed useremo la scrittura "Insieme" con l'iniziale maiuscola per indicare un insieme nel senso usuale.

Con queste premesse possiamo definire il concetto chiave della nostra teoria:

Definizione 4 *Un* sistema (semplice) di equazioni *é una tripla*

$$\varepsilon = \langle X, C; e \rangle$$

dove

- X *é un Insieme non vuoto di incognite (detto l'Insieme delle incognite di* ε*).*
- C *é un Insieme di atomi.*
- e *é una funzione che mappa ogni elemento di* X *in un sottoinsieme di* $X \cup C$*.*

Inoltre[1]

- $b_v = e_v \cap X$ *é l'Insieme delle incognite da cui* $v \in X$ *dipende.*
- $c_v = e_v \cap C$ *é l'Insieme degli atomi da cui* $v \in X$ *dipende.*
- *una* soluzione *per* ε *é una funzione* s *con dominio* X *tale che*

$$s_v = \{s_w \mid w \in b_v\} \cup c_v \ .$$

Notazione 5 *Indicheremo con* $V_A[X]$ *la collezione di tutti gli insiemi formati a partire da* $A \cup X$*;* $V_A[\emptyset]$ *viene abbreviato in* V_A*.*

L'Assioma di Antifondazione[2], nella sua formulazione più semplice, é:

Assioma 6 (AFA) *Ogni sistema semplice di equazioni* $\varepsilon = \langle X, C; e \rangle$ *in un universo* $V_A[X]$ *ammette una ed una sola soluzione* s*, ed ogni valore* $s_v \in V_A$*.*

La teoria **ZFA** é costituita da tutti gli assiomi di **ZF**, eccetto che **FA** é sostituito con **AFA**.

Per poter usare questo impianto formale, é necessario sviluppare alcuni lemmi e teoremi.

---

[1] Spesso useremo la scrittura f_x invece di $f(x)$, per evidenziare il fatto che f, e non x, é il centro della nostra attenzione.

[2] In letteratura, spesso questo assioma viene chiamato Flat Solution Lemma.

Definizione 7 *Sia $\varepsilon = \langle X, A; e\rangle$ un sistema semplice di equazioni, e sia s la sua unica soluzione; per* insieme soluzione *(notiamo che é un oggetto dell'universo del discorso di **ZFA**) intendiamo $\{s_v \mid v \in X\}$.*

La filosofia di **ZFA** [BE87] é che ogni insieme deve essere l'insieme soluzione di un sistema semplice di equazioni. La teoria che stiamo per sviluppare ha lo scopo precipuo di fornire un criterio di confronto per l'uguaglianza tra due insiemi. L'Assioma di Estensionalità, da solo, é insufficente a questo scopo, poichè più di un sistema può descrivere lo stesso insieme; quindi é necessario sviluppare uno strumento di confronto che modelli naturalmente il senso dell'Assioma di Estensionalità nella teoria allargata.

Iniziamo a dare un criterio di confronto tra sistemi di equazioni:

Definizione 8 *Siano $\varepsilon = \langle X, C; e\rangle$ e $\varepsilon' = \langle X', C'; e'\rangle$ due sistemi semplici di equazioni; una* relazione di bisimilarità *(*bisimulazione*) tra ε e ε' é una relazione R su $X \times X'$ tale che:*

- $\forall x \in X.\ \exists x' \in X'.\ x\ R\ x'$;
- $\forall x' \in X'.\ \exists x \in X.\ x\ R\ x'$;
- $\forall x, x'.\ x\ R\ x' \rightarrow \forall y \in b_x.\ \exists y' \in b_{x'}.\ y\ R\ y'$;
- $\forall x, x'.\ x\ R\ x' \rightarrow \forall y' \in b_{x'}.\ \exists y \in b_x.\ y\ R\ y'$;
- $\forall x, x'.\ x\ R\ x' \rightarrow c_x = c_{x'}$.

Diciamo inoltre che ε e ε' sono bisimili *($\varepsilon \equiv \varepsilon'$) se esiste una relazione di bisimilarità tra di essi.*

Teorema 9 *Due sistemi semplici di equazioni, detti $\varepsilon = \langle X, C; e\rangle$ ed $\varepsilon' = \langle X', C'; e'\rangle$, hanno lo stesso insieme soluzione se e solo se sono bisimili.*

Dimostrazione.

- $(\rightarrow)$
  Siano s ed s' le soluzioni di ε e ε' rispettivamente. Sia $R \subseteq X \times X'$ la relazione definita come

$$x\ R\ x' \quad \text{se e solo se} \quad s_x = s'_{x'} \ .$$

  La relazione R é una bisimulazione tra ε e ε':
  · sia $x \in X$, allora $s_x \in \text{solution} - \text{set}(\varepsilon) = \text{solution} - \text{set}(\varepsilon')$, quindi esiste $x' \in X'$ tale che $s'_{x'} = s_x$, ovvero $x\ R\ x'$. Analogamente si prova la condizione simmetrica per $x' \in X'$.
  · siano $x \in X$, $x' \in X'$ tali che $x\ R\ x'$, allora, se $y \in b_x$, poichè $s_y \in s_x = s'_{x'}$, deve esistere y' tale che $y' \in e'_{x'}$, e $s_y = s'_{y'}$, ovvero $y\ R\ y'$. Analogamente si prova la condizione simmetrica.

· l'insieme degli atomi in s_x é $e_x \cap A$ poichè tutti gli s_y sono insiemi; lo stesso vale per $s'_{x'}$. Se $x\ R\ x'$, allora $s_x = s'_{x'}$ e quindi $c_x = e_x \cap A = e'_{x'} \cap A = c_{x'}$.

- ($\leftarrow$)

  Supponiamo che R sia una bisimulazione tra ε e ε', ed s e s' siano soluzioni di ε e ε' rispettivamente.

  Poichè abbiamo assunto di avere a disposizione abbastanza incognite, esistono abbastanza incognite nuove (non in X, nè in X') per coprire $X \times X'$. Per snellire la scrittura le indicheremo con $\langle u, u' \rangle$ dove $u \in X$ e $u' \in X'$.

  Sia $\varepsilon^* = \langle X^*, C; e^* \rangle$ dove

$$X^* = \{\langle v, v' \rangle \in X \times X' \mid v\ R\ v'\}\ ,$$

  e

$$e^*_{\langle u,u' \rangle} = \{\langle v, v' \rangle \in X^* \mid v \in e_u \wedge v' \in e_{u'}\} \cup c_u\ .$$

  Questo é un sistema semplice di equazioni e pertanto ammette una ed una sola soluzione.

  Consideriamo $s^1_{\langle u,u' \rangle} = s_u$ e $s^2_{\langle u,u' \rangle} = s'_{u'}$: entrambe sono soluzioni di ε^*. Proviamo il fatto per s^1, essendo la prova per s^2 simmetrica.

  Dobbiamo mostrare che

$$s^1_{\langle u,u' \rangle} = \{s^1_{\langle v,v' \rangle} \mid \langle v, v' \rangle \in e^*_{\langle u,u' \rangle}\} \cup (e^*_{\langle u,u' \rangle} \cap C)\ .$$

  Sia $\alpha \in s^1_{\langle u,u' \rangle} = s_u$; poichè s é soluzione di ε, $\alpha = s_w$ per qualche $w \in e_u \cap X$, oppure $\alpha \in e_u \cap C$. Nel primo caso, esiste $w' \in e'_v \cap X'$ con $u\ R\ v$ tale che $w\ R\ w'$, quindi $\langle w, w' \rangle \in X^*$; ma questo significa che $\alpha = s_w = s^1_{\langle w,w' \rangle}$. Nel secondo caso, $\alpha \in e^*_{\langle u,u' \rangle} \cap C$ per definizione di $e^*_{\langle u,u' \rangle}$.

  Questo dimostra che

$$s^1_{\langle u,u' \rangle} \subseteq \{s^1_{\langle v,v' \rangle} \mid \langle v, v' \rangle \in e^*_{\langle u,u' \rangle}\} \cup (e^*_{\langle u,u' \rangle} \cap C)\ .$$

  Sia ora $s^1_{\langle v,v' \rangle} \in \{s^1_{\langle w,w' \rangle} \mid \langle w, w' \rangle \in e^*_{\langle u,u' \rangle}\}$, ma $s^1_{\langle v,v' \rangle} = s_v$ e $s^1_{\langle u,u' \rangle} = s_u$, quindi, essendo s soluzione di ε, $s_v = s_u$. Se $\alpha \in C \cap e^*_{\langle u,u' \rangle}$, allora $\alpha \in C \cap e_u$ per definizione di $e^*_{\langle u,u' \rangle}$, quindi $\alpha \in s^1_{\langle u,u' \rangle}$.

  In totale

$$\{s^1_{\langle v,v' \rangle} \mid \langle v, v' \rangle \in e^*_{\langle u,u' \rangle}\} \cup (e^*_{\langle u,u' \rangle} \cap C) \subseteq s^1_{\langle u,u' \rangle}\ .$$

  Quindi s^1 é soluzione di ε^*. In modo simmetrico si prova che s^2 é soluzione di ε^*, quindi, per ogni $u \in X$, $u' \in X'$ tali che $u\ R\ u'$,

$$s_u = s^1_{\langle u,u' \rangle} = s^2_{\langle u,u' \rangle} = s'_{u'}\ .$$

  Sia $\beta \in \text{solution} - \text{set}(\varepsilon)$, allora $\beta = s_x$ per un qualche $x \in X$. Ma R é una bisimulazione, quindi esiste $x' \in X'$ tale che $x\ R\ x'$.

Per quanto sopra, $s_x = s'_{x'} = \beta$, quindi $\beta \in \text{solution} - \text{set}(\varepsilon')$. Per simmetria vale anche il viceversa, quindi ε e ε' hanno lo stesso insieme soluzione. $\square$

La conseguenza diretta del teorema appena provato é che esiste un buon criterio di confronto per gli oggetti del discorso di **ZFA**; é sufficente considerare i sistemi di equazioni che generano gli insiemi per poter confrontare gli insiemi stessi.

Il fatto di ragionare con sistemi di equazioni e le loro bisimulazioni é scomodo ed inelegante. Quindi deriviamo un criterio di confronto che richieda l'analisi solo di insiemi.

Definizione 10 *Una* bisimulazione tra insiemi *é una relazione binaria R tale che, se $a\ R\ b$, con a e b insiemi,*

- $\forall c \in a.\ \exists d \in b.\ c\ R\ d$,
- $\forall d \in b.\ \exists c \in a.\ c\ R\ d$,
- $\forall x.\ x \in a \leftrightarrow x \in b$,

dove c, d sono insiemi ed x é un atomo.

Teorema 11 (Estensionalità Forte) *Se R é una bisimulazione tra insiemi, allora $R \subseteq I$, la relazione identica. Ovvero se $a\ R\ b$, allora $a = b$.*

Dimostrazione. Iniziamo notando che I é una bisimulazione, applicando banalmente la definizione.

Siano a e b due insiemi tali che $a\ R\ b$.

Siano inoltre $\varepsilon_a = \langle X_a, C_a; e^a \rangle$ e $\varepsilon_b = \langle X_b, C_b; e^b \rangle$ i due sistemi canonici per a e b, ovvero

$$\begin{array}{ll} C_a = \{x \in a^+ \mid x \text{ é un atomo}\} & C_b = \{x \in b^+ \mid x \text{ é un atomo}\} \\ X_a = \{a\}^+ \setminus C_a & X_b = \{b\}^+ \setminus C_b \\ e^a_x = x & e^b_x = x \end{array}$$

dove α^+ é la chiusura transitiva [3] di α.

É immediato verificare che la soluzione di ε_a e di ε_b é la funzione identica.

[3] $\alpha^+ = \{x \mid x \in \alpha \vee \exists y.\ x \in y \wedge y \in \alpha^+\}$

Sia $\alpha \in C_a$, allora $\alpha \in a' \in a^+$ per un qualche a':

$$a' = a_n \in \ldots \in a_0 = a \ .$$

Poichè R é una bisimulazione, per induzione su n, esiste $b' \in C_b$ tale che $a' \ R \ b'$, ovvero $\alpha \in C_b$, essendo α un atomo.

Quindi $C_a \subseteq C_b$; simmetricamente si prova che $C_b \subseteq C_a$, quindi $C_a = C_b$.

Sia R^* la restrizione di R a $X_a \times X_b$, e sia

$$Y_a = \{x \in X_a \mid \exists x' \in X_b.\ x \ R^* \ x'\} \ .$$

Ma $a \in Y_a$ e se $x \in Y_a$ e $y \in x$, allora $y \in Y_a$, essendo X_b un insieme chiuso per transitività. Quindi, essendo $\{a\}^+$ il più piccolo insieme contenente a chiuso per transitività, $X_a \subseteq Y_a$.

Nello stesso modo si dimostra che $X_b \subseteq Y_b$.

Sia ora $x \ R^* \ y$ e $x' \in e^a_x \cap X_a$, quindi $x' \in x \cap X_a$, e x' é un insieme. Essendo R una bisimulazione tra insiemi, esiste $y' \in y$ tale che $x' \ R \ y'$, e, per transitività di X_b, $y' \in X_b$, quindi $y' \in e^b_y \cap X_b$ e $x' \ R \ y'$.

Sia $x \ R^* \ y$, quindi

$$A_x = \{\alpha \in x \mid \alpha \text{ é un atomo}\} = \{\alpha \in y \mid \alpha \text{ é un atomo}\} = A_y \ .$$

Ma $A_x \subseteq C_a$ e $A_y \subseteq C_b$, quindi $e^a_x \cap C_a = x \cap C_a = A_x$ ed $e^b_y \cap C_b = A_y$, ovvero $e^a_x \cap C_s = e^b_y \cap C_b$.

Quindi R^* é una bisimulazione tra ε_a e ε_b. Essendo s^a e s^b le soluzioni di ε_a ed ε_b ed essendo esse mappe identiche,

$$a = s^a_a = s^b_b = b \ .$$

□

Il Teorema di Estensionalità Forte ricopre il ruolo che ha l'Assioma di Estensionalità in **ZF**.

Con questi strumenti é possibile sviluppare una teoria della circolarità che soddisfi tutti i requisiti descritti nell'introduzione.

Per quanto non parte di ciò che ci accingiamo a sviluppare, vogliamo brevemente dare un'idea della prova di consistenza di **ZFA** [Acz88,BM96].

Supponiamo che $\mathcal{U}$ sia un universo modello per **ZF**. Sia $\varepsilon = \langle X, C; e\rangle$ un sistema semplice di equazioni e sia $x \in X$; sia X_x il più piccolo insieme contenente x tale che, per ogni $y \in X$, $b_y \subseteq X_x$. Sia ε_x il sistema $\langle X_x, C; e^x\rangle$ dove e^x é la restrizione di e ad X_x.

Il lemma basilare che serve (senza dimostrazione) é:

Lemma 12 *Sia ε un sistema di equazioni, x un incognita ed s la soluzione di ε. Sia s' la soluzione di ε_x, allora s' é la restrizione di s ad X_x.*

Per costruire un modello per **ZFA**, usiamo coppie $\langle\overline{\varepsilon}, \overline{x}\rangle$ dove $\overline{\varepsilon}$ é una opportuna codifica del sistema ε ed $\overline{x}$ é la codifica dell'incognita x di ε.

Definiamo $\langle\varepsilon, x\rangle \equiv \langle\varepsilon', x'\rangle$ se e solo se esiste una bisimulazione R tra ε_x ed $\varepsilon'_{x'}$, tale che $x\ R\ x'$. Costruendo il quoziente di $\mathcal{U}$ rispetto a $\equiv$, otteniamo il modello desiderato, con l'appartenenza definita come: $\langle\varepsilon, x\rangle \in \langle\delta, y\rangle$ se e solo se esiste $z \in B^\delta_y$ tale che $\langle\varepsilon, x\rangle \equiv \langle\delta, z\rangle$.

Utilizzando tecniche standard é possibile provare che ogni assioma di **ZFA** é vero in questo modello.

Analizzando l'impianto della prova di consistenza ci rendiamo conto che essa assume la consistenza di **ZF**. Infatti abbiamo assunto di avere un universo $\mathcal{U}$ che fosse modello per **ZF**, e, mediante una opportuna costruzione, abbiamo immerso in $\mathcal{U}$ un modello per **ZFA**.

Quindi, la prova della consistenza di **ZFA**, é, in effetti, una prova di indipendenza dell'Assioma di Antifondazione.

2.4 Punti Fissi

Uno dei modi più tipici [Smu94] di dare una definizione circolare ha la struttura

$$X \textit{ é il più piccolo oggetto tale che } X = \Gamma(X)$$

per qualche operazione Γ.

Il concetto soggiacente é:

Definizione 13 *Un* punto fisso *per la trasformazione* $\Gamma\colon \mathcal{U} \longrightarrow \mathcal{U}$ *é una soluzione dell'equazione* $X = \Gamma(X)$.

Per poter usare i punti fissi come strumenti definitori, é necessario garantirne l'esistenza ed un modo per selezionarne uno, quello, d'interesse.

La condizione sufficente per garantire l'esistenza di punti fissi é legata al concetto di monotonicità.

Definizione 14 *Un* operatore *é una qualsiasi funzione che trasforma elementi dell'universo di un modello di* ***ZFA*** *in elementi dello stesso universo.*

Definizione 15 *Un operatore* Γ *é detto* monotono *se, per ogni* a, b *tali che* $a \subseteq b$, *allora* $\Gamma(a) \subseteq \Gamma(b)$.

Alcuni esempi di operatori monotoni sono:

$\Gamma_1(a) = \mathcal{P}(a)$ dove $\mathcal{P}(a)$ é l'insieme potenza di a.

$\Gamma_2(a) = \mathcal{P}_{\text{fin}}(a)$

$\Gamma_3(a) = A \times a$ per un insieme fissato A.

$\Gamma_4(a) = \{f \mid f \text{ é una funzione parziale da } a \text{ in } a\}$

$\Gamma_5(a) = \mathcal{P}(A \times a)$ per un insieme fissato A.

Proposizione 16 *La composizione di operatori monotoni é monotona.*

Per nostra comodità definiamo le proprietà interessanti di un operatore monotono rispetto ai punti fissi.

Definizione 17 *Sia* Γ *un operatore monotono*

- *un insieme* G *é detto* Γ-corretto *se* $G \subseteq \Gamma(G)$*;*
- *un insieme* G *é detto* Γ-chiuso *se* $\Gamma(G) \subseteq G$*;*
- *un insieme* G *é un* punto fisso per Γ *se é sia* Γ*-chiuso che* Γ*-corretto;*
- *un insieme* G *é il* più piccolo punto fisso di Γ *se* G *é un punto fisso per* Γ *e, per ogni punto fisso* H *di* Γ, $G \subseteq H$*;*
- *un insieme* G *é il* più grande punto fisso di Γ *se* G *é un punto fisso per* Γ *e, per ogni punto fisso* H *di* Γ, $H \subseteq G$.

Intuitivamente la nozione di minimo punto fisso corrisponde ad una definizione per induzione.

Come primo passo formalizziamo questa intuizione.

Teorema 18 (Minimo Punto Fisso) *Ogni operatore monotono* Γ *ammette un minimo punto fisso (denotato con* Γ_**). Esso é caratterizzato come*

- $\Gamma_* = \bigcup_\alpha \Gamma_\alpha$, *con* α *ordinale e* $\Gamma_\alpha = \bigcup_{\beta<\alpha} \Gamma(\Gamma_\beta)$.
- Γ_* *é la più piccola classe* Γ*-chiusa.*

Dimostrazione. Sia $\Gamma_* = \bigcup_\alpha \Gamma_\alpha$, e sia $a \subseteq \Gamma_*$; per definizione esiste β tale che $a \subseteq \Gamma_\beta$, quindi per monotonicità $\Gamma(a) \subseteq \Gamma(\Gamma_\beta) = \Gamma_{\beta+1}$, ovvero $\Gamma(a) \subseteq \Gamma_*$, quindi Γ_* é Γ- chiuso.

Per induzione su α, se G é Γ-chiuso, allora $\Gamma_\alpha \subseteq G$:

- $\alpha = 0$, ovviamente $\Gamma_0 = \emptyset \subseteq G$;
- $\alpha = \beta + 1$, e $\Gamma_\beta \subseteq G$, allora $\Gamma(\Gamma_\beta) = \Gamma_{\beta+1} = \Gamma_\alpha \subseteq \Gamma(G) \subseteq G$;
- $\alpha = \lambda$ (ordinale limite) e $\forall \beta < \lambda . \Gamma_\beta \subseteq G$, allora, per ogni $a \in \Gamma_\lambda$, esiste $\beta < \lambda$ tale che $a \in \Gamma_\beta \subseteq G$, quindi $\Gamma_\lambda \subseteq G$.

Quindi, per ogni α ordinale, $\Gamma_\alpha \subseteq G$, da cui segue che $\Gamma_* \subseteq G$.

In altre parole Γ_* é la più piccola classe Γ-chiusa.

Questo fatto prova l'equivalenza delle due caratterizzazioni di Γ_*.

Proviamo che Γ_* é un punto fisso e, notando che ogni punto fisso é anche Γ-chiuso, questo implica che Γ_* é il minimo punto fisso.

Ora $\Gamma(\Gamma_*) \subseteq \Gamma_*$ perchè Γ_* é Γ-chiuso. Ma per monotonicità vale anche che $\Gamma(\Gamma(\Gamma_*)) \subseteq \Gamma(\Gamma_*)$, quindi $\Gamma(\Gamma_*)$ é Γ-chiuso, e, per minimalità di Γ_*, $\Gamma_* \subseteq \Gamma(\Gamma_*)$, ovvero Γ_* é Γ-corretto.

Quindi é il minimo punto fisso. □

Questo teorema ci fornisce anche due metodi per definire oggetti e per derivarne alcune proprietà:

Metodo 19 *Per provare che* $\Gamma_* \subseteq G$*, mostrare che* G *é* Γ*-chiuso.*

Metodo 20 (Induzione) *Per provare che* $\Gamma_* \subseteq G$*, mostrare che* $\Gamma(G \cup \Gamma_*) \subseteq G$.

Questi metodi sono la base formale che consente di generare le regole di induzione su una particolare struttura ed essi garantiscono la buona fondazione di una definizione induttiva.

Come già detto nell'introduzione, siamo interessati anche alla definizione duale, quella di massimo punto fisso, cui é naturalmente associato il principio di coinduzione.

Lemma 21 *Sia Γ un operatore monotono, e sia $\Gamma^* = \bigcup\{a \mid a \text{ é } \Gamma\text{-corretto}\}$.*

(1) Sia $a \subseteq \Gamma^*$, allora esiste un insieme b Γ-corretto tale che $a \subseteq b$.
(2) Sia $a \subseteq G$, con G Γ-corretto, allora esiste $b \subseteq G$ tale che $a \subseteq \Gamma(b)$.

Dimostrazione.

(1) Per ogni $c \in a$, $c \in \Gamma^*$, quindi esiste b_c tale che $c \in b_c \subseteq \Gamma(b_c)$, per definizione di Γ^*. Sia $b = \bigcup_{c\in a} b_c$, allora $a \subseteq b$ e, per monotonicità $b = \bigcup_{c\in a} b_c \subseteq \bigcup_{c\in a} \Gamma(b_c) \subseteq \Gamma(b)$, quindi b é Γ-corretto.
(2) Per ogni $c \in a$, $c \in G$, quindi, essendo G Γ-corretto, esiste $b_c \subseteq G$ tale che $c \in \Gamma(b_c)$. Sia $b = \bigcup_{c\in a} b_c$, allora $a \subseteq \Gamma(b)$ per monotonicità di Γ.

□

Teorema 22 (Massimo Punto Fisso) *Ogni operatore Γ che sia monotono, ammette un massimo punto fisso, denotato con Γ^*.*

Esso é caratterizzato in uno dei seguenti modi:

- $\Gamma^* = \bigcup\{a \mid a \text{ é } \Gamma\text{-corretto}\}$;
- Γ^* *é la massima classe Γ-corretta.*

Dimostrazione. Sia $\Gamma^* = \bigcup\{a \mid a \text{ é } \Gamma\text{-corretto}\}$ e sia $b \in \Gamma^*$, allora esiste a tale che $b \in a \subseteq \Gamma(a)$ per definizione di Γ^*, e $a \subseteq \Gamma^*$.

Quindi $\Gamma(a) \subseteq \Gamma(\Gamma^*)$ per monotonicità di Γ, ma

$$b \in a \subseteq \Gamma(a) \subseteq \Gamma(\Gamma^*)$$

ovvero $b \in \Gamma(\Gamma^*)$, in altre parole $\Gamma^* \subseteq \Gamma(\Gamma^*)$, ossia Γ^* é Γ-corretto.

Sia G una classe Γ-corretta: $G \subseteq \Gamma(G)$. Sia $b \in G$. Definiamo $a_0 = \{b\}$, $a_1 \subseteq G$ tale che $a_0 \subseteq \Gamma(a_1)$, e, in generale

$$a_{n+1} \subseteq G \quad \text{tale che} \quad a_n \subseteq \Gamma(a_{n+1}) \ .$$

Questi insiemi esistono in virtù del lemma precedente.

Sia $a = \bigcup_{n\in\mathbb{N}} a_n$; se $d \in a$, allora per un qualche n,

$$d \in a_n \subseteq \Gamma(a_{n+1}) \subseteq \Gamma(a) \ .$$

Questo significa che $a \subseteq \Gamma(a)$, quindi $a \subseteq \Gamma^*$. Ma $b \in a_0 \subseteq a$, quindi $b \in \Gamma^*$, da cui segue che $G \subseteq \Gamma^*$, quindi Γ^* é la massima classe Γ-corretta.

Ma per Γ-correttezza, $\Gamma^* \subseteq \Gamma(\Gamma^*)$; per monotonicità di Γ, $\Gamma(\Gamma^*) \subseteq \Gamma(\Gamma(\Gamma^*))$, quindi $\Gamma(\Gamma^*)$ é una classe Γ-corretta, e per massimalità di Γ^*, $\Gamma(\Gamma^*) \subseteq \Gamma^*$, ovvero Γ^* é Γ-chiusa, per cui Γ^* é un punto fisso e, per di più, il massimo. □

Come in precedenza, il teorema fornisce due metodi per definire nuovi oggetti e per analizzarne le proprietà.

Metodo 23 *Per provare che $G \subseteq \Gamma^*$, mostrare che $G \subseteq \Gamma(G)$.*

Metodo 24 (Coinduzione) *Per provare che $G \subseteq \Gamma^*$, mostrare che $G \subseteq \Gamma(G \cup \Gamma^*)$.*

Per dare un'idea di come questi metodi trovano applicazione, consideriamo un caso semplice: i numeri naturali.

Consideriamo l'operatore

$$\Gamma(a) = \{\emptyset\} \cup \{b \cup \{b\} \mid b \in a \text{ é un insieme}\} \ .$$

É immediato verificare che Γ é monotono.

In **ZFA**, dove abbiamo sviluppato la nostra teoria, consideriamo sia Γ_* che Γ^*.

- $\Gamma_* = \bigcup_\alpha \bigcup_{\beta<\alpha} \Gamma(\Gamma_\beta) = \omega$, ovvero il minimo punto fisso della trasformazione Γ é il primo ordinale limite, isomorfo all'insieme $\mathbb{N}$ dei numeri naturali.
- $\Gamma^* = \omega \cup \Omega$ [4]. Infatti, sia G un qualsiasi punto fisso per Γ, e sia $a_0 \in G$ non ben fondato, allora per una qualche $a_1 \in G$ non ben fondato, $a_0 = a_1 \cup \{a_1\}$. Continuando otteniamo a_2, a_3, ..., $a_n = a_{n+1} \cup \{a_{n+1}\}$, ...

  Quindi $\{a_0\}^* = \bigcup_n a_n$ é un insieme che contiene solo insiemi non ben fondati e che sia chiuso per transitività; Ω é l'unico insieme con questa caratteristica.

Provando ad istanziare i principi di induzione e coinduzione per il nostro particolare Γ otteniamo:

- Induzione:

  Per provare che $\omega \subseteq G$, mostrare che $\Gamma(G) \subseteq G$, ovvero $w \subseteq G$ se $\{\emptyset\} \cup \{b \cup \{b\} \mid b \in G\} \subseteq G$.

[4] Dove Ω é l'insieme soluzione dell'equazione $x = \{x\}$. Esso é ovviamente non ben fondato, ma per l'Assioma di Antifondazione esiste ed é univocamente determinato.

In forma di regola:

$$\dfrac{\begin{array}{c}[b \in G] \\ \vdots \\ \emptyset \in G \qquad b \cup \{b\} \in G\end{array}}{\omega \subseteq G}$$

che é la classica regola di induzione per i naturali nella scrittura propria della teoria degli insiemi.

- Coinduzione:
  Per provare che $G \subseteq \omega \cup \Omega$, mostrare che $G \subseteq \Gamma(G)$, ovvero $G \subseteq \omega \cup \Omega$ se $G \subseteq \{\emptyset\} \cup \{b \cup \{b\} \mid b \in G\}$.

La regola di induzione consente di provare proprietà che valgono per ω. Sia $G = \{x \mid \psi(x)\}$ dove ψ é una proprietà d'interesse; la regola d'induzione stabilisce che, se vale $\psi(0)$ e, se, supponendo che valga $\psi(x)$, vale $\psi(x+1)$, allora ψ vale per ogni $x \in \omega$.

La regola di coinduzione permette di costruire oggetti che ereditino proprietà da $\omega \cup \Omega$. Se G é un insieme contenente 0 e chiuso rispetto al successore, allora $G \subseteq \omega \cup \Omega$, quindi se ψ vale per ogni $x \in \omega \cup \Omega$, allora ψ vale per ogni $x \in G$.

2.5 Bisimulazione

Come abbiamo visto nell'introduzione, uno dei concetti chiave per avere una teoria della circolarità soddisfacente, é quello di bisimulazione.

Tuttavia il concetto di bisimulazione introdotto a proposito dell'Algebra dei Processi sembra essere molto più generale e flessibile degli analoghi visti nell'impianto di **ZFA**.

Tutti i concetti di bisimulazione visti hanno due punti in comune:

- la struttura formale;
- il fatto che sono introdotti per definire un concetto di uguaglianza.

Lo scopo di questa sezione consiste nel mostrare una formulazione alternativa [BM96,BM91], in apparenza più generale, ma equivalente, dell'Assioma di Antifondazione , sfruttando appieno le bisimulazioni tra insiemi.

Con questo strumento saremo in grado di definire su un modello di **ZFA**, ogni forma di bisimulazione, mostrando come il concetto di bisimulazione tra insiemi sia, in effetti, il più generale possibile.

Definizione 25 *Un* sistema (generale) di equazioni *é una tripla* $\varepsilon = \langle X, A; e\rangle$ *in cui* X *é un Insieme di incognite,* A *é un Insieme di atomi ed* $e\colon X \longrightarrow V_A[X]$.

Per definire cosa é la soluzione di un tale sistema, occorre definire il concetto di sostituzione.

Definizione 26 *Una* sostituzione *é una funzione* s *il cui dominio sia un Insieme di incognite. Una* operazione di sostituzione *é una operazione sub il cui dominio sia una classe di coppie* $\langle s, b\rangle$ *dove* s *é una sostituzione e* $b \in \mathcal{U} \cup V[\mathcal{U}]$ [5] *tale che soddisfi le seguenti condizioni:*

- *se* $x \in \mathrm{dom}(s)$, *allora* $sub(s, x) = s_x$
- *se* $x \in \mathcal{U} \setminus \mathrm{dom}(s)$, *allora* $sub(s, x) = x$
- *per ogni insieme* b, $sub(s, b) = \{sub(s, p) \mid p \in b\}$.

Teorema 27 (Esistenza ed Unicità di *sub***)** *Esiste una unica operazione sub che sia una operazione di sostituzione e che sia definita per ogni coppia* $\langle s, b\rangle$ *in cui* s *sia una sostituzione e* $b \in \mathcal{U} \cup V[\mathcal{U}]$.

Dimostrazione.

(1) Esistenza

Definiamo $sub(s, b) = c$ se s é una funzione con dominio un Insieme di incognite per cui valga una delle seguenti condizioni:

- $b \in \mathrm{dom}(s)$ e $c = s_b$;
- $b \in \mathcal{U} \setminus \mathrm{dom}(s)$ e $c = b$;
- $b \in V[\mathcal{U}]$ e, detti

$$X = (\{b\} \cup \mathrm{range}(s))^+ \setminus \mathcal{A} \ ,$$

$$A = (\{b\} \cup \mathrm{range}(s))^+ \cap \mathcal{A} \ ,$$

$$\varepsilon' = \langle X, A; e'\rangle$$

con

$$e'_z = \{s_x \mid x \in z \cap \mathrm{dom}(s)\} \cup \{x \mid x \in z \cap (A \setminus \mathrm{dom}(s))\} \cup (z \cap X) \ ,$$

e $c = sol_b$ dove sol é la soluzione di ε'.

[5] Indichiamo con $\mathcal{U}$ la classe unione di tutte le incognite e di tutti gli atomi e con $\mathcal{A}$ la classe di tutti gli atomi.

Per definizione, *sub* soddisfa le prime due condizioni per essere una sostituzione. Per quanto riguarda la terza, sia b un insieme, e siano ε_b e sol_b i corrispondenti insieme di equazioni e soluzione come dalla definizione di *sub*.

Notiamo che, se $b' \in b \setminus \mathcal{A}$, $\varepsilon_{b'}$ é un sottosistema di ε_b per cui $sol_{b'}(b') = sol_b(b') \in sol_b(b)$.

Quindi $sub(s,b) = sol_b(b) = \{s_x \mid x \in b \cap \mathrm{dom}(s)\} \cup \{x \mid x \in b \cap (A \setminus \mathrm{dom}(s))\} \cup \{sub(s,b') \mid b' \in b \setminus A\}$.

Se $x \in b \cap \mathrm{dom}(s)$, $sub(s,x) = s_x$, e, se $x \in b \cap (A \setminus \mathrm{dom}(s)) \subseteq \mathcal{U} \setminus \mathrm{dom}(s)$, allora $sub(s,x) = x$.

Quindi $sub(s,b) = \{sub(s,p) \mid p \in b\}$. Ovvero *sub* é una operazione di sostituzione.

(2) Unicità

Sia sub' una operazione di sostituzione definita per ogni coppia $\langle s, b\rangle$.

Fissando s, si definisce

$$R = \{\langle sub(s,b), sub'(s,b)\rangle \mid b \in \mathcal{U} \cup V[\mathcal{U}]\} \ .$$

La relazione R é una bisimulazione tra insiemi:

- sia $z \in \mathcal{U} \cap sub(s,b)$, ma, essendo b un insieme, z é della forma $sub(s,x)$ per un qualche $x \in \mathcal{U} \cap b$; e $z = sub(s,x) = s_x = sub'(s,x) \in sub'(s,b)$.

  In modo simmetrico si verifica l'altra proprietà per gli atomi.
- sia $c \in sub(s,b)$ un insieme; se $b \in \mathcal{A}$ allora $c \in s_b = sub'(s,b)$.

  Se b é un insieme, allora $c = sub(s,p)$ per un qualche $p \in b$, e $\langle sub(s,p), sub'(s,p)\rangle \in R$.

Quindi, per ogni insieme b, $sub(s,b) = sub'(s,b)$, e, per il Teorema di Estensionalità Forte, $sub = sub'$.

□

Per comodità di notazione scriviamo $b[s]$ invece di $sub(s,b)$.

La nozione di sostituzione consente di definire cosa sia la soluzione di un sistema generale di equazioni.

Definizione 28 *Sia $\varepsilon = \langle X, A; e\rangle$ un sistema generale di equazioni; una* soluzione *di ε é una funzione s con dominio X tale che, per ogni $x \in X$. $s_x = e_x[s]$.*

Il risultato principale riguardante i sistemi generali di equazioni é noto in letteratura come *General Solution Lemma* [BM96,BM91]. La sua dimostrazione é una conseguenza del lemma seguente.

Lemma 29 *Sia $\varepsilon = \langle X, A; e\rangle$ un sistema generale di equazioni; esiste un sistema semplice di equazioni $\varepsilon^b = \langle Y, A; e'\rangle$ con $X \subseteq Y$ tale che:*

- *se s é una soluzione di ε allora s si estende alla soluzione s' per ε^b.*
- *se s' é la soluzione di ε^b ed $s = s' \restriction X$ (la restrizione di s' ad X) allora s é soluzione di ε.*

Dimostrazione. Sia

$$Y = (X \cup \bigcup_{x \in X} (e_x)^+)) \setminus A \ .$$

Se $x \in X$, definiamo $e'_x = e_x$, notando che $e'_x \subseteq Y \cup A$.

Se $x \in Y \setminus X$, definiamo $e'_x = x$, notando che $e'_x \subseteq Y \cup A$.

In questo modo abbiamo determinato ε^b.

(1) s soluzione di $\varepsilon \Rightarrow s$ si estende ad s', soluzione di ε^b.

Definiamo s' come $s'_y = y[s]$. Evidentemente s' estende s poichè, per ogni $x \in X$, $s'_x = x[s] = s_x$.

Occorre provare che s' é soluzione di ε^b.

Poichè $a \cap X = \emptyset$, per ogni $a \in A$, $a[s] = a = a[s']$.

La definizione di sostituzione e la transitività [6] di Y implicano che, per ogni $y \in Y \setminus X$,

$$s'_y = y[s] = \{z[s] \mid z \in y\} \cup \{y \cap A\} = \{s'_z \mid z \in y\} \cup \{y \cap A\} = e'_y[s'] \ .$$

Per $x \in X$, $s'_x = s_x = e_x[s]$, quindi

$$\begin{aligned} s'_x &= \{z[s] \mid z \in e_x\} = \\ &= \{z[s] \mid z \in e_x \cap (Y \setminus X)\} \cup \{s_z \mid z \in e_x \cap X\} \cup (e_x \cap A) = \\ &= \{s'_z \mid z \in e_x \cap (Y \setminus X\} \cup \{s'_z \mid z \in e_x \cap X\} \cup (e'_x \cap A) = e'_x[s'] \ . \end{aligned}$$

Da cui segue, per definizione, che s' é (l'unica) soluzione di ε^b.

(2) s' soluzione di ε^b ed $s = s' \restriction X \Rightarrow s$ soluzione di ε.

Vogliamo innanzitutto provare che, per ogni $y \in Y$, $s'_y = y[s]$.

Sia $R = \{\langle s'_y, y[s]\rangle \mid y \in Y\}$; questa relazione é una bisimulazione tra insiemi.

Supponiamo che $\langle s'_y, y[s]\rangle \in R$. Sia $z \in \mathcal{U} \cap s'_y$, per definizione di soluzione di un sistema semplice di equazioni, $z \in e_y \cap A = y \cap A$. Ma $X \cap A = \emptyset$, implica che $z = z[s] \in y[s]$.

Nell'altro verso, supponiamo che $z \in y[s] \cap \mathcal{U}$. Poichè s prende insiemi come valori, $p[s] \in \mathcal{U}$ é possibile solamente quando $p \notin \mathrm{dom}(s)$. Ma, dato che $z = z[s]$, $z \notin \mathrm{dom}(s)$, quindi $z \in A$, ovvero $z \in s'_y$.

[6] Un insieme A si dice transitivo se $x \in y \in A$ implica $x \in A$.

Supponiamo che $c \in s'_y$ e che c sia un insieme. Questo implica che $c = s'_v$ per un qualche $v \in Y$. Ma $\langle c, v[s]\rangle \in R$ quindi ancora una volta riusciamo a soddisfare le condizioni sulla bisimulazione tra insiemi.

Infine supponiamo che $c \in y[s]$ e che c sia un insieme. Per le condizioni nella definizione di sostituzione, $c = v[s]$ con $v \in y$. Essendo v un insieme, ed essendo Y transitivo, $v \in Y$, quindi $\langle s'_v, v[s]\rangle \in R$.

Ovvero R é una bisimulazione tra insiemi, e per estensionalità forte, $s'_y = y[s]$ per ogni $y \in Y$.

Questo fatto ci consente di provare che s é soluzione di ε: poichè $s_x = s'_x = e'_x[s'] = e_x[s']$, per ogni $x \in X$,

$$\begin{aligned} s_x &= \{s'_z \mid z \in e_x \setminus A\} \cup (e_x \cap A) = \\ &= \{s'_z \mid z \in e_x \cap (Y \setminus X)\} \cup \{s'_z \mid z \in e_x \cap X\} \cup (e_x \cap A) = \\ &= \{z[s] \mid z \in e_x \cap (Y \setminus X)\} \cup \{z[s] \mid z \in e_x \cap (X \cup A)\} = \\ &= e_x[s] \ . \end{aligned}$$

□

Teorema 30 (General Solution Lemma) *Ogni sistema generale di equazioni ε ammette un'unica soluzione s. Inoltre l'insieme soluzione di ε é un sottoinsieme di $V[A]$, dove A é l'insieme degli atomi di ε.*

Dimostrazione. Conseguenza immediata del lemma precedente e del Flat Solution Lemma. □

Il risultato che avevamo preannunciato all'inizio di questa sezione, é il seguente:

Teorema 31 ***AFA*** *(l'Assioma di Antifondazione) é equivalente all'asserzione che ogni sistema generale di equazioni ammette un'unica soluzione.*

Dimostrazione. Conseguenza immediata del General Solution Lemma e della prova del lemma 29. □

Come ultimo risultato della nostra analisi teorica di **ZFA**, presentiamo una proposizione che utilizzeremo per mostrare come si possa risolvere il paradosso dell'ipergioco, ma che riveste un significato autonomo.

Definizione 32 *Un insieme a é detto* riflessivo *se $a \in a$.*

Proposizione 33 (Difference Lemma) *Sia V un insieme transitivo e sia $b = V \setminus \{v\}$, allora $b \notin V$.*

Dimostrazione. Se V non é riflessivo, allora $b = V$ e, per definizione di non riflessivo, $b \notin V$.

Supponiamo che V sia riflessivo: se $b \in V$ (ipotesi d'assurdo), allora $b \in V \setminus \{V\} = b$ poichè $V \notin b$, e quindi $V \neq b$.

Quindi anche b é riflessivo.

Sia $R = \{\langle V, b\rangle\} \cup \{\langle a, a\rangle \mid a \in b\}$. Proviamo che R é una bisimulazione tra insiemi:

- per ogni $a \in V$ esiste $c \in b$ tale che $\langle a, c\rangle \in R$; se $a = V$ allora $c = b$, altrimenti $c = a$.
- per ogni $a \in b$ esiste $c \in V$ tale che $\langle a, c\rangle \in R$; poichè V é transitivo, $c = a$.
- per definizione di b, b e V hanno lo stesso insieme di atomi.

Per il Teorema di Estensionalità Forte, $b = V$.

Ma $V \in V$ per ipotesi e $V \notin b$ per ipotesi d'assurdo, quindi $b \neq V$. Abbiamo pertanto una contraddizione, quindi $b \notin V$. $\square$

3 Applicazioni

Nell'introduzione di questo lavoro, abbiamo presentato alcuni esempi ed alcuni paradossi inerenti il concetto di circolarità.

Avendo sviluppato l'apparato teorico, é tempo di presentare una formalizzazione degli esempi, mostrando come la teoria **ZFA** sia sufficentemente potente per modellarli tutti, ed in modo *naturale*.

Inoltre intendiamo mostrare il modo in cui **ZFA** renda i paradossi, ovvero come essi siano costruzioni impossibili, o con un significato diverso, talora più interessante, della semplice inconsistenza che, in apparenza, essi presuppongono nell'idea di circolarità.

Infine mostreremo una costruzione particolarmente notevole in quanto presenta applicazioni in logica, che illustra come alcune nozioni che coincidono in **ZF** diano luogo a strutture molto differenti in **ZFA**: parleremo degli insiemi ereditariamente finiti.

3.1 Esempi Introduttivi

3.1.1 Sequenze

Nell'introduzione abbiamo presentato, intuitivamente, il concetto di lista e di sequenza, evidenziando come una teoria della circolarità accettabile debba essere in grado di rappresentare appropriatamente entrambe le strutture dati.

In **ZFA**, ciò é possibile, e gli strumenti sviluppati nella parte teorica consentono di dare un modello *naturale* per queste strutture dati.

Sia A un insieme; vogliamo costruire due nuovi insiemi L ed S, che rappresentino le liste e le sequenze sull'alfabeto A.

A tal fine, definiamo l'operatore $\Gamma(c) = A \times c$; esso é evidentemente, monotono.

Notando che $\Gamma(\emptyset) = \emptyset$, il minimo punto fisso per Γ é l'insieme vuoto. Tuttavia Γ^* (il massimo punto fisso per Γ) é non banale:

$$\Gamma^* = \bigcup\{a \mid a \subseteq \Gamma(a)\} = \bigcup\{a \subseteq A \times a\} \ .$$

Consideriamo la mappa ψ: Sequenze $\longrightarrow \Gamma^*$:

$$\psi(\mathbf{Nil}) = \emptyset \text{ e } \psi(\mathbf{Cons}\ \alpha\ x) = \langle \alpha, \psi(x) \rangle \ .$$

Essa é totale e biiettiva, infatti

- se σ é una sequenza allora $\sigma = \mathbf{Nil}$ oppure $\sigma = \mathbf{Cons}\ \alpha\ \tau$ con $\alpha \in A$ e τ sequenza, quindi ψ é totale.
- se $\sigma = \tau$ allora $\sigma = \tau = \mathbf{Nil}$ e $\psi(\sigma) = \psi(\tau)$, oppure $\sigma = \mathbf{Cons}\ \alpha\ \sigma'$ e $\tau = \mathbf{Cons}\ \alpha\ \tau'$; per ipotesi $\psi(\sigma') = \psi(\tau')$, quindi anche $\psi(\sigma) = \psi(\tau)$. Ovvero ψ é iniettiva.
- se $\langle \alpha, \beta \rangle \in \Gamma^*$ allora, per ipotesi, esiste σ tale che $\psi(\sigma) = \beta$ e quindi $\psi(\mathbf{Cons}\ \alpha\ \sigma) = \langle \alpha, \beta \rangle$; inoltre $\emptyset \in \Gamma^*$ e $\psi(\mathbf{Nil}) = \emptyset$, provando la suriettività di ψ.

Quindi Γ^* é un modello in **ZFA** per le sequenze.

Consideriamo l'equazione $\psi(x) = \psi(\mathbf{Cons}\ \alpha\ x)$: essa ammette soluzione, infatti $x = \langle \alpha, x \rangle$ é un sistema generale di equazioni e pertanto ammette una ed una sola soluzione; la sequenza costituita da elementi α.

Banalmente otteniamo un Principio di Coinduzione ed uno di Coricorsione:

Principio 34 (Coinduzione) *$Z \subseteq \Gamma^*$ se $Z \subseteq A \times Z$.*

Principio 35 (Coricorsione) *Sia C un insieme e siano $G\colon C \longrightarrow A$ ed $H\colon C \longrightarrow C$ due funzioni, allora esiste una unica funzione $F\colon C \longrightarrow \Gamma^*$ tale che, per ogni $c \in C$,*

$$F(c) = \langle G(c), F(H(c)) \rangle \ .$$

Dimostrazione. Sia X un insieme di incognite in corrispondenza biunivoca con C. Sia $\varepsilon = \langle X, A; e \rangle$ un sistema generale di equazioni con

$$e_{x_c} = \langle G(c), x_{H(c)} \rangle \ .$$

Questo sistema ammette una unica soluzione s. Definiamo $F(c) = s_{x_c}$. Ma

$$s_{x_c} = \langle G(c), x_{H(c)} \rangle[s] = \langle G(c), F(H(c)) \rangle \ ,$$

ovvero $F(c) = \langle G(c), F(H(c)) \rangle$. $\square$

In questo modo abbiamo uno strumento per definire funzioni su sequenze: ad esempio, $\mathrm{map}(f, s) = \langle f(\mathrm{head}(s)), \mathrm{map}(f, \mathrm{tail}(s)) \rangle$ risulta ben definita per il Principio di Coricorsione.

Come risultato, possiamo dire che la nostra teoria permette di codificare il concetto di sequenza in modo naturale.

Consideriamo l'operatore Γ' tale che $\Gamma'(c) = (A \times (c \cup \{\emptyset\})) \cup \{\emptyset\}$.

É immediato verificare che il minimo punto fisso di Γ' esiste (per monotonicità) ed é non banale, così come il massimo punto fisso.

Definendo ψ: Liste $\longrightarrow \Gamma'_*$ come

$$\psi(\mathbf{Nil}) = \emptyset \quad \text{e} \quad \psi(\mathbf{Cons}\ \alpha\ x) = \langle \alpha, \psi(x) \rangle$$

e ripetendo il ragionamento fatto in precedenza riguardo l'interpretazione per le sequenze, otteniamo una caratterizzazione per le liste sull'alfabeto A. In modo analogo a quanto visto per le sequenze, possiamo introdurre un Principio di Induzione ed un Principio di Ricorsione.

Più interessante é analizzare Γ'^*: infatti esso coincide con Γ^*, se $A \neq \emptyset$.

Proposizione 36 $\Gamma'^* = \Gamma^*$.

Dimostrazione.

(1) $\Gamma^* \subseteq \Gamma'^*$ infatti, usando il Principio di Coinduzione per Γ', abbiamo che

$$\begin{aligned} \Gamma^* \subseteq \Gamma'(\Gamma^*) &= (A \times (\Gamma^* \cup \{\emptyset\})) \cup \{\emptyset\} \\ &= (A \times \Gamma^*) \cup \{\emptyset\} \\ &= \Gamma^* \cup \{\emptyset\} \\ &= \Gamma^* \end{aligned}$$

poichè $\emptyset \in \Gamma^*$.

(2) $\Gamma'^* \subseteq \Gamma^*$, infatti Γ'^* é Γ-corretto. Per provare questo mostriamo che $\Gamma'^* = A \times \Gamma'^*$.

Sia

$$R = \{\langle \alpha, \langle \beta, \alpha \rangle \rangle \mid \beta \in A, \alpha \in \Gamma'^*\}\ .$$

Questa é una bisimulazione tra Γ'^* e $A \times \Gamma'^*$:

- $\forall \alpha \in \Gamma'^*.\ \exists \beta \in A \times \Gamma'^*.\ \alpha\ R\ \beta$, basta prendere $\beta = \langle a, \alpha \rangle$ con $a \in A$.
- $\forall \alpha \in A \times \Gamma'^*.\ \exists \beta \in \Gamma'^*.\ \beta\ R\ \alpha$, basta prendere $\beta = \gamma$, dove $\alpha = \langle a, \gamma \rangle$ con $a \in A$.
- Gli atomi in Γ'^* sono in A così come in $A \times \Gamma'^*$.

Sapendo che $A \times \Gamma'^* = \Gamma'^*$, per il Principio di Coinduzione su Γ, notando che $\Gamma'^* \subseteq A \times \Gamma'^* = \Gamma(\Gamma'^*)$, deduciamo che $\Gamma'^* \subseteq \Gamma^*$.

□

Quindi esiste modo di caratterizzare le liste e le sequenze come minimo e massimo punto fisso del medesimo operatore, che attraverso le opportune interpretazioni, codifica esattamente la usuale dichiarazione di queste strutture dati.

In modo analogo possono essere modellate tutte le strutture dati definite per induzione, generando parallelamente le costrutture come massimi punti fissi della medesima trasformazione.

3.1.2 Chiusure

Nell'introduzione abbiamo visto come il concetto algebrico di chiusura sia in relazione con la circolarità. Come esempio abbiamo usato la chiusura riflessiva e transitiva di una relazione.

Tale esempio é formalizzabile in maniera semplice all'interno della nostra teoria. Sia R una relazione, consideriamo l'operatore Γ definito come:

$$\begin{aligned}\Gamma(c) = &\{\langle a, a\rangle \mid \exists b.\ \langle a, b\rangle \in c \vee \langle b, a\rangle \in c\} \cup \\ &\{\langle a, b\rangle \mid \exists d.\ \langle a, d\rangle \in c \wedge \langle d, b\rangle \in R\} \cup R\ .\end{aligned}$$

É immediato verificare la monotonia di Γ.

Consideriamo Γ_*, il minimo punto fisso di Γ:

- Γ_* é una relazione poichè ogni suo elemento é una coppia; inoltre $R \subseteq \Gamma_*$ poichè $\Gamma(\emptyset) \subseteq \Gamma_*$, per la caratterizzazione di quest'ultimo e $\Gamma(\emptyset) = R$.
- Γ_* é una relazione riflessiva poichè $\Gamma(\Gamma_*) = \Gamma_*$ e, in particolare questo significa che

  $$\forall a.\ (\exists b.\ \langle a, b\rangle \in \Gamma_* \vee \langle b, a\rangle \in \Gamma_*) \rightarrow \langle a, a\rangle \in \Gamma_*\ ,$$

  per definizione di Γ.
- per gli stessi motivi, Γ_* é una relazione transitiva.
- Sia Q una relazione riflessiva, transitiva, che contenga R: $\Gamma(Q) = Q \cup Q' \cup R$, con $Q' \subseteq R$, per definizione di Γ, ovvero $\Gamma(Q) = Q$; ma Γ_* é il minimo insieme che sia un punto fisso per Γ, quindi $\Gamma_* \subseteq Q$.

Tutto ciò comporta che Γ_* é la chiusura riflessiva e transitiva di R.

Notiamo come il fenomeno dell'impredicatività venga a coincidere, nella struttura della nostra teoria, con il concetto di insieme non ben fondato, e che, mediante una trattazione appropriata di questi insiemi, sia possibile utilizzare

e circoscrivere opportunamente il fenomeno in virtù dei risultati che abbiamo sviluppato.

Un'altra richiesta che abbiamo introdotto quando abbiamo parlato di chiusure, é stato il concetto di costruzione duale. Vediamo come tale costruzione sia il naturale sviluppo della nostra teoria applicata all'esempio della cochiusura riflessivo-transitiva; sia Δ l'operatore definito come:

$$\begin{aligned}\Delta(c) = &\{\langle a,a\rangle \mid \langle a,a\rangle \in R\} \cup \\ &\{\langle a,b\rangle \mid \langle a,b\rangle \in R \wedge \exists d \in c.\ \langle a,d\rangle \in c \wedge \langle d,b\rangle \in c\}\ .\end{aligned}$$

Anche in questo caso, la monotonia di Δ é evidente.

Consideriamo Δ^*, il massimo punto fisso di Δ:

- poichè $\forall c.\ \Delta(c) \subseteq R$, $\Delta^* \subseteq R$.
- per definizione di Δ, ed essendo $\Delta^* = \Delta(\Delta^*)$, Δ^* é una relazione riflessiva e transitiva.
- per massimalità di Δ^*, ogni altra relazione riflessiva e transitiva che sia contenuta in R, é contenuta in Δ^*.

Quindi Δ^* é, secondo la nostra definizione, la cochiusura riflessivo-transitiva di R.

L'operazione di cochiusura può essere efficacemente usata per definire nuovi oggetti. Sia R una relazione, Γ un operatore monotono, Γ^* la cochiusura di R rispetto a Γ, e Q un sottoinsieme di Γ^*. Un modo *naturale* per definire un nuovo oggetto, é considerare il minimo insieme Q^* che contenga Q e che sia Γ-corretto.

La naturalità di questa operazione deriva da alcune costruzioni similari che vengono usate in Topologia [Csá78], specialmente quando si parla di compattificazione.

Per garantire l'esistenza e l'unicità di tale Q^* é necessario richiedere qualche condizione aggiuntiva sull'operatore Γ.

Il seguente sviluppo teorico consente di identificare una condizione sufficente, di vasta applicabilità, per garantire una buona definizione di un tale Q^*.

Definizione 37 *Un operatore monotono* Γ commuta con intersezioni binarie *se, per ogni insieme* a *e* b, $\Gamma(a \cap b) \subseteq \Gamma(a) \cap \Gamma(b)$.

Un operatore monotono Γ commuta con tutte le intersezioni *se, per ogni* b, $\Gamma(\bigcap b) = \bigcap_{c \in b} \Gamma(c)$.

Proposizione 38 *Esistono operatori monotoni che non commutano con intersezioni binarie.*

Dimostrazione. Sia Γ definito come

$$\Gamma(b) = \begin{cases} \emptyset & \text{se } b \subseteq \{\emptyset\} \\ b & \text{altrimenti} \end{cases} .$$

Banalmente si verifica che Γ é monotono.

Siano $a = \{\emptyset, 1\}$ e $b = \{\emptyset, 2\}$:

$$\Gamma(a \cap b) = \Gamma(\{\emptyset\}) = \emptyset \ ,$$

ma

$$\Gamma(a) \cap \Gamma(b) = \{\emptyset, 1\} \cap \{\emptyset, 2\} = \{\emptyset\} \ .$$

□

Corollario 39 *Esistono operatori monotoni che non commutano con tutte le intersezioni.*

Notiamo, per inciso, che tutti gli operatori presentati come esempio di monotonia quando si é introdotto il concetto di punto fisso, commutano con tutte le intersezioni.

Proposizione 40 *Se Γ commuta con tutte le intersezioni allora l'intersezione di una famiglia di insiemi Γ-corretti, é Γ-corretta.*

Dimostrazione. Sia c una famiglia di insiemi Γ-corretti:

$$\bigcap_{b \in c} b \subseteq \bigcap_{b \in c} \Gamma(b) = \Gamma(\bigcap_{b \in c} b) \ .$$

□

Lemma 41 *Se Γ commuta con tutte le intersezioni e $a \subseteq \Gamma^*$, allora esiste un insieme b minimalmente Γ-corretto tale che $a \subseteq b$.*

Dimostrazione. Sia $a \subseteq \Gamma^*$, allora, dal Teorema di Massimo Punto Fisso, sappiamo che esiste un insieme b Γ-corretto tale che $a \subseteq b$.

Sia $c = \bigcap\{b' \subseteq b \mid b' \text{ é } \Gamma\text{-corretto e } a \subseteq b'\}$.

Ovviamente, $a \subseteq c$; per la proposizione precedente, c é Γ-corretto. Sia d un insieme Γ-corretto con $a \subseteq d$. Ma questo significa che $d \cap c$ é Γ-corretto, e, per definizione di c, $c \subseteq d \cap c$, ovvero $c \subseteq d$. $\Box$

Definizione 42 *Sia* Γ *un operatore che commuti con tutte le intersezioni, e sia* $a \subseteq \Gamma^*$*; un insieme* b *é la* Γ-chiusura *di* a *se* b *é* Γ*-corretto,* $a \subseteq b$ *ed é il minimo insieme con queste proprietà.*

In virtù del lemma precedente, la definizione di Γ-chiusura é ben data, ovvero identifica sempre ed in modo univoco un oggetto.

In sintesi, una condizione sufficente per garantire l'esistenza della Γ-chiusura di un insieme a, é data dal fatto che Γ commuti con tutte le intersezioni. Inoltre tale condizione é vera per molti degli operatori monotoni che ricorrono nella pratica.

3.1.3 Auto-Applicazione

Nell'introduzione abbiamo visto come il concetto di auto-applicazione, che, naturalmente, ricade sotto il dominio di una teoria della circolarità, sia modellabile attraverso il λ-Calcolo [Bar84], e la Logica Combinatoria [HS86,CF58].

Per semplificare l'esposizione, ci concentreremo sulla Logica Combinatoria (in sigla **CL**), mostrando come i concetti di *convergenza* e *divergenza* di cui accennato nell'introduzione, ed i cui corrispettivi formali sono in relazione alle forme normali per un termine, abbiano una naturale caratterizzazione in **ZFA**.

In questa sezione mostreremo come sia possibile immergere la Logica Combinatoria in **ZFA**, seguendo l'idea intuitiva che un termine denota un valore dato dalla sua forma normale.

Mostreremo che tale immersione fornisce una rappresentazione elementare per il concetto di uguaglianza in **CL**, per la nozione di forma normale, di termine fortemente normalizzabile e di termine insolubile.

Osservando la rappresentazione fornita, avremo un modello per **CL** che mostra come codificare in generale i requisiti di cui abbiamo fatto richiesta nella parte introduttiva di questo lavoro.

L'idea intuitiva che intendiamo perseguire per rappresentare un termine di **CL** come un insieme in **ZFA** é la seguente: un termine che sia in forma normale denota un valore, mentre un termine che non sia in forma normale, denota l'insieme dei termini a cui può essere ridotto. Formalmente:

Definizione 43 *Sia t un termine, la* rappresentazione *di t in* ***ZFA*** *é*

$$\mathrm{rep}(t) = \begin{cases} \{a_t\} & \textit{se } t \textit{ é una forma normale} \\ \{\mathrm{rep}(s) \mid t \xrightarrow{+} s & \textit{altrimenti} \end{cases}$$

dove a_t é un atomo e $t \not\equiv s$ implica $a_t \neq a_s$ e la relazione $\xrightarrow{+}$ é la chiusura transitiva di $\longrightarrow$, la riduzione in un passo di termini:

$$\mathrm{S}\ x\ y\ z \longrightarrow x\ z\ (y\ z) \quad \mathrm{K}\ x\ y \longrightarrow x$$

$$\frac{x \longrightarrow y}{x\ z \longrightarrow y\ z} \qquad \frac{x \longrightarrow y}{z\ x \longrightarrow z\ y}$$

É immediato verificare che, in **ZFA**, per ogni termine t, $\mathrm{rep}(t)$ é un insieme (non necessariamente ben fondato) ed é univocamente determinato.

Per mostrare che l'immagine di rep é un modello per **CL**, é necessario provare l'esistenza di una rappresentazione che per $\overset{\mathrm{CL}}{=}$.

Proposizione 44 *Siano t ed s due termini:*

$$t \overset{\mathrm{CL}}{=} s$$

se e solo se

$$\mathrm{rep}(t) \cap \mathrm{rep}(s) \neq \emptyset \vee \mathrm{rep}(t) \in \mathrm{rep}(s) \vee \mathrm{rep}(s) \in \mathrm{rep}(t) \ .$$

Dimostrazione.

- Per il Teorema di Church-Rosser, se $t \overset{\mathrm{CL}}{=} s$, allora esiste u tale che $t \xrightarrow{*} u$ e $s \xrightarrow{*} u$.

  Se $t \equiv u$ e $s \equiv u$ allora $t \equiv s$ e $\mathrm{rep}(t) \cap \mathrm{rep}(s) = \mathrm{rep}(t)$, ma, per definizione, per ogni t, $\mathrm{rep}(t) \neq \emptyset$.

  Se $t \equiv u$ e $s \not\equiv u$ allora $s \xrightarrow{+} t$ ed s non é una forma normale, quindi $\mathrm{rep}(t) \in \mathrm{rep}(s)$.

  Se $t \not\equiv u$ e $s \equiv u$ allora $t \xrightarrow{+} s$ e t non é una forma normale, quindi $\mathrm{rep}(s) \in \mathrm{rep}(t)$.

  Se $t \not\equiv u$ e $s \not\equiv u$ allora $t \xrightarrow{+} u$, $s \xrightarrow{+} u$ e t ed s non sono forme normali, quindi $\mathrm{rep}(u) \in \mathrm{rep}(t)$ e $\mathrm{rep}(u) \in \mathrm{rep}(s)$, ovvero $\mathrm{rep}(u) \in \mathrm{rep}(t) \cap \mathrm{rep}(s)$.
- Se vale $\mathrm{rep}(t) \in \mathrm{rep}(s)$ allora, per definizione di rep, s non é una forma normale, avendo un insieme come elemento, quindi $s \xrightarrow{+} t$, ovvero $s \overset{\mathrm{CL}}{=} t$.

  Analogamente, se $\mathrm{rep}(s) \in \mathrm{rep}(t)$, si vede che $t \overset{\mathrm{CL}}{=} s$.

Sia perciò $\mathrm{rep}(t) \cap \mathrm{rep}(s) \neq \emptyset$ e $\mathrm{rep}(t) \notin \mathrm{rep}(s)$ e $\mathrm{rep}(s) \notin \mathrm{rep}(t)$; poichè $\mathrm{rep}(t) \cap \mathrm{rep}(s) \neq \emptyset$, esiste $x \in \mathrm{rep}(t)$ e $x \in \mathrm{rep}(s)$.

Se x é un insieme allora nè t, nè s sono forme normali, per cui $x \equiv \mathrm{rep}(u)$ per un certo u e $t \xrightarrow{+} u$ e $s \xrightarrow{+} u$, quindi, per definizione segue che $t \overset{\mathrm{CL}}{=} s$.

Se x non è un insieme allora é un atomo, e, per definizione di rep, é della forma a_u per un certo termine u in forma normale.

Ma questo vuol dire che t ed s devono necessariamente essere in forma normale, poichè un atomo é elemento di $\mathrm{rep}(x)$ se e solo se $\mathrm{rep}(x) = \{a_x\}$. In altre parole $a_u \in \{a_t\}$ e $a_u \in \{a_s\}$, ovvero $a_t = a_s$. Quindi $t \equiv s$, cioé $t \overset{\mathrm{CL}}{=} s$.

□

La proposizione appena provata mostra che $\overset{\mathrm{CL}}{=}$ é rappresentata fedelmente dalla relazione

$$\{\langle x, y\rangle \mid \{x, y\} \subseteq \mathrm{range(rep)} \wedge (x \cap y \neq \emptyset \vee x \in y \vee y \in x)\} \ .$$

La rappresentazione prescelta cattura in maniera naturale i concetti di termine fortemente normalizzabile, di termine normalizzabile e di termine insolubile.

Lemma 45 *Il termine t é fortemente normalizzabile se e solo se* $\mathrm{rep}(t)$ *é ben fondato.*

Dimostrazione.

- Se t é fortemente normalizzabile allora ogni possibile riduzione di t é finita. Formalmente, non esiste s tale che $t \xrightarrow{*} s$ ed $s \xrightarrow{+} s$.

  Quindi, per definizione di insieme ben fondato, $\mathrm{rep}(t)$ é ben fondato.
- Se t non é fortemente normalizzabile, esiste s tale che $t \xrightarrow{*} s$ ed $s \xrightarrow{+} s$. Quindi $\mathrm{rep}(s)$ non é ben fondato, essendo un insieme riflessivo. Ma $\mathrm{rep}(s) \in \mathrm{rep}(t)$ per definizione, quindi $\mathrm{rep}(t)$ non é ben fondato.

□

Definizione 46 *Sia t un termine, indichiamo con* $\mathrm{Base}(t)$ *l'insieme degli atomi presenti in* $\mathrm{rep}(t)$ *ad un qualsiasi livello di innestamento.*

Lemma 47 *Il termine t non ammette forma normale se e solo se* $\mathrm{Base}(t) = \emptyset$.

Dimostrazione. Per costruzione $\mathrm{Base}(t) \subseteq \{a_u \mid u \text{ é una forma normale}\}$.

Quindi $\mathrm{Base}(t) = \emptyset$ implica che t non é una forma normale e $\{a_u\} \notin \mathrm{rep}(t)$ per ogni u, ovvero $t \xrightarrow{+} u$, con u forma normale, non vale. Quindi t non ammette forma normale.

Viceversa se t non ammette forma normale, $\mathrm{rep}(t) = \{\mathrm{rep}(s) \mid t \xrightarrow{+} s\}$ e nessun s é una forma normale, quindi per nessun s, $\mathrm{rep}(s) = \{a_s\}$.

Notando che $\mathrm{Base}(t) = \bigcup_{\mathrm{rep}(s)\in\mathrm{rep}(t)} \mathrm{Base}(s)$, per $\in$-induzione, $\mathrm{Base}(t) = \emptyset$. □

Corollario 48 *Per ogni termine t,* $|\mathrm{Base}(t)| \leq 1$.

Dimostrazione. Se t non ammette forma normale, $\mathrm{Base}(t) = \emptyset$ e quindi $|\mathrm{Base}(t)| = 0$.

Se t ammette forma normale s, ma t non é una forma normale, allora $\mathrm{rep}(s) = \{a_s\} \in \mathrm{rep}(t)$.

Per assurdo, se $|\mathrm{Base}(t)| > 1$ allora esiste $u \not\equiv s$ tale che $a_u \in \mathrm{Base}(t)$. Ma questo implica che esiste un v tale che $\{a_u\} \in \mathrm{rep}(v)$ e $\mathrm{rep}(v) \in \mathrm{rep}(t)$; quindi, per definizione di rep, $\{a_u\} \in \mathrm{rep}(t)$ e $t \xrightarrow{+} u$. Ma $t \xrightarrow{+} s$, quindi per il Teorema di Church-Rosser e sapendo che s ed u sono forme normali, $s \equiv u$, assurdo.

Ovviamente, se t é una forma normale $|\mathrm{Base}(t)| = 1$. □

La conclusione che possiamo trarre dallo sviluppo presentato é che, ancora una volta, i concetti base di **ZFA** (insieme ben fondato, insieme riflessivo, ...) caratterizzano in modo diretto i criteri di convergenza (divergenza) che sorgono da teorie come la Logica Combinatoria o il λ-Calcolo e che costituiscono un modo per definire concetti circolari.

É interessante rilevare come la costruzione da noi presentata, seppur molto sintattica, sia simile ad alcuni dei modelli semantici proposti (ad esempio i Graph Models [Plo72,Sco74] o i Böhm Trees [Böh68]) ma manchi delle difficoltà in esse intrinseche per via di un ambiente di definizione (la teoria degli insiemi **ZF**) che non permtte di trattare direttamente nozioni circolari.

3.1.4 Concorrenza

Al fine di mostrare come si possa codificare la nozione di bisimulazione tra processi all'interno di **ZFA**, fornendo di un sistema fondazionale tale concetto, é necessario rappresentare i processi medesimi come insiemi.

Informalmente, un processo é identificato con l'insieme dei comportamenti che é in grado di esibire. Se vogliamo quindi rappresentare i processi CCS, e siamo interessati a cogliere il loro comportamento rispetto ad ogni azione che sono in grado di compiere, verrà naturale identificare la bisimulazione tra processi con la bisimulazione tra gli insiemi che li rappresentano.

Formalmente un processo CCS é definito per induzione a partire dai costruttori del linguaggio; in modo analogo noi possiamo costruire un sistema generale di equazioni in cui, ad ogni variabile, verrà associato un unico insieme, in virtù del General Solution Lemma, che é la rappresentazione del processo medesimo.

A tal punto é sufficente provare che la nozione di bisimulazione tra insiemi coincide con la nozione di bisimulazione tra processi.

Definizione 49 *Un processo CCS P é rappresentato dalla soluzione s_{x_P} associata al sistema generale di equazioni ε_P costruito per induzione sulla struttura di P, come segue:*

- $P \equiv \text{nil}$

  $$\varepsilon_P = \langle \{x_P\}, \emptyset; e \rangle$$

  con $e_{x_P} = \emptyset$.
- $P \equiv \alpha \,.\, Q$

  $$\varepsilon_P = \langle \{x_P\} \cup X_Q, \{\alpha\} \cup A_Q; e \rangle$$

  dove $\varepsilon_Q = \langle X_Q, A_Q; e^Q \rangle$ *é il sistema associato a* Q *e*

  $$e \restriction X_Q = e^Q, \quad e_{x_P} = \langle \alpha, x_Q \rangle \ .$$

- $P \equiv \overline{\alpha} \,.\, Q$

  $$\varepsilon_P = \langle \{x_P\} \cup X_Q, \{\overline{\alpha}\} \cup A_Q; e \rangle$$

  dove $\varepsilon_Q = \langle X_Q, A_Q; e^Q \rangle$ *é il sistema associato a* Q *e*

  $$e \restriction X_Q = e^Q, \quad e_{x_P} = \langle \overline{\alpha}, x_Q \rangle \ .$$

- $P \equiv \sum \Delta$

  $$\varepsilon_P = \langle \{x_P\} \cup \bigcup_{Q \in \Delta} X_Q, \bigcup_{Q \in \Delta} A_Q; e \rangle$$

  dove, per ogni $Q \in \Delta$, $\varepsilon_Q = \langle X_Q, A_Q; e^Q \rangle$ *é il sistema associato a* Q *e*

  $$e \restriction X_Q = e^Q, \quad e_{x_P} = \bigcup_{Q \in \Delta} \{x_Q\} \ .$$

- $P \equiv Q \mid R$

$$\varepsilon_P = \langle \{x_P\} \cup X_Q \times X_R, A_Q \cup A_R; e \rangle$$

dove $\varepsilon_Q = \langle X_Q, A_Q; e^Q \rangle$ *e* $\varepsilon_R = \langle X_R, A_R; e^R \rangle$ *sono i sistemi associati a* Q *ed* R*, rispettivamente ed* e *é definita come*

$$e_{x_P} = e_{x_{Q|R}}, \quad e_{x_{\alpha|\beta}} = \{\langle \gamma, x_{\alpha'|\beta'} \rangle \mid \alpha \mid \beta \xrightarrow{\gamma} \alpha' \mid \beta' \vee \alpha \mid \beta \xrightarrow{\overline{\gamma}} \alpha' \mid \beta'\} \ .$$

- $P \equiv Q \setminus \Gamma$

$$\varepsilon_P = \langle \{x_P\} \cup X_Q, A_Q \setminus \Gamma; e \rangle$$

dove $\varepsilon_Q = \langle X_Q, A_Q; e^Q \rangle$ *é il sistema associato a* Q *e*

$$e \restriction X_Q = e^Q \text{ ristretta ad } A_Q \setminus \Gamma, \quad e_{x_P} = x_Q \ .$$

- $P \equiv Q[\Phi]$

$$\varepsilon_P = \langle \{x_P\} \cup X_Q, \Phi(A_Q); e \rangle$$

dove $\varepsilon_Q = \langle X_Q, A_Q; e^Q \rangle$ *é il sistema associato a* Q*,* $\Phi(A_Q) = \{\Phi(\alpha) \mid \alpha \in A_Q\}$ *e*

$$e \restriction X_Q = \Phi \circ e^Q, \quad e_{x_P} = x_Q \ .$$

- $P \equiv \text{rec } x.\ Q$

$$\varepsilon_P = \langle \{x_P\} \cup X_Q, A_Q; e \rangle$$

dove $\varepsilon_Q = \langle X_Q, A_Q; e^Q \rangle$ *é il sistema associato a* Q *(in cui comparirà una variabile,* x *solo nel lato destro delle equazioni), e*

$$e \restriction (X_Q \setminus \{x\}) = e^Q, \quad e_{x_P} = x, \quad e_x = x_P \ .$$

Per induzione sulla struttura di un processo P é facile convincersi che

Proposizione 50 *Se* $P \xrightarrow{\alpha} Q$*, allora* $\langle \alpha, x_Q \rangle \in e_{x_P}$ *in* $\varepsilon_P = \langle X_P, A_P; e \rangle$ *il sistema associato a* P*.*

Analogamente si può verificare che, in base alla definizione del nostro sistema ε_P ed alla definizione della relazione di transizione:

Proposizione 51 *Se* $\langle \alpha, x_Q \rangle \in e_{x_P}$ *nel sistema* $\varepsilon_P = \langle X_P, A_P; e \rangle$ *associato a* P*, allora esiste un processo* Q *tale che*

(1) $P \xrightarrow{\alpha} Q$*;*
(2) Il sistema associato a Q *é la restrizione di* ε_P *a cui sia stato sottratto la variabile* x_P*, modulo una bisimulazione tra sistemi.*

Le due proposizioni appena enunciate (di cui omettiamo la dimostrazione, essendo totalmente standard) garantiscono che la nostra rappresentazione dei processi sia completa e fedele rispetto alla relazione di transizione.

Il concetto di bisimulazione tra processi coincide con la bisimulazione tra insiemi.

Teorema 52 *Siano P e Q due processi, e siano P' e Q' i corrispondenti insiemi nella rappresentazione in **ZFA**; $P \approx Q$ se e solo se $P' = Q'$.*

Dimostrazione.

(1) $P \approx Q$ implica $P' = Q'$.
Per definizione di bisimulazione tra processi, $P \approx Q$ se e solo se

$$\forall \alpha, \overline{P}.\ P \xrightarrow{\alpha} \overline{P} \rightarrow \exists \overline{Q}.\ Q \xrightarrow{\alpha} \overline{Q} \wedge \overline{P} \approx \overline{Q}$$

e

$$\forall \alpha, \overline{Q}.\ Q \xrightarrow{\alpha} \overline{Q} \rightarrow \exists \overline{P}.\ P \xrightarrow{\alpha} \overline{P} \wedge \overline{P} \approx \overline{Q}\ .$$

Sia R la relazione tra insiemi che siano rappresentazione di processi definita come: $a\ R\ b$ se e solo se

$$\forall \alpha, a'.\ \langle \alpha, a' \rangle \in a \rightarrow \exists b'.\ \langle \alpha, b' \rangle \in b \wedge \langle a', b' \rangle \in R$$

e

$$\forall \alpha, b'.\ \langle \alpha, b' \rangle \in b \rightarrow \exists a'.\ \langle \alpha, a' \rangle \in a \wedge \langle a', b' \rangle \in R$$

Questa é una bisimulazione tra insiemi come si prova immediatamente.
Ma, se $P \approx Q$, allora $P'\ R\ Q'$, infatti

$$\forall \alpha, \overline{P}.\ P \xrightarrow{\alpha} \overline{P} \rightarrow \exists \overline{Q}.\ Q \xrightarrow{\alpha} \overline{Q} \wedge \overline{P} \approx \overline{Q}$$

equivale, per le proposizioni precedenti, a

$$\forall \alpha, \overline{P}.\ \langle \alpha, \overline{P} \rangle \in P' \rightarrow \exists \overline{Q}.\ \langle \alpha, \overline{Q} \rangle \in Q' \wedge \overline{P} \approx \overline{Q}$$

ovvero, secondo l'ipotesi che $\overline{P} \approx \overline{Q} \rightarrow \overline{P}'\ R\ \overline{Q}'$, questo si riduce a $P'\ R\ Q'$. Quindi $P' = Q'$ essendo R una bisimulazione.

(2) É immediato provare che $P \approx Q$ sapendo che $P' = Q'$: infatti, sfruttando la bisimulazione R introdotta nel punto precedente, risulta immediato verificare la tesi.

□

In un certo senso la prova é costruttiva, esibendo effettivamente una bisimulazione tra insiemi che agisca come $\approx$ sulle rappresentazioni dei processi.

In generale é possibile cambiare la codifica dei processi per effettuare osservazioni differenti su di essi, e la naturale nozione di bisimulazione che viene generata da una osservazione risulta coincidente con la bisimulazione tra gli insiemi rappresentazione dei processi.

Le dimostrazioni dei relativi risultati, ad esempio, riguardo l'uguaglianza osservazionale, sono del tutto simili a quelle presentate.

3.2 Soluzione ai Paradossi

3.2.1 Russell

Come é noto, la soluzione al paradosso di Russell che viene fornita nella teoria **ZF** consiste nel bandire tale collezione, mostrando l'impossibilità di costruire un insieme che soddisfi la condizione.

Definiamo $R_b = \{x \in b \mid x \notin x\}$. É facile mostrare che, in **ZF**, questo é un insieme. Il paradosso di Russell afferma che $R_b \notin b$, e questo fatto non induce alcuna inconsistenza nella teoria.

La soluzione fornita da **ZFA** é identica: poichè il solo modo per costruire un insieme che soddisfi l'enunciato di Russell implica l'uso dell'Assioma di Comprensione, e questo stabilisce che l'insieme costruito debba essere sottoinsieme di un insieme dato, segue che, se esistesse $R = \{x \mid x \notin x\}$, R deve essere sottoinsieme dell'insieme di tutti gli insiemi.

In **ZF** ciò é impossibile poichè non esiste un oggetto identificabile con l'insieme di tutti gli insiemi, per l'Assioma di Fondazione.

In **ZFA** l'oggetto identificable come *l'insieme di tutti gli insiemi* non può essere costruito[7], ma se fosse possibile esso sarebbe il massimo punto fisso dell'operatore potenza insiemistica.

Per quanto visto nella parte relativa ai punti fissi, tale punto fisso esiste, a patto di prendere una opportuna base di atomi. Tale base deve formare una classe propria, quindi il massimo punto fisso di $\mathcal{P}$ é una classe propria, esattamente come in **ZF**.

Tirando le somme, il paradosso di Russell non inficia **ZFA**, ma é utile per

[7] Per via del Teorema di Cantor, che afferma che la cardinalità della potenza di X é maggiore della cardinalità di X, per ogni insieme X.

mostrare che alcuni insiemi non sono costruibili, come, ad esempio, un insieme R_b che appartenga a b.

3.2.2 Mentitore

Il paradosso del mentitore[Mar84] deriva dall'autoriferimento contenuto nella frase *questa frase é falsa*. Vediamo di analizzare formalmente la nozione di circolarità soggiacente.

Una sentenza del mentitore ha la seguente struttura

$$\neg \mathrm{True}_h(\mathrm{this}) \ .$$

Teorema 53 (Mentitore) *Sia α una sentenza del mentitore:*

$$\alpha \equiv \neg \mathrm{True}_h(\mathrm{this}) \ .$$

Se $\mathcal{M}$ é un modello (parziale) per cui sia possbile esprimere α, allora una delle seguenti condizioni é falsa:

(1) this *denota α in $\mathcal{M}$.*
(2) h denota $\mathcal{M}$ in $\mathcal{M}$.
(3) $\mathcal{M} \models \alpha \vee \neg\alpha$.

Dimostrazione. Assumiamo le tre condizioni e deriviamone una contraddizione: poichè $\mathcal{M} \models \alpha \vee \neg\alpha$, allora $\mathcal{M} \models \alpha$ oppure $\mathcal{M} \models \neg\alpha$.

Se $\mathcal{M} \models \alpha$ allora $\mathcal{M} \models \neg \mathrm{True}_h(\mathrm{this})$, ma this denota α ed h denota $\mathcal{M}$, e, per definizione del predicato di verità, $\mathcal{M} \models \neg\alpha$, assurdo.

Se $\mathcal{M} \models \neg\alpha$, allora $\mathcal{M} \models \mathrm{True}_h(\mathrm{this})$ e, analogamente, $\mathcal{M} \models \alpha$, assurdo. □

Apparentemente quindi, una qualsiasi soluzione del paradosso del mentitore deve rendere falsa una condizione del teorema.

In realtà, seppur questo é vero, la situazione é più complessa, soprattutto se vista in relazione al concetto circolarità.

L'esempio più interessante riguarda la possibilità di costruire un modello in cui si abbia autoriferimento, che sia totale e che permetta di esprimere una sentenza del mentitore.

Per formalizzare l'esempio, faremo uso della teoria dei modelli per la logica a tre valori di Kleene [Res69]. Rimandiamo alla letteratura la presentazione di tale teoria [BM96] in quanto esula dagli scopi del nostro lavoro.

Sia $\alpha \equiv \neg \text{True}_h(\text{this})$; il modello $\mathcal{M} = \langle D, L, E, A, d, c\rangle$ é definito come:

- $D = \{\alpha, \mathcal{M}\}$ l'universo del discorso, il dominio del modello.
- $L = \{m, \text{True}\}$ le costanti extralogiche, il linguaggio.
- $E = \{\langle \text{True}, \emptyset\rangle\}$ l'estensione, ovvero i predicati che vengono interpretati come veri.
- $A = \{\langle \text{True}, D \times D\rangle\}$ l'antiestensione, ovvero i predicati che hanno valore logico falso.
- $d = \{\langle m, \mathcal{M}\rangle, \langle \text{this}, \alpha\rangle\}$ la denotazione, o l'interpretazione dei simboli per costante.
- $c = \emptyset$ l'interpretazione delle varabili.

Poichè h non é denotato in $\mathcal{M}$, ed $\mathcal{M}$ é un modello per la logica di Kleene a tre valori, $\mathcal{M} \not\models \alpha$ e $\mathcal{M} \not\models \neg\alpha$, ovvero α é indefinito su $\mathcal{M}$.

Tuttavia $\mathcal{M}$ é totale poichè ogni predicato atomico non é indefinito.

Occorre notare che $\mathcal{M} \models \neg \text{True}_m(\text{this})$, ma questo non genera alcun paradosso, poichè this denota α e $\alpha \not\equiv \neg \text{True}_m(\text{this})$.

Quindi un qualsiasi modello per una logica con indefiniti, che ammetta autoriferimento può essere bisimulato entro **ZFA** da un insieme riflessivo.

Inoltre, a seconda della particolare soluzione al paradosso, tali modelli in **ZFA** saranno costruibili secondo le linee guida negli esempi citati.

3.2.3 Ipergioco

Come abbiamo già detto nell'introduzione, la natura dell'ipergioco é differente dagli altri paradossi. Nelle sezioni precedenti abbiamo visto come il paradosso d Russell non possa occorrere in **ZFA**, e come il paradosso del mentitore sia modellabile per mostrare che certi insiemi non possano essere costruiti.

Il paradosso dell'ipergioco coinvolge direttamente l'idea di circolarità e quindi merita un'analisi formale dettagliata.

Definizione 54 *Sia S un insieme di giochi, il* supergioco *su S, denotato con S^+ é definito informalmente come segue: il giocatore I sceglie un gioco $G \in S$, poi il giocatore II inizia G, ed il resto del gioco é G. Il vincitore di S^+ é il vincitore di G.*

É chiaro che, per ogni S, esiste il supergioco S^+.

Proposizione 55 *Sia S un insieme di giochi*

(1) Se S é un insieme ben fondato allora S^+ é ben fondato.

(2) Se S é un insieme ben fondato allora $S^+ \notin S$.

Dimostrazione.

(1) Un gioco viene modellato come l'insieme delle sequenze di mosse possibili. Essendo S ben fondato, per ipotesi, ogni $G \in S$ é ben fondato. Formalmente $S^+ = \{\langle x, \sigma\rangle \mid x \in S \wedge \sigma \in x\}$, ovvero la prima mossa (x) é la scelta di un gioco in S ed il resto della partita (σ) é uno svolgimento di x.

Se S^+ fosse non ben fondato, esso conterrebbe una sequenza discendente infinita, ma ciò é possibile solo se esiste $\sigma \in x$ per un certo $x \in S$ tale che σ sia infinita, contro ipotesi.

Da cui segue che S^+ é ben fondato.

(2) Per assurdo, se $S^+ \in S$ allora in S deve esistere la sequenza

$$\langle S^+, \langle S^+, \langle S^+, \dots\rangle\rangle\rangle$$

che ha lunghezza transfinita, per cui S^+ non é ben fondato, contraddicendo il punto (1).

□

Corollario 56 *Non esiste un insieme i cui elementi siano precisamente tutti i giochi ben fondati.*

Dimostrazione. Per assurdo, sia S tale insieme, allora esiste S^+ ed é ben fondato per la proposizione precedente, quindi $S^+ \in S$, assurdo. □

Definizione 57 *Sia S un insieme di giochi,* l'ipergioco *su S, indicato con S^*, é definito informalmente come segue: il giocatore I sceglie un gioco $G \in S \cup \{S^*\}$, poi il giocatore II inizia G, ed il resto del gioco é G. Il vincitore di S^* é il vincitore di G.*

In questo caso, é necessario provare che il gioco S^* é ben definito in **ZFA**, ovvero che l'insieme delle sequenze di mosse che individua esista e sia unico.

Proposizione 58 *Per ogni insieme di giochi S ben fondato, l'ipergioco S^* é un gioco ben definito.*

Dimostrazione. Ogni gioco é modellabile come una quadrupla

$$\langle M, R, W_{\mathrm{I}}, W_{\mathrm{II}}\rangle$$

dove l'insieme M é costituito da tutte le possibili sequenze di mosse; R é una relazione tra sequenze di mosse che afferma che, se $\sigma\ R\ \tau$, allora τ corrisponde ad una possibile prosecuzione di σ; W_{I}, W_{II} sono sottoinsiemi di R che debbono essere ben fondati, quindi i cui elementi siano sequenze finite, contenenti, rispettivamente, le sequenze che assegnano la vittoria al giocatore I ed al giocatore II.

Se $G \in S$ indichiamo $G = \langle M_G, R_G, W_{\mathrm{I}_G}, W_{\mathrm{II}_G}\rangle$.

Consideriamo il seguente sistema di equazioni:

$$\begin{cases} x &= \langle y, z, w, v\rangle \\ y &= M \\ z &= R \\ v &= W_{\mathrm{I}} \\ w &= W_{\mathrm{II}} \end{cases} \tag{4}$$

con

$$M = \{\langle \alpha, \tau\rangle \mid (\alpha \in S \wedge \tau \in M_\alpha) \vee (\alpha = x \wedge \tau \in y)\}$$

R é definita come: per ogni $\rho \in M$, se $\rho = \langle x, \ldots, x, \tau\rangle$ allora $\rho\ R\ \tau$, $\tau \in M$, con un numero finito di x nel prefisso; se esiste un gioco $G \in S$ ed un q tale che $q \in M_G$, con $\rho = \langle G, q\rangle$ o $\rho = \langle x, \ldots, x, G, q\rangle$, allora $\rho\ R\ q$; in ogni altro caso R non vale.

Inoltre

$$W_{\mathrm{I}} = \{\rho \mid \rho = \langle x, \ldots, x, G, q\rangle \text{ dove } \rho \text{ ha lunghezza dispari e } \rho \in M\rangle\}$$

$$W_{\mathrm{II}} = \{\rho \mid \rho = \langle x, \ldots, x, G, q\rangle \text{ dove } \rho \text{ ha lunghezza pari e } \rho \in M\rangle\}\ .$$

É ovvio che il sistema (4) codifica S^* per come abbiamo definito M, R e W_{I}, W_{II}.

Tuttavia (4) é un sistema generale di equazioni in **ZFA**, per cui ammette una ed una sola soluzione s. Ovviamente $S^* = s_x$.

In effetti é immediato provare che s_x soddisfa la descrizione informale dell'ipergioco; in conclusione la definizione di ipergioco é ben data. □

Proposizione 59 *Sia S un insieme di giochi ben fondati, allora S^* non é ben fondato, da cui $S^* \notin S$.*

Dimostrazione. Notiamo che, dalla costruzione formale di S^*, la sequenza $\langle S^*, S^*, \ldots \rangle$ é una mossa lecita (ovvero é in M_{S^*}), e nessun prefisso di essa costituisce una vittoria per alcun giocatore. Quindi S^* non é ben fondato. □

La lettura che questi risultati ci danno rispetto al paradosso dell'ipergioco é che, in realtà, la descrizione informale dell'ipergioco é ambigua: il paradosso nasce dal fatto che, implicitamente, in tale descrizione, identifichiamo S^+ con S^*.

Avendo provato che non esiste un insieme di tutti i giochi ben fondati, abbiamo analizzato come formalizzare il paradosso preso un insieme di giochi ben fondati (*regolari*). Il risultato é che, rifacendo la costruzione del paradosso, assumendo l'ipergioco irregolare, otteniamo un gioco regolare, il supergioco, che non appartiene all'insieme iniziale; invece facendo la costruzione inversa, in cui, nel paradosso, si supponeva l'ipergioco regolare, ma che, in **ZFA**, possiamo effettuare senza tale ipotesi, otteniamo l'ipergioco, e, come il paradosso deduce, esso risulta irregolare.

Una lettura alternativa dell'analisi condotta porta al seguente risultato:

Lemma 60 *Sia s un insieme, allora non esiste alcun insieme a che sia soluzione dell'equazione:*

$$a = \{b \in s \cup \{a\} \mid b \text{ é ben fondato}\} \ .$$

Dimostrazione. Supponiamo che tale a esista. Per definizione, per ogni $b \in a$, b é ben fondato, per cui a é ben fondato.

Ma allora $a \in \{b \in s \cup \{a\} \mid b \text{ é ben fondato}\} = a$, ovvero a é riflessivo e quindi non ben fondato. □

In conclusione possiamo leggere il paradosso dell'ipergioco come una lezione che insegna che alcune classi di sistemi di equazioni tra insiemi di **ZFA**, hanno una unica soluzione, ma un sistema qualsiasi non ricade sotto il dominio dei risultati ottenuti sulla teoria di **ZFA**, e quindi nulla si può dire riguardo all'esistenza e/o unicità delle sue soluzioni.

3.3 Insiemi Ereditariamente Finiti

Spesso, in molte branche della Matematica [Bar77,MB65,Mac71,Csá78], si ha a che fare con insiemi finiti, insiemi di insiemi finiti, ...

Vi sono diversi modi di formalizzare una tale costruzione, e, in **ZF**, essi sono equivalenti. In **ZFA** ciò non avviene e questo fatto illustra bene come l'intuizione nella teoria degli insiemi non ben fondati, sia differente.

Oltre a costituire un ottimo esempio per rimarcare le differenze tra **ZFA** e la teoria degli insiemi standard, specialmente in rapporto all'idea di circolarità, gli insiemi ereditariamente finiti forniscono anche una concreta applicazione, di per se interessante, di **ZFA**; il loro punto di forza é costituito dalle numerose proprietà di cui godono e dal fatto che essi, seppur non così semplicemente come in **ZFA**, trovano formalizzazione anche nella teoria degli insiemi usuale.

Vi sono tre modi di formalizzare l'intuizione che sottende alla costruzione degli insiemi ereditariamente finiti:

Definizione 61 *Sia A un insieme; l'operatore Δ é definito come:*

$$\Delta(b) = \mathcal{P}_{\text{fin}}(b \cup A) = \{c \mid c \subseteq b \cup A \wedge |c| \in \mathbb{N}\}$$

Evidentemente Δ é un operatore monotono.

Definiamo $\mathrm{HF}^0[A]$ come il minimo punto fisso Δ_*; definiamo $\mathrm{HF}^1[A] = \Delta^*$, il massimo punto fisso di Δ. Infine definiamo $\mathrm{HF}^{1/2}[A]$ come l'insieme costituito da tutti gli elementi in $\mathrm{HF}^1[A]$, la cui chiusura transitiva sia finita.

Al solito scriveremo HF^0, HF^1, $\mathrm{HF}^{1/2}$ al posto di $\mathrm{HF}^0[\emptyset]$, $\mathrm{HF}^1[\emptyset]$, $\mathrm{HF}^{1/2}[\emptyset]$.

Le relazioni tra questi insiemi sono descritte dalla seguente proposizione:

Proposizione 62 *Sia A un insieme*

(1) Se A é transitivo allora $\mathrm{HF}^0[A]$, $\mathrm{HF}^{1/2}[A]$, $\mathrm{HF}^1[A]$ sono transitivi.
(2) $\mathrm{HF}^0[A] \subseteq \mathrm{HF}^{1/2}[A] \subseteq \mathrm{HF}^1[A]$.
(3) $\mathrm{HF}^0[A] = \{b \mid b \in \mathrm{HF}^1[A] \wedge b$ *é ben fondato*$\}$.
(4) $\mathbb{N} \subseteq \mathrm{HF}^0[A]$.
(5) $\Omega \in \mathrm{HF}^{1/2}[A]$.
(6) $\langle 0, \langle 1, \langle 2, \ldots \rangle\rangle\rangle \in \mathrm{HF}^1[A]$.
(7) $\mathrm{HF}^0[A] \neq \mathrm{HF}^{1/2}[A]$ *e* $\mathrm{HF}^{1/2}[A] \neq \mathrm{HF}^1[A]$.

Dimostrazione.

(1) Osservando che, in generale, se A é transitivo e B é un punto fisso di Δ, allora B é transitivo, segue che $\mathrm{HF}^0[A]$ e $\mathrm{HF}^1[A]$ sono transitivi.

Per $\mathrm{HF}^{1/2}[A]$, se $a \in b$, allora $a^+ \subseteq b^+$, dove x^+ é la chiusura transitiva di x. Per cui se la chiusura transitiva di un insieme é finita, così é la chiusura transitiva di tutti i suoi elementi.

(2) In generale, per ogni operatore Γ monotono, $\Gamma_* \subseteq \Gamma^*$, quindi $\mathrm{HF}^0[A] \subseteq \mathrm{HF}^1[A]$.

Usando il principio di induzione per $\mathrm{HF}^0[A]$, si prova che $\mathrm{HF}^0[A] \subseteq \mathrm{HF}^{1/2}[A]$: sia b un sottoinsieme finito di $A \cup (\mathrm{HF}^{1/2}[A] \cap \mathrm{HF}^0[A])$; allora $b^+ = b \cup \bigcup_{a \in b} a^+$ é una unione finita di insiemi finiti, ovvero B^+ é finito. In altre parole

$$\mathcal{P}_{\mathrm{fin}}(A \cup (\mathrm{HF}^{1/2}[A] \cap \mathrm{HF}^0[A])) = \Delta(\mathrm{HF}^{1/2}[A] \cap \mathrm{HF}^0[A]) \subseteq \mathrm{HF}^{1/2}[A] \ .$$

Per il principio di induzione segue che $\mathrm{HF}^0[A] \subseteq \mathrm{HF}^{1/2}[A]$.

Per provare che $\mathrm{HF}^{1/2}[A] \subseteq \mathrm{HF}^1[A]$, notiamo che $\mathrm{HF}^{1/2}[A]$ é un punto fisso di Δ: questa é una conseguenza immediata del fatto che

$$b^+ = \bigcup \{c^+ \mid c \in b \text{ é un insieme}\} \cup \{x \mid x \in b \text{ é un atomo}\} \ .$$

(3) Sia WF la classe (propria) di tutti gli insiemi ben fondati:

$$\mathcal{P}_{\mathrm{fin}}(A \cup (WF \cap \mathrm{HF}^0[A])) \subseteq WF$$

poichè ogni insieme i cui elementi siano atomi o insiemi ben fondati é, a sua volta, ben fondato. Quindi, per il principio di induzione su $\mathrm{HF}^0[A]$, $\mathrm{HF}^0[A] \subseteq WF$, ovvero tutti gli elementi di $\mathrm{HF}^0[A]$ sono ben fondati. Questo prova che

$$\mathrm{HF}^0[A] \subseteq \{b \mid b \in \mathrm{HF}^1[A] \wedge b \in WF\} \ .$$

Sia $b \in WF \cap \mathrm{HF}^1[A]$, assumiamo che ogni elemento $c \in b$ con $c \in WF \cap \mathrm{HF}^1[A]$, appartenga a $\mathrm{HF}^0[A]$, allora $b \subseteq A \cup \mathrm{HF}^1[A]$ e b é finito. Ma WF e $\mathrm{HF}^1[A]$ sono entrambe collezioni transitive e $b \subseteq_\omega \mathrm{HF}^0[A] \cup A$ per ipotesi, quindi, per $\in$-induzione su WF, $b \in \mathrm{HF}^0[A]$. Ovvero $WF \cap \mathrm{HF}^1[A] \subseteq \mathrm{HF}^0[A]$.

(4) Per induzione su $\mathbb{N}$: si supponga che ogni $m < n$ appartenga a $\mathrm{HF}^0[A]$; poichè n é un insieme finito, $n \subseteq_\omega \mathrm{HF}^0$, quindi $n \subseteq_\omega \mathrm{HF}^0[A]$, ma questo implica, per definizione di Δ, che $n \in \mathrm{HF}^0[A]$.

(5) Notando che Ω^+ contiene un solo elemento, segue che $\Omega \in \mathrm{HF}^{1/2}[A]$.

(6) La sequenza $\sigma = \langle 0, 1, \dots \rangle$ é un elemento di $\mathrm{HF}^1[A]$, poichè ogni prefisso proprio di σ é un insieme finito, per cui $\sigma \in \Delta^* = \mathrm{HF}^1[A]$ per definizione di massimo punto fisso.

(7) Poiché $\Omega \in \mathrm{HF}^{1/2}[A]$ e Ω non é ben fondato, $\Omega \notin \mathrm{HF}^0[A]$, quindi $\mathrm{HF}^0[A] \neq \mathrm{HF}^1/2[A]$ e $\mathrm{HF}^0[A] \neq \mathrm{HF}^1[A]$.

Inoltre la chiusura transitiva di $\sigma = \langle 0, 1, \dots \rangle$ contiene $\mathbb{N}$ per cui $\sigma \notin \mathrm{HF}^{1/2}[A]$, ovvero $\mathrm{HF}^{1/2}[A] \neq \mathrm{HF}^1[A]$.

□

Come accennato in precedenza gli insiemi ereditariamente finiti, in qualsiasi formalizzazione, godono di alcune interessanti proprietà.

Lemma 63 *Sia $A \subseteq B$, allora* $\mathrm{HF}^0[A] \subseteq \mathrm{HF}^0[B]$ *e* $\mathrm{HF}^1[A] \subseteq \mathrm{HF}^1[B]$.

Dimostrazione. Banalmente, per induzione su $\mathrm{HF}^0[A]$, e per coinduzione su $\mathrm{HF}^1[B]$. □

Lemma 64 *Sia B un insieme di atomi, e sia $A \subseteq \mathrm{HF}^1[B]$, allora $A^\infty \subseteq \mathrm{HF}^1[B]$, dove A^∞ é l'insieme delle sequenze su alfabeto A.*

Dimostrazione. Sia $\sigma \in A^\infty$; se $\sigma = \emptyset$, allora $\sigma \in \mathrm{HF}^1[B]$, se $\sigma = \langle \alpha, \tau \rangle$, allora $\alpha \in A \subseteq \mathrm{HF}^1[B]$ e τ, per ipotesi, appartiene a $\mathrm{HF}^1[B]$, quindi, essendo $\mathrm{HF}^1[B]$ chiuso per coppia, segue che $\sigma \in \mathrm{HF}^1[B]$.

Ovvero $A^\infty \subseteq \mathrm{HF}^1[B]$. □

4 Conclusioni

In questo lavoro abbiamo cercato di delineare una teoria della circolarità. In primo luogo abbiamo mostrato come l'idea di definizione circolare, di strutture autoreferenziali ricorra frequentemente in Informatica ed in Matematica, e che tali concetti sono fonte di problemi se affrontati in modo improprio.

Per costruire una teoria della circolarità abbiamo presentato **ZFA**, la teoria degli insiemi non ben fondati e sulle sue fondamenta abbiamo sviluppato una teoria dei punti fissi.

Vale la pena sottolineare che la presentazione esposta é elementare, non usando generalizzazioni categoriali [BM96] o rappresentazioni logiche [Acz88].

Sebbene questi aspetti siano molto interessanti, essi non sono, a nostro avviso, necessari per affrontare i problemi legati alla circolarità nella usuale pratica informatica e matematica.

Tutte queste parti non sono orginali ed il nostro contributo é limitato ad una presentazione omogenea in una notazione consistente.

Per quanto riguarda le applicazioni, in letteratura esistono caratterizzazioni equivalenti a quella da noi presentata per le parti sulle sequenze [BM96] e sulla Teoria dei Processi [Mil89].

Analogamente il concetto di insieme ereditariamente finito é introdotto in molti lavori [Acz88,BM96,BM91] riguardanti la teoria degli insiemi non ben fondati.

Diverso é il discorso riguardante le chiusure: tale parte non trova sviluppo nella letteratura a nostra conoscenza, con un approccio simile a quello introdotto. Sebbene il concetto di cochiusura sia utilizzato [Csá78], esso non sembra avere uno sviluppo sistematico come quello che abbiamo cercato di introdurre.

La parte relativa alla Logica Combinatoria é integralmente nuova: sebbene vi siano analogie con altr modelli semantici (Graph Models e Böhm trees, in particolare), lo sviluppo di un modello consistente all'interno di una teoria degli insiemi non ben fondati non ha precedenti di cui siamo a conoscenza.

L'analisi dei paradossi é standard: essa é ricavata, adattando le prove al nucleo di **ZFA** presentato, dalla letteratura esistente [BM96,Bar77,Kun80,Mar84].

In conclusione questo lavoro é in massima parte di rassegna, ma contiene un paio di sviluppi autonomi che, speriamo, possano suggerire al lettore un modo alternativo di modellare problemi.

Volutamente non abbiamo illustrato applicazioni propriamente logiche della teoria della circolarità [BM96,Bar77], in quanto alcune di esse saranno oggetto del lavoro di tesi dell'autore ed altre sono ampiamente illustrate in letteratura.

Lo scopo del lavoro é stato fornire una presentazione il più possibile autocontenuta della teoria della circolarità, mostrando come essa sia utile ed intuitiva nelle sue applicazioni.

I futuri sviluppi di questo lavoro nella prospettiva di ricerca dell'autore sono alcune applicazioni alla Teoria dell Dimostrazione per Logiche Costruttive [FMO97,Ben97] (che compariranno nella tesi di dottorato) ed un approfondimento della modellazione della Logica Combinatoria e del λ-Calcolo, particolarmente verso le versioni di tali teorie in cui l'operazione di applicazione funzionale sia parziale [BKd96].

[Acz88] Peter Aczel. *Non Well-Founded Sets*. Number 14 in CSLI Lecture Notes. CSLI Publications, Stanford, 1988.

[AHU83] A. V. Aho, J. E. Hopcroft, and J. D. Ullman. *Data Structures and Algorithms*. Addison-Wesley, Reading, Massachusettes, 1983.

[Bar77] Jon Barwise. *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, 1977.

[Bar84] Henk P. Barendregt. *The Lambda Calculus: Its Syntax and Semantics*, volume 103 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, 2nd edition, 1984.

[Bar89] Jon Barwise. On the model theory of common knowledge. In *The Situation in Logic*, number 17 in CSLI Lecture Notes, pages 201–220. CSLI Publications, Stanford, 1989.

[BE87] Jon Barwise and John Etchemendy. *The Liar: An Essay in Truth and Circularity*. Oxford University Press, Oxford, 1987.

[Ben97] Marco Benini. The collection method in second-order intuitionistic logic. *Annals of Pure and Applied Logic*, 1997. submitted.

[BKd96] Inge Bethke, Jan W. Klop, and R. deVrijer. Completing partial combinatory algebras with unique head-normal forms. In 11^{th} *Annual Symposium on Logic in Computer Science*, pages 448–454. IEEE, IEEE Computer Society Press, 1996.

[BM91] Jon Barwise and Lawrence C. Moss. Hypersets. *Mathematical Intelligencer*, 13:31–41, 1991.

[BM96] Jon Barwise and Lawrence C. Moss. *Vicious Circles*. Number 60 in CSLI Lecture Notes. CSLI Publications, Stanford, 1996.

[Böh68] Corrado Böhm. Alcune proprietà delle forme β-η-normali nel λ-K-calcolo. *Pubblicazioni dell'Istituto per le Applicazioni del Calcolo, Roma*, 696, 1968.

[CF58] Haskell B. Curry and Robert Feys. *Combinatory Logic*, volume I. North-Holland, Amsterdam, 1958.

[Csá78] A'kos Császár. *General Topology*. Hilger, Bristol, 2nd edition, 1978.

[FMO97] Mauro Ferrari, Pierangelo Miglioli, and Mario Ornaghi. Strongly constructive formal systems. *Annals of Pure and Applied Logic*, 1997. submitted.

[Göd31] Kurt Gödel. Über formal unentscheidbare sätze der Principia Mathematica und verwandter Systeme. *Monatsh. Math. Phys.*, I(38):173–198, 1931.

[Hal60] P. Halmos. *Naive Set Theory*. Van Nostrand, New York, 1960.

[HS86] Roger J. Hindley and Jonathan P. Seldin. *Introduction to Combinators and the Lambda Calculus*. Number 1 in London Mathematical Society student texts. Cambridge University Press, Cambridge, 1986.

[JH56] K. Jaakko and J. Hintikka. Identity, variables and impredicative definitions. *Journal of Symbolic Logic*, 21(3), September 1956.

[Kri75] Saul A. Kripke. Outline of a theory of truth. *The Journal of Philosophy*, 72:52–81, 1975.

[Kun80] Keith Kunen. *Set Theory: An Introduction to Independence Proofs*, volume 102 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, 1980.

[Lan65] S. Lang. *Algebra*. Addison-Wesley, Reading, Massachusettes, 1965.

[Mac71] Saunders MacLane. *Categories for the Working Mathematician*. Springer-Verlag, 1971.

[Mar84] Robert L. Martin. *Recent Essays on Truth and the Liar Paradox*. Clarendon Press, Oxford, 1984.

[MB65] Saunders MacLane and Garret Birkhoff. *Algebra*. The MacMillan Company, 1965.

[Mil73] Robin Milner. Processes: a mathematical model of computing agents. In Rose and Shepherdson, editors, *Logic Colloquium '73*, pages 157–174. North-Holland, 1973.

[Mil80] Robin Milner. *A Calculus of Communicating Systems*, volume 92 of *Lecture Notes in Computer Science*. Springer-Verlag, 1980.

[Mil89] Robin Milner. *Communication and Concurrency*. Prentice-Hall, 1989.

[Pau92] Lawrence C. Paulson. Set theory as a computational logic: I from foundations to functions. Technical Report 271, Cambridge University, Computer Laboratory, 1992.

[Pau93] Lawrence C. Paulson. Coinduction and corecursion in higher-order logic. Technical Report 304, Cambridge University, Computer Laboratory, 1993.

[Plo72] Gordon Plotkin. A set-theoretical definition of application. School of Artificial Intelligence, University of Edinburgh, 1972. Memo MIP-R-95.

[Res69] Nicholas Rescher. *Many Valued Logic*. McGraw-Hill, New York, 1969.

[Rus06] Bertrand Russell. Some difficulties in the theory of transfinite numbers and order types. *Proc. London Math. Soc.*, 4(2):29–53, 1906.

[Sco74] Dana S. Scott. The language LAMBDA. *Journal of Symbolic Logic*, 39:425–427, 1974. (abstract).

[Sho77] J. R. Shoenfield. Axioms of set theory. In *Handbook of Mathematical Logic* [Bar77], chapter B.1, pages 321–344.

[Smu94] Raymond S. Smullyan. *Diagonalization and Self-Reference*. Number 27 in Oxford Logic Guides. Oxford Science Publications, 1994.

[Tar39] Alfred Tarski. On undecidable statements in enlarged systems of logic and the concept of truth. *Journal of Symbolic Logic*, 4(4):105–112, 1939.

[Tur37] Alan M. Turing. Computability and lambda-definability. *Journal of Symbolic Logic*, 2(4), December 1937.

[Zwi87] William S. Zwicker. Playing games with games: the hypergame paradox. *American Mathematical Monthly*, 94(6):507–514, 1987.