



Bollati Boringhieri

Vincenzo Manca

Logica matematica

Strutture Rappresentazioni Deduzioni



Bb

Vincenzo Manca
Logica matematica

Il libro è un manuale sintetico per un corso introduttivo di logica matematica. Il sottotitolo *Strutture Rappresentazioni Deduzioni* vuole mettere in rilievo un principio ispiratore del testo. Le strutture sono le entità di riferimento del linguaggio logico. Le deduzioni sono gli strumenti con cui si elaborano le formule per «calcolarne» i rapporti di conseguenza. Le rappresentazioni giocano un ruolo fondamentale, spesso dato per scontato o solo accennato nei manuali di logica, che è preliminare all'attività deduttiva. Riuscire a esprimere in formule proprietà e relazioni, su un certo insieme di oggetti, è un lavoro spesso non semplice cui questo libro dedica particolare attenzione. Il lettore è guidato con vari esempi ed esercizi a capire il senso e il funzionamento dei meccanismi di base della logica dei predicati. Inoltre, in termini di rappresentabilità logica, sono analizzati alcuni fenomeni cruciali della logica

matematica intimamente connessi col rapporto tra deduzione e calcolo. Esempi di rappresentabilità entro modelli e teorie indicano alcuni importanti sviluppi in cui la logica diventa uno strumento prezioso dell'informatica teorica nella comprensione e nella scoperta di nuovi modelli di calcolo. In appendice è data la traduzione di una recente conferenza di Gregory Chaitin, un protagonista in ricerche di confine tra logica e informatica, che in modo informale ma avvincente tratteggia una storia delle idee della logica matematica nel xx secolo.

Vincenzo Manca è docente presso il Dipartimento di Informatica dell'Università di Pisa, dove tiene il corso di Logica matematica e quello di Linguaggi formali e automi. Gran parte dei suoi lavori, pubblicati in riviste e volumi internazionali, riguardano la logica equazionale, la teoria dei linguaggi formali e, recentemente, i modelli di calcolo basati su meccanismi biologici.

ISBN 88-339-5656-3



LIRE 35.000 (I.I.)
€ 18,08

Vincenzo Manca

Logica matematica

Strutture Rappresentazioni Deduzioni

con un saggio di Gregory Chaitin

Bollati Boringhieri

Prima edizione gennaio 2001

© 2001 Bollati Boringhieri editore s.r.l., Torino, corso Vittorio Emanuele II, 86
I diritti di memorizzazione elettronica, di riproduzione e di adattamento totale o parziale con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche) sono riservati

Stampato in Italia dalla Stampatre di Torino

ISBN 88-339-5656-3

Schema grafico della copertina di Pietro Palladino e Giulio Palmieri

Indice

7 *Prefazione*

Logica matematica

13 Introduzione

17 1. Fondamenti matematici

1.1. Operazioni, numeri e classi, 18 1.2. Proprietà e relazioni, 22 1.3. Ordinamenti, 23 1.4. Insiemi, 24 1.5. Funzioni, 27 1.6. Sequenze, 29
1.7. Variabili e λ -notazione, 31 1.8. Strutture matematiche, 33 1.9. Induzione strutturale, 36 1.10. Numeri ordinali e cardinali*, 40 1.11. Principi di massimalità*, 48 1.12. La costruzione del linguaggio matematico, 50

54 2. Logica predicativa

2.1. Sintassi predicativa, 54 2.2. Semantica predicativa, 59 2.3. Logica proposizionale, 70 2.4. Tableau analitici, 77 2.5. Completezza e compattezza, 87 2.6. Forme di Skolem ed espansione di Herbrand, 92 2.7. Teoremi di Löwenheim-Skolem*, 95

98 3. Calcoli logici

3.1. Deduzione naturale, 100 3.2. Deducibilità secondo Herbrand-Skolem, 107 3.3. Metodo di risoluzione, 107 3.4. Calcolo dei sequenti*, 109 3.5. Calcoli logici equazionali*, 112 3.6. Tipologia dei calcoli logici*, 114

118 4. Rappresentabilità logica

4.1. Modelli e teorie, 119 4.2. Linguaggi formali, 129 4.3. Grammatiche e automi, 134 4.4. Teorie monoidali*, 137 4.5. Rappresentazione logica delle macchine di Turing*, 143 4.6. Semidecidibilità e decidibilità, 146

148 5. Indecidibilità e incompletezza

5.1. Dall'ideografia di Frege ai teoremi di Gödel, 151 5.2. Relazioni strutturali tra modelli e teorie*, 152

159 6. Esercizi finali

167	Appendice. Un secolo di dispute sui fondamenti della matematica (<i>Gregory Chaitin</i>) 1. Introduzione, 167 2. La crisi della teoria degli insiemi, 168 3. I paradossi di Bertrand Russell, 170 4. La soluzione assiomatico-formale di David Hilbert, 171 5. Che cos'è la metamatematica, 173 6. Kurt Gödel scopre l'incompletezza, 174 7. Alan Turing scopre l'indcidibilità, 175 8. Gregory Chaitin scopre la casualità nella matematica pura, 178 9. Dove siamo diretti?, 185
189	Elenco dei teoremi fondamentali
191	Alfabeto greco
193	Elenco dei simboli
195	<i>Bibliografia</i>
199	<i>Indice analitico</i>

Prefazione

Questo libro raccoglie l'esperienza didattica di molti anni di insegnamento in corsi elementari di logica matematica. I contenuti sono in gran parte standard, tuttavia, il modo di organizzarli e di presentarli è fortemente legato ai miei gusti personali, alle ricerche svolte, agli insegnanti e studenti incontrati, e ai colleghi con cui ho collaborato. Un'attenzione notevole è stata posta al rapporto tra logica matematica e informatica teorica (linguaggi, grammatiche, automi, deduzione/calcolo) e alla rappresentazione logica. Riuscire a esprimere in formule proprietà e relazioni su un certo insieme di oggetti (numeri, stringhe, strutture dati) è un lavoro spesso non semplice che si acquisisce con la pratica, ed è un'attività preliminare a quella deduttiva. Spesso gli studenti sanno enunciare e dimostrare teoremi, ma hanno difficoltà nel tradurre in formule semplici fatti aritmetici o geometrici. Uno scopo del testo è quello di guidare con esempi ed esercizi a capire il senso e il funzionamento dei meccanismi espressivi di base della logica dei predicati.

Varie stesure precedenti hanno visto la luce come dispense, e un estratto in inglese è apparso come voce di un'enciclopedia americana.

I capitoli essenziali si possono svolgere in quaranta ore (dense), di cui molte dedicate ad esempi ed esercizi. Altre parti più impegnative (evidenziate nell'Indice con asterisco) possono essere accennate o sviluppate come approfondimenti. Vi sono molte "linee di fuga" che il lettore può facilmente individuare dal cambiamento di registro dell'esposizione (storico-filosofica). Percorrerne qualcuna, con le varianti suggerite dall'occasione, è un modo per sollecitare lo studente a guardare le cose da un punto non meramente scolastico, introducendolo alla riflessione critica, e a una prospettiva più profonda.

Devo dire che fino ad ora, nel rileggere il testo, provo una certa insoddisfazione e noto che molte delle motivazioni e delle ragioni profonde non affiorano, o affiorano solo in modo incompleto. Sono convinto che la ma-

tematica, e la scienza in genere, siano animate da ragioni che hanno una forte componente emozionale e l'insegnamento abbia vero successo quando questa componente riesce ad essere comunicata: solo allora gli occhi della mente si concentrano a guardare e ad analizzare, e vedono perché vogliono vedere. Lo stile di questo libro è sicuramente animato da questa tensione comunicativa, tuttavia, per ovvie ragioni di sintesi, esso segue essenzialmente il criterio espositivo di un manuale, con tutti i limiti che questo comporta. Un limite tipico è quello di presentare teorie senza storia, calate dall'alto, senza farne cogliere i fattori storici e psicologici che stanno alla base della loro creazione. Presentare una teoria nella sua forma ultima porta a un grandissimo vantaggio di economia e coerenza espositiva, ma spesso equivale a mostrare solo la punta dell'iceberg, nascondendo le motivazioni iniziali, le questioni sottostanti, i tentativi, i fallimenti, e in generale, i nodi del tragitto intellettuale che è stato percorso per collocarla nel quadro teorico attuale. I matematici, prima di esprimere i risultati in formule, lottano spesso con pregiudizi intellettuali e con stratificazioni del senso comune annidati nella loro mente e nella comunità scientifica del loro tempo. Penso che queste vicende debbano in qualche modo (anche molto sintetico) giungere allo studente per comunicargli l'entusiasmo intellettuale che è alla base di uno studio autentico e proficuo.

Per compensare in parte i limiti del manuale ho inserito nel testo brevi intermezzi, anche solo poche righe, che fungono da indicatori per le "linee di fuga" sopra menzionate, ovvero cambiando metafora, da "finestre socchiuse" da "aprire sulla valle". Per lo stesso motivo, ho aggiunto in appendice la traduzione di una recente conferenza tenuta da Gregory Chaitin (Un secolo di dispute sui fondamenti della matematica). Mi sembra che questo ricercatore, protagonista di importanti ricerche di informatica teorica, esprima in modo semplice e profondo le intime convinzioni che hanno sempre animato il mio insegnamento e la mia ricerca in logica matematica. Le sue parole fanno capire i legami profondi tra la logica matematica e l'informatica. Il lettore che si annoia a leggere definizioni, teoremi e algoritmi legga e rilegga quelle poche pagine. Le grandi teorie nascono per rispondere, anche se parzialmente, a grandi domande e senza una cornice ampia in cui inquadrare i singoli risultati della scienza si rischia di perdere il senso di tutto lo scenario. La strada concettuale che porta ai computer parte dallo studio cantoriano dei vari ordini di infinito, passa per i paradossi insiemistici di Russell, per il formalismo hilbertiano, per i teoremi limitativi di Gödel, fino all'analisi di Turing della calcolabilità e dell'indcidibilità, e alla versione "informazionale" di tali concetti, legata al rapporto tra entropia, informazione e casualità. Le recenti teorie sulla complessità algoritmica sono protese verso le nuove frontiere in cui logica e informatica si misurano con i grandi problemi scientifici del futuro.

Viviamo in un periodo in cui la tecnologia è sempre più pressante nei confronti della scienza, spingendola a fare maturare idee in modo sempre più veloce, per rispettare richieste e ritmi di mercato (come la frutta che si coglie acerba e si matura artificialmente secondo le esigenze di consumo, facendogli perdere il sapore). In un periodo del genere, i testi scientifici teorici hanno una funzione culturale in più, perché sollecitano una riflessione seria sul rapporto tra scienza e tecnologia. Un rapporto corretto esclude ogni forma di arroganza, imponendo un rispetto reciproco, un atteggiamento di collaborazione, ma anche di consapevolezza delle diverse finalità e vocazioni. Una domanda di fondo, a cui spesso ho dovuto rispondere durante il mio insegnamento, è: "Ma a che serve?" Prevenendo il lettore incredulo, fornisco subito una risposta a effetto, prendendo in prestito le parole da Kant: "Niente è più utile di una buona teoria!"

Sento il bisogno di menzionare varie persone verso cui sono legato da un debito di riconoscenza, e a cui, a vari livelli e in modi diversi, devo qualcosa per la realizzazione del libro: Alessandro Berarducci, Alfonso Caracciolo di Forino, Santi Carta, Salvatore Ciampa, Matteo Coccia, Erzsebet Csuhaj-Varju, Ennio De Giorgi, Alex Küronya, Beppe Longo, Fabrizio Luccio, Roberto Magari, Solomon Marcus, Carlos Martín-Vide, Marco Martino, Andrea Masini, Istvan Némethi, Nello Onesto, Gheorghe Păun, Nino Salibra, Pippo Scollo.

Vincenzo Manca

Pisa, 19 settembre 2000

Logica matematica

A Elena

La logica formale di Aristotele, con la teoria dei sillogismi, costituisce il primo studio sistematico delle regole deduttive. La novità fondamentale dell'impostazione aristotelica consiste nell'aver compreso che la struttura logica di certe deduzioni dipende dalla loro *forma* a prescindere dal significato specifico delle proprietà che in esse compaiono. A partire dalla seconda metà dell'Ottocento, i logici hanno sviluppato l'aspetto formale della logica, elaborando in modo radicalmente nuovo una notazione simbolica per rappresentare proposizioni e deduzioni. Si parla equivalentemente di logica simbolica o matematica, in quanto lo sviluppo della componente simbolica è intrinsecamente collegato al processo di matematizzazione della logica e a una tendenza generale della matematica verso l'astrazione, il metodo assiomatico e la ricerca dei suoi concetti fondamentali.

L'elaborazione di un metodo simbolico-matematico ha avuto come pioniere Leibniz (1646-1716) e risultati nodali nelle ricerche di De Morgan (1806-1871), Boole (1815-1864), Peirce (1839-1914), Schröder (1841-1902), Frege (1848-1925), Peano (1858-1932), Hilbert (1862-1943), Russell (1872-1970), Löwenheim (1878-1957), Skolem (1887-1963), Post (1897-1954), Tarski (1901-1983), Church (1903-1995), Gödel (1906-1978), Herbrand (1908-1931), Gentzen (1909-1945), Kleene (1909-1994), Turing (1912-1954).

L'aspetto basilare del metodo matematico consiste nella definizione di un *linguaggio formale* in cui, a differenza che nei linguaggi naturali, si distingue nettamente tra *sintassi* e *semantica*. La sintassi stabilisce quali sequenze di simboli sono da considerarsi ben formate; la semantica stabilisce come interpretare le espressioni simboliche sintatticamente corrette. Dalla definizione rigorosa di interpretazione conseguono quelle di verità, conseguenza e indipendenza logica.

La distinzione tra sintassi e semantica non va intesa in modo contrapposto, ma complementare. Infatti, la sintassi definita a prescindere dalla se-

mantica rende possibile l'elaborazione simbolica delle proposizioni tramite veri e propri calcoli. La semantica, nella sua generalità, può rendere rigorosa l'intuizione di Leibniz secondo cui le proposizioni logicamente valide sono quelle vere in tutti i mondi possibili.

Una chiara e rigorosa definizione di un linguaggio logico, attraverso una definizione matematica della sua sintassi e semantica, fu raggiunta a opera della scuola logica di Varsavia e il passo decisivo in tal senso fu fatto da Alfred Tarski intorno al 1930.

Sintassi e semantica sono i due filoni concettuali che sovrintendono alle due principali discipline della logica matematica: la *teoria della dimostrazione* e la *teoria dei modelli*.

La teoria della dimostrazione è collegata alla nozione di procedimento effettivo e quindi ai concetti di algoritmo e di calcolo. Questi costituiscono l'oggetto di studio della *teoria della calcolabilità*, sviluppatasi in modo autonomo dopo il fondamentale lavoro di Alan Mathison Turing (1936). In tale lavoro era dato il primo modello matematico di calcolatore; i contributi di Post, Gödel, Church, Julia Robinson, Kleene, Curry, e von Neumann determinarono le linee principali di sviluppo di questa teoria in connessione allo studio matematico dei *linguaggi formali* e degli *automi*.

La teoria dei modelli, sin dal suo nascere, è stata collegata a teorie fondamentali della matematica: la teoria degli insiemi, l'aritmetica, le teorie delle strutture algebriche e geometriche. Intorno al 1960, elaborando concetti di tale teoria, Abraham Robinson ha introdotto la cosiddetta *analisi non standard* che, aprendo prospettive del tutto nuove, forniva una base rigorosa alle intuizioni di Leibniz sul calcolo infinitesimale, in contrapposizione alla formalizzazione di Cauchy e Weierstrass (basate sulla definizione ε - δ di limite).

L'estensione dei metodi della logica formale a campi diversi dalla matematica ha avuto uno sviluppo notevole a partire dalla seconda metà del Novecento, spesso in ripresa di classici temi filosofici o di approcci alternativi ai fondamenti della matematica. Infatti, molte formalizzazioni richiedono la rappresentazione logica di concetti che vanno al di là delle situazioni tipiche della matematica: contesti spazio-temporali, modali, o epistemici, processi di calcolo, ragionamenti approssimati o incerti, rappresentazioni della conoscenza. Tutti questi settori costituiscono il reame delle logiche cosiddette non classiche o alternative quali: *logica modale*, *intuizionista*, *temporale*, *intensionale*, *lineare*.

Questo ampio spettro di applicazioni dimostra la vitalità della logica matematica. Inoltre l'importanza che tutti i temi non classici hanno per l'informatica teorica e la centralità della logica nella ricerca di processi di automazione del ragionamento giustificano il legame profondo tra le due discipline. In tal senso, il rapporto tra Logica e Informatica (teorica) può essere paragonato a quello tra Analisi Matematica e Fisica.

Il nucleo di partenza di quasi tutti i sistemi logici è costituito dalla cosiddetta logica predicativa, che costituirà l'argomento centrale di questo testo. Prima di intraprendere il suo studio, daremo una sintetica presentazione dei concetti fondamentali della matematica.

Tale capitolo iniziale ha due motivazioni distinte e complementari. Infatti, il rapporto tra la logica matematica e i fondamenti della matematica è stato duplice. Dal punto di vista storico, l'inizio della logica matematica coincide con quello di una *logica per la matematica*: un'analisi rigorosa di concetti e principi su cui basare le teorie matematiche al riparo dai paradossi scoperti a partire dalla fine dell'Ottocento. Era questo lo spirito basilare delle ricerche di Frege, Peano, Russell, Hilbert (metamatemica). Tuttavia, strettamente connessa alla prima, si poneva un'altra ricerca, quella di una *matematica per la logica*: matematizzare i procedimenti deduttivi per analizzare i concetti di interpretazione, conseguenza logica e deduzione. Era questo l'evidente intento dei lavori di Boole, Hilbert, Gödel, Herbrand, Gentzen.

La teoria quadro in cui queste due tendenze si sono incontrate, arricchendosi a vicenda, è la teoria degli insiemi, ovvero il *paradiso di Cantor* dove (con anticipazioni nelle ricerche di Bernard Bolzano) questo grande pensatore era approdato, a partire da problemi di analisi (serie di Fourier), formulando in maniera radicalmente nuova il problema dell'infinito matematico e scoprendone una vertiginosa gamma di possibili gradi. Entro questo paradiso, una valle centrale è rappresentata dai principi di induzione che sono alla base di tutte le strutture tipiche della matematica discreta (strutture aritmetiche, sintattiche e in qualche senso finitiste). Per analogia, potremmo parlare in questo caso di un *paradiso di Peano* (o forse meglio di Grassmann, Dedekind e Peano).

Insiemi e induzione sono strumenti basilari di qualsiasi officina entro cui si producono le macchine per esplorare e viaggiare nei mondi del pensiero matematico. Teoria degli insiemi e induzione forniscono in particolare gli strumenti matematici per una rigorosa definizione della sintassi e semantica della logica predicativa.

Capitolo I

Fondamenti matematici

Presenteremo brevemente i concetti di operazione, numero e classe. A partire da essi definiremo le altre nozioni matematiche fondamentali di relazione, equivalenza, ordinamento, insieme, sequenza, funzione e induzione. In senso lato, una struttura matematica è un'entità definita in termini di tali concetti basilari. La loro individuazione come nozioni matematiche fondamentali, suscettibili a loro volta di analisi matematica, costituisce l'essenza e in un certo senso l'inizio della logica matematica.

Useremo spesso la freccia $\Rightarrow$ per indicare l'usuale *implicazione matematica* (*se allora*), la doppia freccia $\Leftrightarrow$ per indicare l'*equivalenza* tra proposizioni (*se e solo se* abbreviato anche con *sse*), il segno $=$ per l'*uguaglianza* e il segno $\equiv$ per indicare un'uguaglianza posta per definizione.

Nel seguito, si introdurranno simboli, espressioni simboliche e terminologia che verrà spiegata di volta in volta, tuttavia, è bene avvertire subito il lettore che spesso uno stesso simbolo o uno stesso termine può assumere significati diversi in base al contesto in cui viene usato. In linea di principio tale fenomeno potrebbe essere evitato, ma sia per economia espositiva (è dispendioso introdurre simboli che hanno un uso strettamente locale a un dato discorso), sia per aderenza all'uso simbolico corrente, seguiremo la tendenza matematica abituale di *predicare bene* (rigore assoluto) e *razzolare male* (non troppo assoluto, altrimenti si diventa pedanti). Basta un poco di cautela e di collaborazione da parte del lettore per evitare confusioni grossolane e intendersi bene lo stesso, senza dovere spendere troppe energie nel controllo della coerenza espressiva che, quando diventa assoluta, spesso è antagonista della comprensione (il saggio in appendice spiega che il formalismo estremo va bene solo per le macchine, e tra l'altro gli sforzi attuali sono rivolti a sollevare anche queste verso forme di comunicazione *intelligente*).

1.1. Operazioni, numeri e classi

Operazioni, classi e numeri naturali sono i concetti alla base di qualsiasi teoria matematica.

Un'operazione è una *regola* che si può applicare a un *argomento* producendo un *risultato*.

Quando f è applicabile all'argomento a , si dice anche che f è definita su a . In tal caso il risultato dell'applicazione si indica con

$$f(a).$$

Quando, in corrispondenza all'argomento a , f non produce alcun risultato si scrive

$$f(a) \uparrow$$

o anche

$$f(a) = \uparrow.$$

Una *classe* è una collezione di oggetti completamente determinata dagli elementi che a essa appartengono. La classe costituita dagli elementi $a_1, \dots, a_k$ si indica con $\{a_1, \dots, a_k\}$. Per indicare che a è un *elemento* o membro della classe A , si scrive $a \in A$ (o anche $A \ni a$), mentre, per indicare che a non è elemento di A , si scrive $a \notin A$ (o anche $A \not\ni a$). Date due classi A e B , si dice che A è *inclusa* o contenuta in B , o anche che A è *sottoclasse* di B , quando tutti gli elementi di A sono anche elementi di B . Si scrive $A \subseteq B$ per indicare che A è inclusa in B , senza escludere che A possa essere uguale a B , mentre si scrive $A \subset B$ per indicare che A è contenuta strettamente o propriamente in B , escludendo quindi l'uguaglianza tra le due classi (o equivalentemente, invertendo l'ordine delle classi e orientando i simboli di inclusione al contrario).

La classe priva di elementi si indica con $\emptyset$ e si dice *classe vuota*. Ovviamente la classe vuota è inclusa in ogni classe. Si indica con $\mathbb{N}$ la classe dei numeri naturali $\{0, 1, 2, 3, \dots\}$. Le classi si rappresentano spesso con cerchi i cui punti interni (o solo alcuni di essi) rappresentano i relativi elementi. I diagrammi che ne risultano si dicono *diagrammi di Venn*.

Per l'applicazione di un'operazione vi sono varie notazioni; indichiamo qui di seguito le più comuni:

- $f(a)$ notazione prefissa con parentesi;
- fa notazione prefissa;
- $(a)f$ notazione postfissa con parentesi;
- af notazione postfissa;
- f_a notazione indicizzata (con pedice).

Delle notazioni sopra menzionate le prime due sono quelle di gran lunga più usate nella matematica occidentale. Le altre si usano in contesti piuttosto limitati. È evidente che tale preferenza notazionale affonda le radici nella tradizione più diffusa di scrivere da sinistra verso destra. Benché si tratti di una mera scelta convenzionale, le radici storiche e psicologiche di tale uso sono molto profonde (legate alle coppie antitetiche destra/sinistra, orario/antiorario); cambiare abitudine notazionale diventa estremamente disorientante, soprattutto quando i sistemi simbolici raggiungono una certa complessità. In un sistema notazionale di tipo prefisso può apparire la notazione postfissa, ma solo in poche situazioni, generalmente per distinguere dei casi speciali.

La distinzione tra argomento e operazione è una convenzione che non ha un carattere assoluto, ma relativo alla teoria in cui ci si pone. Essa è legata alla distinzione tra prefisso e postfisso. Infatti, la scrittura fa ha due possibili letture: I) f è l'operazione, II) a è l'argomento, III) fa il risultato dell'applicazione; oppure, in modo simmetrico: I) f è l'argomento, II) a è l'operazione, III) fa il risultato dell'applicazione.

Una teoria matematica è ben costruita quando in essa la simbologia e la terminologia hanno la capacità di evocare immagini mentali che collimano con i concetti rappresentati, entrando in risonanza con le loro potenzialità di sviluppo. Leibniz, che fu matematico oltre che filosofo e pioniere della moderna logica matematica, da profondo studioso dei sistemi simbolici, usava paragonarli, in modo suggestivo, al *filo di Arianna* seguendo il quale la mente umana può districarsi nel labirinto dei concetti. La storia della matematica conferma tale intuizione. Basti considerare la fioritura dell'algebra moderna a partire dagli algebristi italiani del Rinascimento, dopo l'introduzione in Europa del sistema di rappresentazione posizionale indoarabico da parte del matematico del XII secolo Leonardo Fibonacci (detto anche Leonardo Pisano).

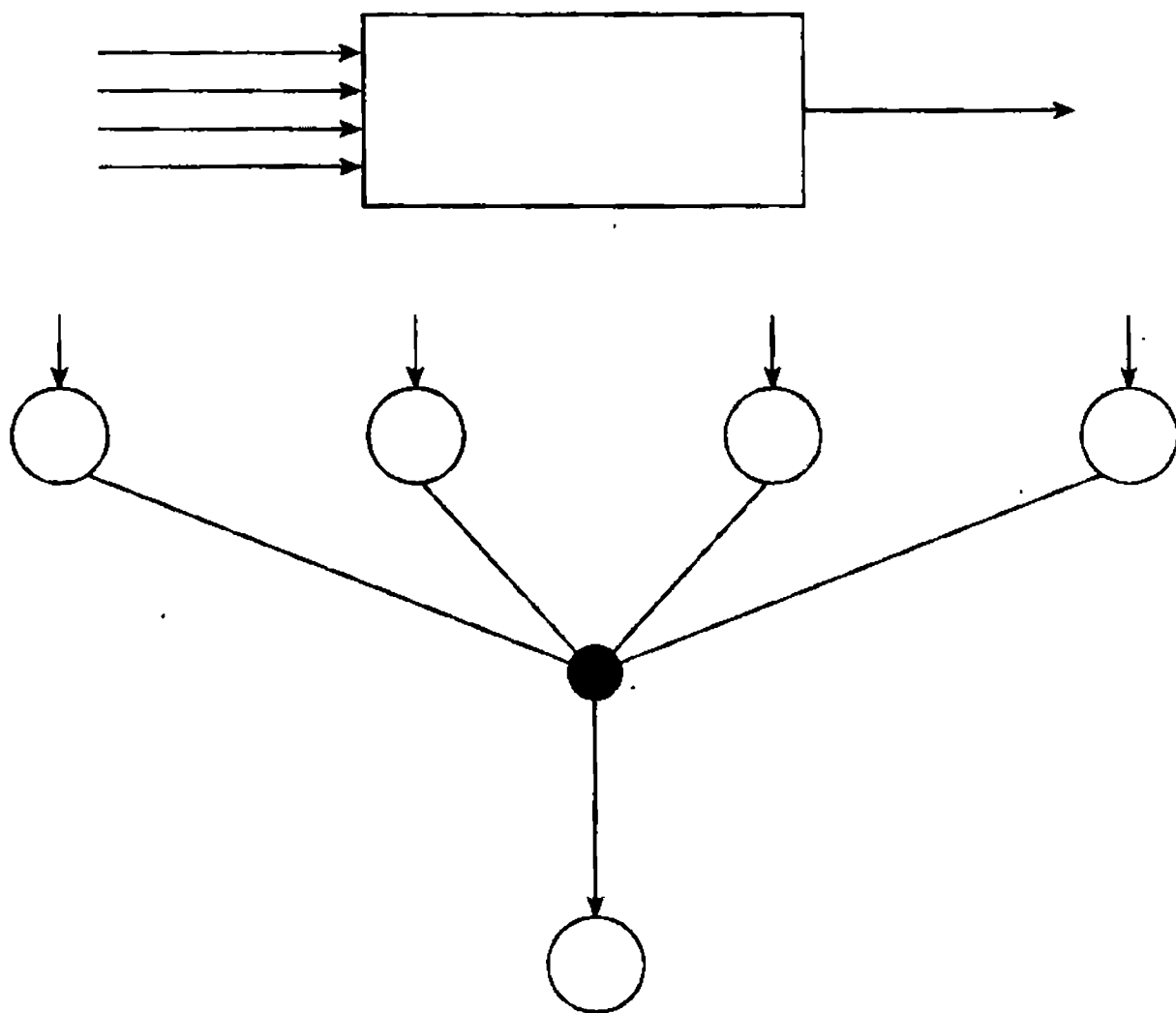
L'intuizione sottostante al concetto di operazione si può illustrare considerando alcuni modelli fisici di operazioni. Il modello associativo è quello basato sulla metafora contenente/contenuto. Un'operazione intesa in questo senso è rappresentata da un contenitore suddiviso in locazioni entro le quali sono posti degli elementi. Applicare l'operazione a una locazione equivale a prelevare l'elemento in essa contenuto. Tale intuizione si ritrova nelle tabelle, nei dizionari e nelle memorie elettroniche. Il modello di tipo compositivo è basato sulla metafora componenti/composto. In tal caso l'applicazione consiste nel comporre un oggetto mettendone insieme degli altri. Tale nozione si ritrova nella composizione di composti chimici, nella costruzione di strutture sintattiche e in genere nella formazione di oggetti complessi. Infine, il modello trasformativo è quello basato sulla metafora stato/evento presente in tutti i verbi di cambiamento (aprire, accendere, tagliare, allonta-

nare, ruotare, ...). Tale nozione si ritrova in fisica e in tutti i fenomeni che determinano un cambiamento di stato. Secondo tale punto di vista, l'applicazione consiste nel dare l'avvio a un processo che trasforma una configurazione di partenza ottenendone una finale.

Un'operazione f può essere definita su più argomenti, considerati in un dato ordine; se f è definita sui k argomenti $a_1, \dots, a_k$ appartenenti a una classe A , allora

$$f(a_1, \dots, a_k)$$

indica il risultato dell'applicazione e in tal caso si dice che f è un'operazione k -aria o k -argomentale o di *arietà* k (definita) sulla classe A . Se f è definita su ogni possibile scelta di k argomenti di A , allora si dice sempre definita o *totale* su A . L'operazione f si dice *chiusa* in A (o anche A si dice chiusa rispetto a f) se f è totale su A e se, applicando f ad argomenti di A , si ottiene sempre un risultato che è in A . Le seguenti sono alcune rappresentazioni diagrammatiche di operazioni a 4 argomenti.

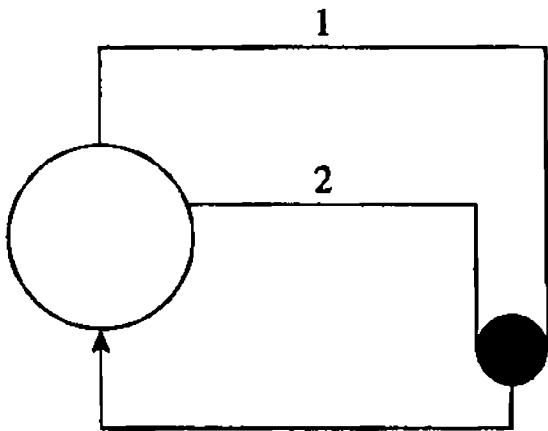


Se $*$ è un'operazione binaria, allora l'applicazione si indica spesso con la notazione infissa, che si dice notazione moltiplicativa (perché adottata frequentemente per la usuale moltiplicazione numerica).

La somma, il prodotto, la differenza, la divisione sono operazioni 2-arie (binarie) sulla classe $\mathbb{N}$ dei numeri naturali. Le prime due sono chiuse su $\mathbb{N}$, mentre le ultime due, su tale classe, sono talvolta indefinite.

Un'operazione $*$ binaria si dice *associativa* se dati tre oggetti qualsiasi x, y, z vale $(x * y) * z = x * (y * z)$. La somma e il prodotto di numeri sono operazioni associative, mentre la differenza e la divisione non lo sono.

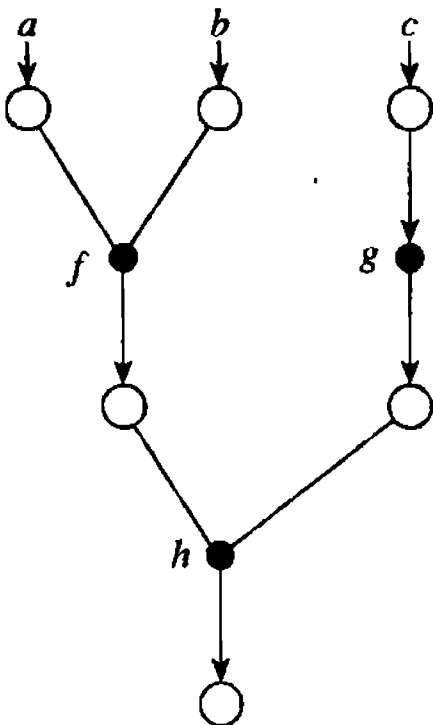
La seguente è una rappresentazione diagrammatica di un'operazione binaria definita su una classe (i numeri indicano l'ordine degli argomenti):



L'applicazione multipla di operazioni a certi argomenti si indica con espressioni operatorie costruite con simboli di parentesi, secondo l'usuale metodo algebrico.

$$h(f(a, b), g(c))$$

Indica l'applicazione di tre operazioni f, h, g di cui le prime due sono binarie e l'ultima è unaria, secondo l'ordine espresso geometricamente dal diagramma:



1.2. Proprietà e relazioni

Una *proprietà* è un'operazione che, dato un oggetto come argomento, può fornire come risultato uno tra due possibili valori, usualmente detti *valori di verità*, e indicati con 0, 1 (falso, vero). Si scrive semplicemente $P(a)$ per indicare che $P(a) = 1$ e si dice in tal caso che la proprietà P vale sull'oggetto a , ovvero che l'oggetto a soddisfa la proprietà P . Se $P(a) = 0$, spesso si sbarra il simbolo P in $P(a)$ e si dice che la proprietà P non vale sull'oggetto a . Una proprietà di arietà $k \geq 2$ su una classe A si dice più propriamente una *relazione* k -aria o k -argomentale su A .

Esempi di proprietà aritmetiche sono quella di numero pari, dispari, primo; relazioni aritmetiche binarie sono l'uguaglianza, l'ordinamento, la divisibilità tra numeri, la congruenza rispetto a un numero n (quando i due numeri, divisi per n danno lo stesso resto). Esempi di relazioni geometriche (binarie) sono l'appartenenza di un punto a una retta, il parallelismo tra rette, la congruenza di segmenti, l'allineamento di punti.

Sia R una relazione binaria totale su una classe A , useremo la *notazione infissa* xRy in alternativa alla notazione $R(x, y)$. Le seguenti sono notevoli proprietà di relazioni.

R è *simmetrica* se per ogni $x, y \in A$: $xRy \Rightarrow yRx$.

R è *antisimmetrica* se per ogni $x, y \in A$: $(xRy \text{ e } yRx) \Rightarrow x = y$.

R è *transitiva* se per ogni $x, y, z \in A$: $(xRy \text{ e } yRz) \Rightarrow xRz$.

R è *riflessiva* se per ogni $x \in A$: xRx .

R è *lineare* o *totale* se per ogni $x, y \in A$: xRy oppure yRx .

R è *irriflessiva* se per ogni $x \in A$ non vale: xRx .

R è *connessa* se per ogni $x \in A$ esiste un $y \in A$: xRy .

R è un *ordinamento stretto* se è irriflessiva e transitiva.

R è un *preordine* o un *quasi ordine* se è riflessiva e transitiva.

R è un' *equivalenza* se è riflessiva, simmetrica e transitiva.

R è un *ordinamento* se è un preordine e se è antisimmetrica.

Le relazioni binarie si rappresentano naturalmente con diagrammi costituiti da *nodi* e *freccie*. Una freccia che connette due nodi esprime che tra di essi vale la relazione. In tal modo simmetria, riflessività e transitività sono raffigurabili con diagrammi costituiti rispettivamente da componenti del tipo seguente:



Nelle relazioni di ordinamento l'orientamento delle frecce in genere si sostituisce con un ordine verticale dei nodi, e quindi le frecce sono rimpiazzate da semplici linee. I diagrammi che ne risultano si dicono *diagrammi di Hasse*. Data una relazione di equivalenza R su una classe A e un elemento a di A , si indica con $[a]_R$ (omettendo l'indice R quando arguibile dal contesto) la *classe di equivalenza* di a rispetto a R , ovvero la classe di tutti gli elementi di A che sono equivalenti ad a , rispetto a R . La classe $A/R = \{[a]_R \mid a \in A\}$ delle classi di equivalenza dicesi *classe quoziente* di A rispetto a R .

Sulle relazioni si definiscono le seguenti operazioni notevoli.

1. La *composizione* $R \mid Q$ di due relazioni binarie R e Q è la relazione binaria tale che $x(R \mid Q)y$ sse esiste un oggetto z per cui xRz e zQy . Per esempio, *zio* è la composizione delle relazioni binarie *fratello* e *padre*.
2. La relazione *inversa* R° della relazione binaria R è la relazione binaria tale che xR° sse yRx . Per esempio, *figlio* è la relazione inversa della relazione *padre*.
3. La *concatenazione* $S * T$ delle relazioni S, T di arietà rispettivamente k e h è la relazione di arietà $k + h$ tale che $(S * T)(x_1, \dots, x_k, y_1, \dots, y_h)$ sse $S(x_1, \dots, x_k)$ e $T(y_1, \dots, y_h)$.

1.3. Ordinamenti

Gli ordinamenti si indicano solitamente con il segno $\leq$ o con segni simili. Se tra due elementi vale la relazione di ordinamento essi si dicono *confrontabili* (secondo l'ordinamento), altrimenti si dicono *inconfrontabili*. Spesso si parla di *ordinamento parziale* o di *semiordine* quando si vuole rimarcare che non si ha la linearità. Un ordinamento lineare si dice anche *catena*, o *ordine totale*. Dato un ordine totale su una classe A e un suo elemento x , il *segmento* di x in A è costituito da tutti gli elementi di A minori di x . Data una sottoclasse $B \subseteq A$, un elemento $b \in A$ dicesi *maggiorante* di B se $x \leq b$ per ogni $x \in B$, mentre dicesi *minorante* di B se $b \leq x$ per ogni $x \in B$. Un elemento a di una classe A si dice *minimale* in A se non esiste nessun altro elemento x tale che $x \leq a$; si dice invece *massimale* se non esiste nessun altro elemento x tale che $a \leq x$. L'elemento $a \in A$ è il *minimo* di A , indicato con $\min(A)$, se è minore di tutti gli elementi di A ed è il *massimo* di A , indicato con $\max(A)$, se tutti gli elementi di A sono minori di a . Data una sottoclasse B di A , il massimo dei minoranti di B (se esiste) dicesi *estremo inferiore* di B , e si indica con $\inf(B)$, mentre il minimo dei maggioranti di B (se esiste) dicesi *estremo superiore* di B e si indica con $\sup(B)$. Una sottoclasse B di A si dice *limitata superiormente* (rispettivamente, *limitata inferiormente*) se tutti i suoi elementi sono minori (rispettivamente, maggiori) di qualche elemento

di A . Un ordinamento in cui ogni coppia di elementi ha un estremo superiore si dice *diretto* all'insù, mentre se ogni coppia di elementi ha un estremo inferiore dicesi diretto all'ingiù. Un ordinamento diretto nei due sensi si dice *reticolo*. Un ordinamento in cui ogni sua sottoclasse ha estremo inferiore e superiore si dice *ordinamento completo*. Un reticolo in cui esiste un massimo, diciamolo 1 e un minimo, diciamolo 0, si dice *complementato* se per ogni suo elemento x esiste il suo complemento x' tale che $\sup(\{x, x'\}) = 1$ e $\inf(\{x, x'\}) = 0$. Un reticolo è *distributivo* se le operazioni di $\sup$ e $\inf$ tra due elementi sono ciascuna distributiva rispetto all'altra (nello stesso senso in cui l'ordinario prodotto è distributivo rispetto alla somma). Un reticolo complementato e distributivo è un'*algebra di Boole*. Molte nozioni definite sugli ordinamenti si estendono in modo del tutto naturale agli ordinamenti stretti e ai preordini.

Una classe ordinata si dice *densa* se per ogni coppia di suoi elementi $a \leq b$ esiste un elemento c maggiore del primo e minore del secondo. Una classe che non è densa dicesi *discreta*.

In una classe ordinata A un *salto* è una sottoclasse B di A tale che B ha massimo e $A - B$ (definita in §1.4) ha minimo. Mentre B è una *lacuna* se B non ha massimo e $A - B$ non ha minimo.

Una classe ordinata si dice *continua* se non ha né salti né lacune.

Una classe ordinata si dice *completa* se ogni sua sottoclasse limitata inferiormente ha estremo inferiore.

1.4. Insiemi

Una classe è completamente ed esclusivamente individuata dagli oggetti che ad essa appartengono, detti suoi elementi o membri. Per le classi valgono i seguenti princìpi:

1. *Principio di comprensione*: una qualsiasi proprietà P determina la classe costituita da tutti gli oggetti che soddisfano P , indicata usualmente con $\{x \mid P(x)\}$.
2. *Principio di estensione*: due classi sono uguali sse contengono gli stessi elementi.
3. *Principio di dicotomia*: dato un oggetto a e una classe A , è necessariamente $a \in A$ oppure $a \notin A$.

In base al principio di estensione, due classi ciascuna delle quali è inclusa nell'altra sono uguali.

Indichiamo con (a, b) una *coppia ordinata* di elementi. È ormai consuetudine identificare tale coppia con la classe $\{a, \{a, b\}\}$ (detta *coppia di Kuratowski*), o con l'operazione definita sulla classe $\{1, 2\}$ tale che: $(a, b)(1) = a$ e

$(a, b)(2) = b$. Le due rappresentazioni sono del tutto equivalenti (entrambe permettono di individuare gli elementi della coppia, distinguendone uno come primo).

Sulle classi si definiscono le seguenti operazioni dell'*algebra delle classi*. Siano A, B due classi.

- l'unione $A \cup B$ è la classe i cui elementi appartengono alla classe A o alla classe B ;
- l'intersezione $A \cap B$ è classe cui elementi appartengono sia ad A che a B ;
- la classe differenza $A - B$ è la classe i cui elementi appartengono ad A e non appartengono a B ;
- la classe delle parti $\mathcal{P}(A)$ è la classe i cui elementi sono le sottoclassi di A ;
- la classe prodotto cartesiano $A \times B$ è la classe i cui elementi sono le coppie (x, y) in cui $x \in A$ e $y \in B$;
- l'unione estesa di una classe A i cui elementi sono classi è la classe $\bigcup A$ in cui ciascun elemento appartiene a qualche classe che è elemento di A ;
- l'intersezione estesa di una classe A , i cui elementi sono classi, è la classe $\bigcap A$ degli elementi, comuni a tutte le classi, che sono elementi di A .

La proposizione seguente mostra che la nozione intuitiva di classe solleva subito problemi logici notevoli e richiede alcune precauzioni senza le quali si ottengono contraddizioni. I problemi intrinseci al concetto intuitivo di classe derivano dalle classi che possono essere elementi di altre classi.

Proposizione 1.1 (paradosso di Russell) *La nozione intuitiva di classe è contraddittoria: il principio di comprensione e quello di dicotomia non possono valere contemporaneamente.*

Dimostrazione Consideriamo la classe R delle classi che non sono elementi di se stesse:

$$R = \{X \mid X \notin X\}$$

tal definizione può apparire strana, eppure è ottenuta in modo del tutto legittimo utilizzando il principio di comprensione. È semplice trovare casi di classi che non appartengono a se stesse, per esempio, la classe vuota è una tale classe; è invece meno evidente fornire esempi di classi che appartengono a se stesse: la classe di tutte le classi non vuote, essendo non vuota (vi appartiene per esempio la classe dei naturali), appartiene a se stessa. Tornando alla classe R appena definita, osserviamo che, in base al principio di dicotomia, deve valere una delle due possibilità:

$$R \in R \quad \text{oppure} \quad R \notin R.$$

Se $R \in R$, allora R deve soddisfare la condizione $X \notin X$ che caratterizza tutti gli elementi di R , quindi $R \notin R$, il che è assurdo. D'altra parte, se $R \notin R$, allora R soddisfa la condizione che definisce R , quindi $R \in R$, e questo è un altro assurdo. ■

La possibilità di classi a vari livelli di astrazione (classi di classi di classi ...) non è una astratta curiosità logica, ma una caratteristica che si rivela essenziale per rappresentare importanti concetti matematici. Il paradosso di Russell impone però grande cautela nella definizione di classi i cui elementi sono ancora classi.

La definizione della classe di Russell utilizza un meccanismo definitorio detto *impredicativo*. In generale, una definizione di un oggetto matematico si dice *impredicativa* quando le condizioni che determinano l'oggetto vengono formulate assumendo una totalità che include l'oggetto che si sta definendo. Alcune soluzioni al paradosso di Russell erano basate su metodi per la regolazione delle definizioni impredicative, che tuttavia non possono essere completamente evitate senza perdite notevoli nell'espressività del linguaggio matematico (la definizione di minimo di una classe è per esempio impredicativa).

Un altro modo per superare il paradosso di Russell consiste nel considerare una forma limitata del principio di comprensione, nota come *principio di separazione* o di *isolamento*, secondo cui, data una classe A e una proprietà P , si può sempre considerare la classe $\{x \in A \mid P(x)\}$ degli elementi di A che verificano P . In tal modo l'argomento di Russell dimostra solamente che $\{X \in A \mid X \notin X\}$ non può appartenere ad A .

Tale intuizione è alla base della teoria assiomatica ZF (di Zermelo Fraenkel) estesa poi in ZFC (C sta per *choice*; vedi oltre) sviluppata da Thoralf Skolem, Ernst Zermelo e Adolf Fraenkel. Gli assiomi di tale teoria permettono di costruire delle classi, dette *insiemi*, che evitano il paradosso di Russell, stabilendo degli insiemi iniziali e dei procedimenti che permettono di costruire nuovi insiemi da insiemi già dati (vedi § 4.1 per la lista completa degli assiomi di ZFC).

La soluzione NBG (di von Neumann, Bernays, Gödel) considera classi e insiemi. Gli insiemi sono classi che sono a loro volta elementi di classi. Una *classe propria* è una classe che non è elemento di nessuna classe. A questo punto, nel principio di comprensione la proprietà rispetto a cui si astrae si intende riferita solo a insiemi. In tal modo il paradosso di Russell diventa una dimostrazione del fatto che la classe di Russell è una classe propria. Gli assiomi di NBG forniscono delle condizioni affinché certe classi siano insiemi.

Si dimostra che le due teorie ZFC e NBG sono "equivalenti" nel senso che descrivono gli stessi insiemi, cioè, se una proposizione "parla" solo di insiemi, allora essa è deducibile in ZFC se e solo se è deducibile in NBG (si

dice che NBG è un'estensione conservativa di ZFC). Molte altre sono le proposte di teorie degli insiemi o di altre teorie per ovviare al paradosso di Russell. Qui assumeremo una nozione di insieme che corrisponde essenzialmente a quella assiomatizzata secondo ZFC.

Assumiamo la nozione di classe nella sua accezione matematica non assiomatizzata di collezione o di aggregato o di estensione $\{x \mid P(x)\}$ di una proprietà P . Per gli insiemi sono postulate le condizioni seguenti:

1. Ogni insieme è una classe (e quindi verifica il principio di estensionalità e di dicotomia).
2. Una classe inclusa in un insieme è un insieme.
3. Le usuali operazioni tra classi (unione estesa, coppia, prodotto, parti), applicate a insiemi, producono ancora insiemi.
4. La classe dei numeri naturali è un insieme (vedi oltre, § 1.10).

A tali assiomi sono da aggiungere gli assiomi di *rimpiazzamento* e di *scelta* che verranno introdotti più avanti.

Gli insiemi numerici degli interi, dei razionali e dei reali sono indicati solitamente con $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Essi sono tutti definibili insiemisticamente (con procedimenti ormai standard) a partire dai naturali.

Esercizio 1.1 *Spiegare in dettaglio perché il principio di separazione permette di evitare il paradosso di Russell.*

Esercizio 1.2 *Si definiscano insiemisticamente i numeri interi come classi di equivalenza di coppie di naturali. Quindi si definiscano i razionali come classi di equivalenza di coppie di interi.*

1.5. Funzioni

Dati due insiemi A e B , una *funzione* f da A in B (che va da A in B , o manda A in B) è un'operazione tale che, per ogni $x \in A$, se $f(x)$ è definita, allora $f(x) \in B$. In tal caso si scrive

$$f: A \rightarrow B.$$

L'elemento $f(x)$ si dice anche l'*immagine* di x in B (tramite f). Gli insiemi A e B si dicono rispettivamente *dominio* e *codominio* di f , e si scrive $A = \text{dom}(f)$, $B = \text{cod}(f)$.

Se $f(x)$ è definita per ogni $x \in A$, allora la funzione f dicesi *totale*. Almeno di esplicita dichiarazione, per "funzione" si intenderà sempre una funzione totale; per indicare che una funzione non è totale si dice che è *parziale*.

Data una funzione $f: A \rightarrow B$, se X è un sottoinsieme di A , si indica con $f[X]$ (o anche $f(X)$ se ciò non è ambiguo) l'*insieme immagine* di X tramite f :

$$f[X] = \{f(x) \in B \mid x \in X\},$$

mentre se Y è un sottoinsieme di B , si indica con $f^{-1}[Y]$ l'*insieme controimmagine* di Y tramite f :

$$f^{-1}[Y] = \{x \in A \mid f(x) \in Y\}.$$

L'*assioma di rimpiazzamento*, che qui assumiamo, afferma che l'*immagine di un insieme tramite una funzione è ancora un insieme*.

Una funzione $f: A \rightarrow B$ dicesi *iniettiva* se associa risultati diversi ad argomenti diversi e in tal caso scriveremo anche $f: A \hookrightarrow B$; f dicesi *surgettiva* se B coincide con la classe $f[A]$ e in tal caso scriveremo anche $f: A \twoheadrightarrow B$; f si dice *biunivoca* o *bigettiva* se è contemporaneamente iniettiva e surgettiva; in tal caso scriveremo anche $f: A \leftrightarrow B$. Se f è biunivoca (e totale), allora si dice anche che f stabilisce una *corrispondenza 1-1* tra gli insiemi A e B ; è quindi possibile definire la funzione f^{-1} (biunivoca e totale) da B in A , detta *funzione inversa* di f , che fa corrispondere ad ogni $y \in B$ l'unico x di A per cui $f(x) = y$. Un insieme A dicesi *numerabile* se esiste una corrispondenza 1-1 tra l'insieme A e l'insieme $\mathbb{N}$ dei numeri naturali. Una funzione il cui dominio coincide con i numeri naturali si dice anche *successione*.

Se $f: A \rightarrow B$ e $C \subset A$ la *restrizione* di f a C , indicata con $f|_C$, è la funzione da C in B che sugli elementi di C produce in B le stesse immagini di f (e quando non è ambiguo si continua a indicarla con f). Se $f: A \rightarrow B$ e $g: B \rightarrow C$, la *composizione* di g con f , indicata con $g \circ f: A \rightarrow C$, è la funzione (di dominio A e codominio C) definita ponendo $(g \circ f)(x) = g(f(x))$ per ogni $x \in A$. La *funzione identità* su un insieme A , indicata con $i_A: A \rightarrow A$, è tale che $i_A(x) = x$ per ogni $x \in A$.

Un'operazione è identificabile con il suo grafico, ovvero con la classe delle sue coppie (argomento, risultato). Viceversa, una classe di coppie che non contiene coppie distinte con la medesima prima componente rappresenta il grafico di un'operazione. Una funzione f da un insieme A a un insieme B è quindi identificabile con un insieme di coppie che siano grafico di un'operazione e tali che le loro prime componenti costituiscono l'insieme A e le seconde componenti appartengono a B .

La terminologia riguardante operazioni, relazioni e funzioni non è uniforme: in certi contesti si usa il termine *operatore* o *funtore* per designare un'operazione (e/o il simbolo con cui si indica), i termini *corrispondenza*, *associazione*, per indicare relazioni binarie e i termini *applicazione*, *mappa* per indicare funzioni. L'insieme delle funzioni da un insieme A a un insieme B si indica con B^A o anche con $(A \rightarrow B)$.

Dato un insieme di *indici* I , l'insieme $\{f_i \mid i \in I\}$ delle immagini tramite f dicesi *indicizzato* in I , o *I -indicizzato*.

Una *famiglia* F è una funzione definita su un insieme I di elementi, detti *indici*, le cui immagini sono insiemi; si adotta usualmente la seguente notazione: $F = (F_i \mid i \in I)$.

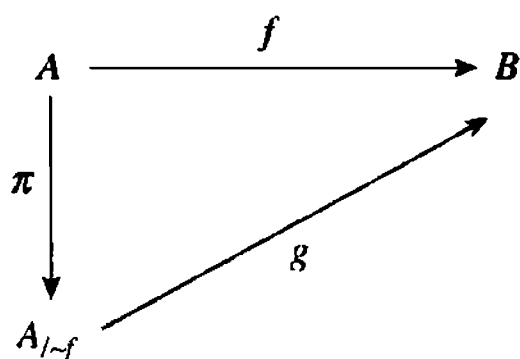
Data una famiglia $F = (F_i \mid i \in I)$, si assume che l'unione di tutti gli elementi della famiglia sia un insieme, indicato con $\bigcup_{i \in I} F_i$. L'intersezione delle immagini di F si indica con $\bigcap_{i \in I} F_i$.

Date due classi A, B e una funzione

$$f: A \rightarrow B,$$

si definisce naturalmente in A la seguente relazione $\sim_f$ ponendo $x \sim_f y \Leftrightarrow f(x) = f(y)$. Si dimostra facilmente che:

1. $\sim_f$ è una relazione di equivalenza su A .
2. $A_{/\sim_f}$ è biunivoco con B tramite la funzione g che associa $f(x)$ a ciascun $[x]_{/\sim_f} \in A_{/\sim_f}$.
3. Il seguente diagramma insiemistico commuta, ovvero $f(x) = g(\pi(x))$, ove π è la funzione che associa a ciascun elemento la sua classe di equivalenza rispetto a $\sim_f$.



Una famiglia F di insiemi non vuoti tali che $\bigcup_{i \in I} A_i = A$ e $A_i \cap A_j = \emptyset$ per ogni $i, j \in I$ si dice *partizione* di A . Si dimostra facilmente che una partizione di un insieme A determina una relazione di equivalenza su A e che, viceversa, una relazione di equivalenza su A determina una partizione di A .

1.6. Sequenze

Dato un numero naturale k una *sequenza* α di *lunghezza* k , detta anche *k -upla*, è una funzione α il cui dominio è l'insieme dei naturali tra 1 e k (compresi). La lunghezza della sequenza α si indica con $|\alpha|$. La posizione 1 di una sequenza costituisce la sua *testa*, mentre la posizione finale rappresenta la sua *coda*. Data una sequenza α e un numero $1 \leq i \leq |\alpha|$, $\alpha(i)$, o anche α_i è l'elemento di α in *posizione* i . Le sequenze si indicano solita-

mente elencando da sinistra a destra gli oggetti che le costituiscono, intercalati da un simbolo di separazione (e.g. virgola, spazio, virgola e spazio, punto, punto e virgola, due punti) e tra due coppie di parentesi (tonde, quadre, angolate). Per esempio: (a, b, b, d, a, b, c) . Talvolta, quando non vi è pericolo di ambiguità, le parentesi vengono omesse.

Notiamo che fino ad ora abbiamo considerato due usi differenti delle parentesi:

1. *applicativo*, per indicare l'applicazione di un'operazione a un argomento; in questo caso l'ordine di applicazione delle operazioni in un'espressione è quello secondo cui si applicano prima le operazioni con parentesi applicative più interne;
2. *sequenziale*, per racchiudere gli elementi costitutivi di una sequenza.

Questi due aspetti sono completamente diversi ed è opportuno che, a livello concettuale, siano considerati ben distinti. Nei contesti in cui è richiesto un maggiore rigore notazionale è consigliabile utilizzare simboli tipografici diversi.

In una sequenza è importante indicare non solo gli elementi, ma anche il loro ordine e il numero di volte con cui compaiono. In ciò una sequenza è completamente diversa da una classe finita. Per esempio:

$$\{a, b, c\} = \{b, a, c\} = \{a, b, c, a\},$$

ovvero $\{a, b, c, a\}$ è una notazione ridondante della classe costituita dagli elementi a, b, c . Invece:

$$(a, b, c) \neq (b, a, c) \neq (a, b, c, a).$$

Un caso speciale di sequenza è quella priva di elementi che si dice *sequenza vuota* e si indica con $()$ o λ . Si pone: $|()| = 0$. Una sequenza costituita da un solo elemento dicesi una *monosequenza*. Notiamo che, a meno di dichiarazione esplicita, dato un elemento a , vale che $a \neq (a)$.

La sottosequenza di α costituita dagli elementi tra due posizioni $1 \leq i \leq j \leq |\alpha|$ si indica con $\alpha[i, j]$. Si intende che $\alpha[i, i] = (\alpha(i))$.

Due sequenze α, β si considerano uguali se hanno la stessa lunghezza e inoltre se hanno gli stessi elementi nelle stesse posizioni. Data una classe A , una sequenza su A è una funzione totale il cui dominio è un segmento $\{1, \dots, n\}$ di naturali e il cui codominio è A . Indichiamo con A^k la classe delle k -uple su A , e con $A_1 \times \dots \times A_k$ la classe delle k -uple α tali che $\alpha(i) \in A_i$ per $i = 1, \dots, k$.

L'operazione di *concatenazione*, date due sequenze α, β , produce una nuova sequenza $\alpha * \beta$ tale che

$$\alpha * \beta = (\alpha(1), \alpha(2), \dots, \alpha(|\alpha|), \beta(1), \beta(2), \dots, \beta(|\beta|))$$

ovvero $|\alpha * \beta| = |\alpha| + |\beta|$ e inoltre

$$(\alpha * \beta)(i) = \alpha(i)$$

per $i \in \{1, \dots, |\alpha|\}$, e

$$(\alpha * \beta)(i) = \beta(i - |\alpha|)$$

per $i \in \{|\alpha| + 1, \dots, |\alpha| + |\beta|\}$.

Si verifica facilmente che la concatenazione è *associativa*; inoltre vale che: $a * () = () * a = a$.

L'insieme A^* delle *stringhe* o *parole* su A è costituito dalle sequenze su A per cui $(a) = a$ per ogni $a \in A$; ovvero una stringa su A è una sequenza su A i cui elementi coincidono con le corrispondenti monosequenze di A . Usualmente le stringhe si indicano giustapponendone gli elementi, senza virgole e parentesi. Per esempio se $A = \{a, b\}$ le seguenti sono stringhe su A^* : aab , bba , a , bb . Un *linguaggio* su A è un qualsiasi sottoinsieme di A^* . In tale contesto A dicesi anche *alfabeto*.

Esercizio 1.3 *Determinare una funzione biunivoca tra un linguaggio su un qualsiasi alfabeto A e uno sull'alfabeto $0, 1$.*

Esercizio 1.4 *Sia α una sequenza su un alfabeto A , di lunghezza n . Si definisca la funzione da $\{1, \dots, n\}$ in A che rappresenta la sequenza reverse (α), inversa della sequenza α (esempio: $\text{reverse}(abccbc) = cbccba$).*

Esercizio 1.5 *Rappresentare la sequenza $(0, 1)$ come insieme costruito a partire da $\{0, 1\}$ (una sequenza è una funzione, una funzione un insieme di coppie e una coppia un insieme di Kuratowski).*

1.7. Variabili e λ -notazione

Le espressioni matematiche contengono usualmente simboli di *variabili*. Per rendersi conto di come le variabili siano essenziali nel linguaggio matematico presentiamo un esempio tratto dal manuale di logica elementare di A. Tarski.¹ Consideriamo l'identità algebrica

$$x^3 - y^3 = (x - y)(x^2 + xy + y^2)$$

ed esprimiamola nel linguaggio ordinario senza l'uso di variabili: *la differenza dei cubi di due numeri è uguale al prodotto di due fattori il primo dei quali è dato dalla differenza dei due numeri, e il secondo dalla somma dei quadrati dei due numeri più il prodotto degli stessi*.

Il vantaggio di una notazione simbolica basata sulle variabili è evidente.

¹ A. Tarski, *Introduction to Logic*, Oxford University Press, Oxford 1965 [trad. it. *Introduzione alla logica*, Bompiani, Milano 1978²].

Una variabile metalinguistica, o semplicemente una *metavariabile*, è un simbolo che denota un elemento generico di un insieme. Quando diciamo: “Sia A un insieme e f una funzione ...” i simboli A e f sono delle *variabili metalinguistiche*. Una variabile *sintattica* è più propriamente una variabile che assume valori su una classe prefissata di espressioni linguistiche. Le variabili si dicono *formali*, quando la loro variabilità è stabilita matematicamente tramite una classe di funzioni, dette assegnamenti, da un insieme V di variabili in un insieme A di valori. Se quindi ρ è un assegnamento, allora associa a ogni $x \in V$ il valore $\rho(x)$.

Se E è un'espressione in cui occorre la variabile x e se $E(a)$ è il valore assunto da $E(x)$ quando x assume il valore a , allora l'espressione

$$\lambda x.E(x)$$

indica la funzione che associa al valore a della variabile il valore $E(a)$ che l'espressione assume in corrispondenza.

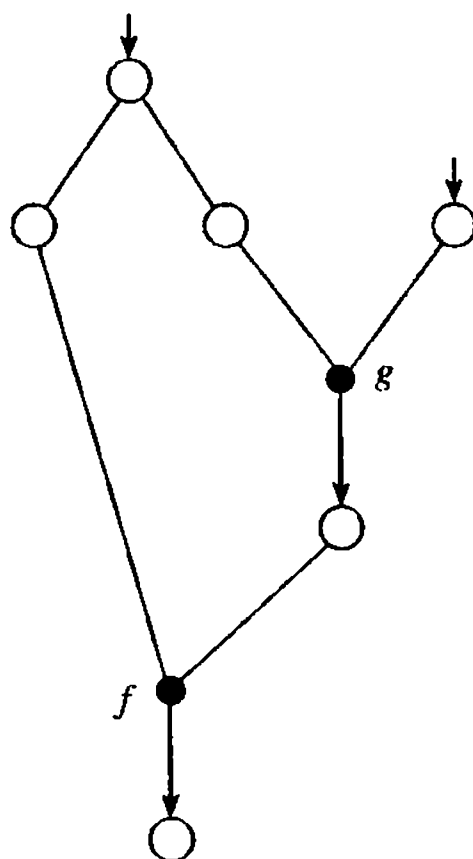
La λ -notazione è essenziale nella rappresentazione di funzioni complesse. Supponiamo che le variabili x e y varino rispettivamente nelle classi A e B e che, in corrispondenza a ciascuna coppia di valori da esse assunte, l'espressione $f(x, g(x, y))$ assuma valore in una classe C . In tal caso si indica con

$$\lambda x, y.f(x, g(x, y))$$

la funzione

$$h: A \times B \rightarrow C$$

tale che, per ogni $a \in A, b \in B, h(a, b) = f(a, g(a, b))$, che possiamo esprimere con il seguente diagramma:



La λ -notazione è un caso di *variabile apparente* o vincolata, nel senso che, nonostante un'espressione del tipo $\lambda x.x^3 + 1$ contenga la variabile x , essa non designa qualcosa di variabile, ma un'entità ben specificata (in questo caso, una funzione rappresentabile con una ben precisa curva). Si dice anche che nella λ -espressione $\lambda x.E(x)$ si astrae in $E(x)$ rispetto alla variabile x . Con ciò si intende dire che il significato della funzione $\lambda x.E(x)$ è indipendente dalla variabile x . Per esempio, $\lambda y.y^3 + 1$ individua la stessa funzione (e quindi la stessa curva) di $\lambda x.x^3 + 1$; infatti, la relazione funzionale che essa esprime (sommare 1 al cubo) prescinde dalla variabile usata. Il senso del simbolo speciale λ , in tale contesto, è appunto quello di indicare questo procedimento di astrazione.

La λ -notazione è utilizzata a vari livelli, come notazione informale e in vari contesti rigorosamente formalizzati. Il livello di formalizzazione di una λ -notazione dipende strettamente da quale nozione di variabile viene assunta.

1.8. Strutture matematiche

Le strutture matematiche sono ottenute combinando opportunamente le nozioni matematiche di base fino ad ora considerate.

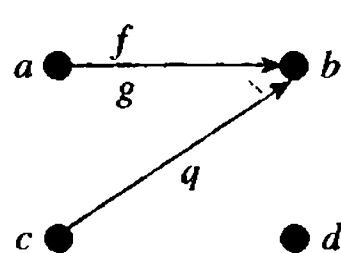
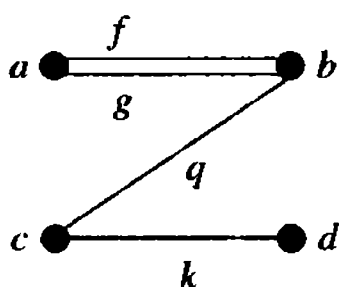
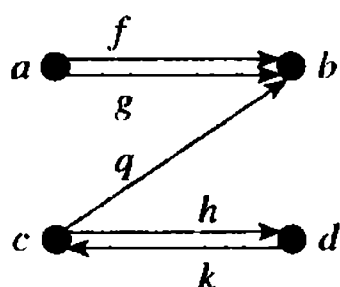
Un'algebra omogenea $A = (D, f_1, f_2, \dots, f_k)$ è determinata da un insieme D detto *dominio* dell'algebra e dalle operazioni $f_1, f_2, \dots, f_k$, ciascuna delle quali determina una funzione definita sull'insieme di n -uple di D (se n è l'arietà della operazione) a valori in D . L'algebra è totale se ogni sua operazione determina una funzione totale, altrimenti è parziale. Un'algebra eterogenea B ha invece più domini, ovvero è una struttura del tipo $B = (D_1, D_2, \dots, D_m, f_1, f_2, \dots, f_k)$. In tal caso l'operazione f_i , con $i = 1, \dots, k$, è una funzione che ha come dominio un prodotto cartesiano i cui fattori sono domini dell'algebra, e come codominio uno di tali domini (anche in tal caso si parla di algebre totali o parziali se tali sono le funzioni). I sistemi numerici tradizionali sono algebre: per esempio, $(\mathbb{N}, +, *)$ è l'algebra dei naturali con somma e prodotto. Spesso in un'algebra si considerano operazioni nullarie, cioè con zero argomenti, dette anche costanti dell'algebra. Tali operazioni identificano degli elementi del dominio; per esempio, un'estensione dell'algebra sopra considerata si ottiene aggiungendo due operazioni nullarie: $(\mathbb{N}, +, *, 0, 1)$. Algebre eterogenee (totali) sono le *strutture relazionali*, ovvero algebre del tipo $(D, \{0, 1\}, f_1, f_2, \dots, f_k, P_1, P_2, \dots, P_m)$, ove $P_1, P_2, \dots, P_m$ sono relazioni su D (operazioni da n -uple di D in $\{0, 1\}$). Una struttura relazionale basilare è quella costituita dai naturali con somma, prodotto e la relazione di minore o uguale tra numeri: $(\mathbb{N}, +, *, \leq)$.

Un grafo orientato G è una struttura relazionale del tipo (V, A, R) , ove l'insieme V è costituito da elementi detti *nodi* o *vertici* e A è un insieme i cui

elementi sono detti *archi* o *spigoli*. La relazione R è definita sulle terne del tipo (n, a, n') di $V \times A \times V$ e quando vale si dice che a è un arco che *connette* i vertici n, n' . Il *grado* di un nodo è il numero di archi che connette il nodo ad altri nodi. Un *cammino* è una successione di nodi in cui ciascun nodo (tranne l'ultimo) è connesso al nodo che lo segue. La *lunghezza* del cammino è il numero dei suoi archi. Un *ciclo* è un cammino in cui inoltre l'ultimo nodo è connesso al primo. Un grafo è *connesso* se tra due suoi nodi qualsiasi vi è sempre un cammino che li connette (o in un verso o in quello opposto). Un grafo è *finito* se ha un numero finito di archi e di nodi, è *vuoto* se ha un insieme vuoto di nodi (e quindi di archi). I grafi finiti si rappresentano con *diagrammi* in cui i vertici sono punti e gli archi sono linee.

Un grafo *non orientato* si può considerare come un grafo orientato simmetrico, ovvero un grafo in cui per ogni arco a che connette la coppia di nodi n, m vi è un arco a' che connette m, n .

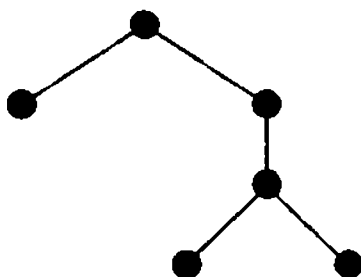
Un grafo *semplice* è un grafo in cui due nodi sono connessi al più da un arco. Un grafo non semplice si dice anche *multigrafo*. I seguenti diagrammi sono relativi a un (multi)grafo, un grafo non orientato e a un grafo semplice:



Un *albero* è un grafo semplice non orientato, connesso e senza cicli. Dato un albero, diciamo *foglia* un nodo che appartiene a un solo arco. Un nodo è *interno* se non è una foglia. Un albero è *atomico* se è costituito da un solo nodo e da nessun arco.

La nomenclatura sugli alberi è un miscuglio di termini genealogici, botanici e matematici.

Un *albero radicato* è un albero in cui è scelto un nodo r detto *radice*. In tal modo si determina un naturale ordinamento, detto genealogico, in cui la radice è il massimo e, dato un cammino dalla radice a un nodo a , ogni nodo che in tale cammino precede a è considerato maggiore di a . Il diagramma che rappresenta un albero radicato ha usualmente uno sviluppo verticale, convenendo che se due nodi sono collegati, quello più in alto è il maggiore e quello più in basso il minore. Il seguente diagramma rappresenta un albero radicato:



Considerando l'ordinamento genealogico, si definiscono in modo del tutto naturale le nozioni di: *padre* di un nodo, come (unico) maggiorante immediato; *figlio* come minorante immediato; *antenato* come maggiorante; *discendente* come minorante; *livello* o *profondità* di un nodo come lunghezza della catena dei suoi predecessori; *altezza* o *profondità* di un albero come il massimo livello raggiunto dai suoi nodi (se l'albero è finito); *foglia* come elemento minimale. Un albero è *k*-ario se ogni nodo interno ha al più *k* figli; un albero *k*-ario è *completo* se ogni nodo interno ha esattamente *k* figli e tutte le foglie hanno la stessa profondità. Un albero è *finitario* se ogni nodo interno ha un numero finito di figli. Di solito quando si parla di albero si assume implicitamente che sia un albero radicato, mentre si parla di albero libero quando si vuole rimarcare che si tratta di un albero non radicato.

Un grafo orientato può essere equivalentemente definito come un'algebra eterogenea totale $(V, A, \text{dom}, \text{cod})$ ove dom e cod sono funzioni da A in V che associano a ciascun arco un nodo di origine (dominio) e un nodo di destinazione (codominio). Estendendo una tale nozione di grafo si perviene alla seguente nozione di categoria.

Una *categoria* è un particolare grafo orientato, riflessivo e *transitivo* nel senso che: I) per ogni nodo vi è un arco *identico* con origine e destinazione il dato nodo; II) per ogni due archi componibili (per cui la destinazione del primo coincide con l'origine del secondo) vi è un arco diretto (dall'origine del primo alla destinazione del secondo) detto *composizione* dei due archi; III) la composizione è *associativa*; IV) la composizione di un arco identico con un altro arco f , o viceversa, è uguale a f . Nel contesto delle categorie gli elementi di V si dicono *oggetti* e quelli di A si dicono *frecce* o *morfismi*.

La nozione di categoria è di una generalità sorprendente: infatti tutte le strutture matematiche conosciute si possono esprimere in termini di categorie e i rapporti tra tipi diversi di strutture si esprimono naturalmente con concetti categoriali. Per tale motivo la teoria delle categorie è diventata una sorta di linguaggio matematico generale per esprimere e indagare le strutture matematiche in quanto tali.

Alla base della nozione considerata di struttura vi è sempre il concetto di algebra, ma in contesti specifici collegati alla natura spazio-temporale di certe intuizioni servono nozioni in cui il semplice schema algebrico insieme/operazioni non basta. È questo il caso della nozione di *topologia*, definita da un insieme in cui ad ogni punto è associata una famiglia di insiemi detti *intorni*. Le famiglie di intorni devono soddisfare delle condizioni che esprimano matematicamente il fatto che un intorno è una sorta di "ambito di vicinanza", e che un punto determina un processo di localizzazione per avvicinamenti successivi. A tal fine si definisce una relazione di *appartenenza interna* più forte della semplice appartenenza: un elemento è interno a un insieme se tale insieme include un intorno del punto. Gli assiomi di una to-

pologia richiedono che: i) ogni intorno di un punto a contenga il punto a ; ii) un insieme che include un intorno di un punto a sia ancora un intorno di a ; iii) l'intersezione di due intorni di un punto a sia ancora un intorno di a ; iv) ogni intorno U di un punto a includa un secondo intorno V del punto a i cui punti siano interni a U .

Uno dei successi più entusiasmanti della nozione di insieme è stata la riduzione dei concetti algebrici e geometrici a una comune base matematica. Infatti usando gli insiemi si può generalizzare la struttura insita nei sistemi numerici tradizionali, pervenendo alla nozione astratta di algebra, ma allo stesso tempo, possono essere definiti insiemisticamente e studiati in modo del tutto astratto i concetti propri della matematica del continuo. È quanto dimostra la topologia generale che, partendo dalla definizione di struttura topologica, ha permesso di astrarre i metodi della cosiddetta “analysis situs”, sviluppando concetti che sono alla base delle teorie geometriche e analitiche elaborate nel XX secolo.

1.9. Induzione strutturale

Il principio di induzione numerica è di importanza fondamentale. La sua comparsa ufficiale in matematica si può far risalire ai seguenti assiomi, formulati nel 1889 dal matematico e logico Giuseppe Peano, per caratterizzare l'insieme $\mathbb{N}$ dei numeri naturali.

1. 0 è un numero naturale.
2. Ogni numero naturale ha un solo successore.
3. 0 non è successore di alcun numero.
4. Numeri distinti hanno successori distinti.
5. Un sottoinsieme di naturali che contiene 0 e il successore di ogni suo numero coincide con l'insieme dei naturali.

La quinta proposizione, nota come *principio di induzione*, giustifica il seguente metodo di dimostrazione.

Per dimostrare che una proprietà P vale per tutti i numeri naturali n si procede nel modo seguente:

- *passo iniziale*: si prova $P(0)$;
- *passo induttivo*: si assume la validità di $P(n)$ e si prova $P(n + 1)$.

Esempio 1.1 Un insieme di n elementi ha 2^n sottoinsiemi.

Passo iniziale

La proprietà vale ovviamente per $n = 0$ perché esiste un solo insieme (l'insieme vuoto) con 0 elementi.

Passo induttivo

Sia dato un insieme A di $n + 1$ elementi e si consideri un suo sottoinsieme B di n elementi. Ogni sottoinsieme di A si ottiene da qualche sottoinsieme di B in due modi possibili: aggiungendogli l'elemento di A che non è in B , o non aggiungendogli nulla. Siccome, per l'ipotesi di induzione, un insieme di n elementi ha 2^n sottoinsiemi, si avranno in totale $2 \cdot 2^n = 2^{n+1}$ sottoinsiemi di A .

Il principio di induzione si applica ai numeri naturali; è comunque semplice estenderlo a successioni numeriche qualsivoglia. Più propriamente si parla di induzione completa quando nel passo induttivo la proprietà da dimostrare è assunta valida non solo per un dato numero, ma anche per tutti i numeri che lo precedono.

Il principio di induzione può essere utilizzato anche come principio di *definizione*. Infatti, una definizione è ben data se è una condizione che individua uno e un solo oggetto (esistenza e unicità). Una definizione induttiva di un oggetto che dipende da un numero naturale si costruisce nel modo seguente:

- ... si pone la definizione per $n = 0$;
- ... assumendo la definizione per un certo n , la si pone per $n + 1$.

Il teorema che segue individua una caratteristica fondamentale degli alberi radicati finitari (in cui ogni nodo ha solo un numero finito di figli); la dimostrazione è basata su una definizione per induzione. Come vedremo, tale teorema sarà utilizzato nella dimostrazione di risultati fondamentali di logica matematica.

Proposizione 1.2 (lemma di König) *Un albero radicato finitario con un insieme numerabile di nodi ha sempre un ramo infinito.*

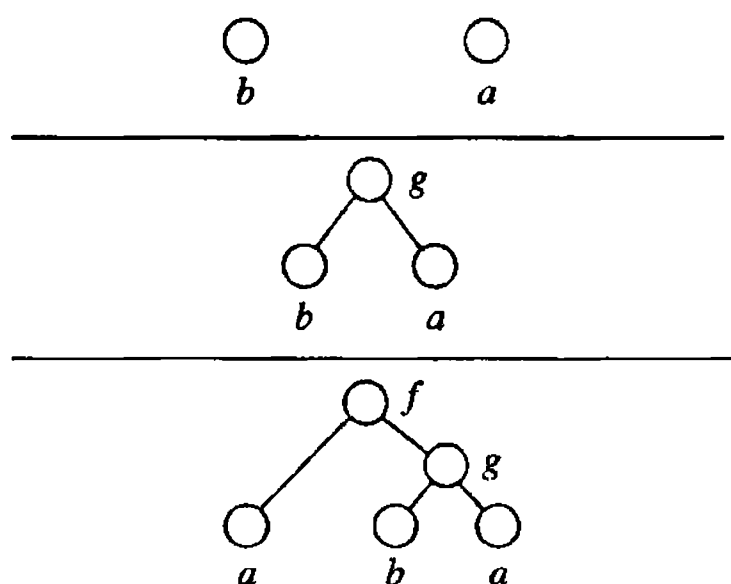
Dimostrazione Si consideri la radice r dell'albero. Questa deve avere almeno un figlio r' che a sua volta è radice di un sottoalbero infinito. Infatti se un tale figlio non dovesse esistere, visto che i figli di r sono in numero finito, anche l'albero di partenza sarebbe finito. Si scelga r' come nodo successore di r nel ramo cercato e si riapplichì il ragionamento appena fatto al sottoalbero di radice r' , ottenendo un figlio r'' di r' . Tale procedimento non può terminare, quindi il ramo che si genera in tal modo è infinito. ■

Il principio di induzione si generalizza ulteriormente per dimostrare o definire proprietà o caratteristiche relative a classi di strutture finite: sequenze, insiemi, alberi, o grafi. Tale uso dell'induzione è solitamente indicato come principio di *induzione strutturale*. In un certo senso l'induzione strutturale è una sorta di induzione numerica indiretta. Infatti si considera

una grandezza numerica tipica delle strutture considerate (una lunghezza, una dimensione, un parametro di complessità, o qualcosa di analogo); si comincia a dimostrare o definire qualcosa per strutture in cui tale grandezza è minima; quindi si considera una generica struttura e si dimostra o si definisce per essa, assumendo di avere già definito o dimostrato per le strutture in cui il valore di tale grandezza è inferiore.

Diamo alcuni esempi di uso dell'induzione strutturale.

Esempio 1.2 Gli alberi etichettati (radicati finiti) sono definiti per induzione nel modo seguente. Si consideri un insieme di simboli Σ in cui ad ogni elemento σ è associato un numero naturale detto *arietà* del simbolo. L'insieme T_Σ di alberi etichettati in Σ è definito per induzione sulla profondità. Gli alberi di profondità nulla sono etichettati con simboli di arietà nulla. Dato un simbolo σ di arietà k e k alberi etichettati $t_1, t_2, \dots, t_k$ di profondità al più n , $\sigma(t_1, t_2, \dots, t_k)$ rappresenta l'albero di profondità $n + 1$ che ha σ come etichetta della radice e i cui figli sono le radici degli alberi etichettati $t_1, t_2, \dots, t_k$. Se consideriamo un insieme di simboli $\{a, b, f, g\}$ in cui a, b hanno arietà nulla e f, g arietà 2, otteniamo la seguente successione di costruzione di un albero di profondità 2:



L'esempio precedente rivela una completa identità strutturale tra il concetto di albero etichettato (radicato finito) e di espressione algebrica con simboli di operazioni Σ (e simboli di variabili). Come vedremo, i termini e le formule della logica dei predicati sono particolari alberi e questo è il motivo fondamentale dell'uso massiccio che faremo di principi induttivi nelle definizioni e dimostrazioni nell'ambito di tale teoria.

Esempio 1.3 Si consideri il linguaggio L delle parole non nulle "equilibrate" su $\{0, 1\}$, ovvero in ciascuna delle quali occorrono lo stesso numero di 0 e di 1. Definiamo per induzione il seguente linguaggio L' :

$$1 \quad 0, 1 \in L'.$$

$$2 \quad \alpha \in L' \Rightarrow 0\alpha, 1\alpha \in L'.$$

$$3 \quad \alpha, \beta \in L' \Rightarrow \alpha\beta \in L'.$$

È evidente che $L' \subseteq L$. Dimostriamo per induzione strutturale che $L \subseteq L'$. Le stringhe $0, 1 \in L$. Si consideri una generica stringa α di L e verifichiamo che essa appartiene anche a L' , assumendo che ciò sia vero per le stringhe più corte. Si hanno due casi alternativi: la prima e l'ultima cifra di α sono diverse, oppure no. Nel primo caso $\alpha = x\beta y$ ove $x \neq y \in \{0, 1\}$, ma β è più corta di α , quindi per l'ipotesi induttiva $\beta \in L'$, e quindi, applicando la seconda regola di generazione di L' , anche $\beta \in L'$. Se $x = y$, si proceda da y verso sinistra. Sicuramente vi è un punto di α in cui si determina una sottosequenza equilibrata, e tale punto non può essere costituito proprio dal simbolo x iniziale, perché altrimenti si dovrebbe avere $x \neq y$, ovvero il contrario di quanto supposto. Sia γ la sottostringa equilibrata così determinata; allora $\alpha = \delta\gamma$ per qualche δ non vuota. Ovviamente δ, γ sono più corte di α , e quindi per l'ipotesi induttiva esse sono in L' , e perciò applicando la terza condizione di generazione di L' , anche α sta in L' . Questo conclude la prova induttiva.

Esercizio 1.6 *Sia R una relazione binaria; si definisca per induzione la sua chiusura transitiva R^* .*

Suggerimento xR^*y sse esiste una sequenza finita di elementi che inizia per x e termina per y e in cui tra due elementi che si susseguono direttamente vale la relazione R . Si proceda per induzione sulla lunghezza di tale sequenza.

Esercizio 1.7 *Si definisca per induzione sulle parole di un alfabeto finito l'operazione $\text{select}(\alpha, i)$ che dato un indice non nullo i inferiore alla lunghezza di α , produce il simbolo di α che trovasi in tale posizione.*

Esercizio 1.8 *Si definisca per induzione la classe dei multinsiemi finiti costruibili a partire da un insieme A .*

Esercizio 1.9 *Si definiscano per induzione i grafi (semplici non orientati) e gli alberi finiti i cui nodi sono numeri naturali.*

Esercizio 1.10 *Un albero binario si dice quasi-completo quando i suoi nodi hanno esattamente due figli, tranne che al suo penultimo livello in cui ne possono avere uno o due. Si dimostri per induzione che un albero quasi-completo di n nodi ha profondità $\lfloor \log_2 n \rfloor$ (il naturale che precede immediatamente $\log_2 n$).*

Esercizio 1.11 *Si dimostri per induzione che in un albero finito non vuoto il numero di nodi supera di uno il numero degli archi.*

1.10. Numeri ordinali e cardinali

Un'ulteriore generalizzazione del principio di induzione numerica è il principio di *induzione noetheriana*.

Un insieme A si dice *ben fondato* rispetto all'ordinamento $\leq$ (o a un ordinamento stretto) quando ogni sottoinsieme non vuoto di A include un elemento minimale.

Per esempio, consideriamo in un albero l'ordinamento, inverso a quello solito, per cui la radice è il minimo e le foglie sono i massimali. Un tale ordinamento è ben fondato. Anzi potremmo definire un albero, su un insieme A di nodi, come un ordinamento ben fondato con la ulteriore proprietà che i minoranti di ogni elemento costituiscono una catena.

Una proprietà si dice *ereditaria* su un insieme A (rispetto a un ordinamento), se essa vale sugli elementi minimali di A , e inoltre vale su un elemento allorquando vale su tutti gli elementi che lo precedono.

Proposizione 1.3 (induzione noetheriana) *In un insieme ben fondato (rispetto a un ordinamento) una proprietà ereditaria su tale insieme vale su tutti gli elementi dell'insieme.*

Dimostrazione Dimostriamolo per assurdo. Sia P una proprietà ereditaria su un insieme A (rispetto a un ordinamento $\leq$). Se P non vale su tutto A , allora il sottoinsieme B di A per cui P non vale è non vuoto, quindi, poiché A è ben fondato, B ha un elemento minimale, diciamolo m . Inoltre, poiché P è ereditaria, m non può essere minimale in A , ovvero in A vi sono elementi inferiori a m . Per come è definito m , la proprietà P deve valere per tutti gli elementi inferiori di m . Ma P è ereditaria e ciò implica che deve valere anche su m , contro le ipotesi. In definitiva, assumendo che B sia non vuoto si perviene a un assurdo, dunque B è vuoto, ovvero P vale su tutto A . ■

Un insieme linearmente ordinato e ben fondato si dice anche *bene ordinato*. L'induzione noetheriana su insiemi bene ordinati si dice più propriamente *induzione transfinita*.

Un insieme bene ordinato può essere concepito come un insieme i cui elementi possono essere messi "in fila" a partire dal più piccolo. Infatti la definizione data di buon ordinamento equivale a richiedere che nell'insieme non vi siano catene infinite decrescenti.

Consideriamo ora una classe i cui elementi individuano essenzialmente tutti i possibili insiemi bene ordinati.

La classe Ω dei *numeri ordinali* è definita come la classe degli insiemi α tali che

$$\alpha = \{\beta \mid \beta \subset \alpha\}$$

che siano anche bene ordinati rispetto alla relazione di inclusione. Quindi $\emptyset$, $\{\emptyset\}$ $\{\emptyset, \{\emptyset\}\}$, ... sono ordinali. Seguendo un'idea di von Neumann, identifichiamo 0 con $\emptyset$ e $n + 1$ con $\{0, 1, \dots, n\}$. In tal modo l'insieme $\mathbb{N}$ dei numeri naturali, si può identificare con il minimo ordinale ω che contiene $\emptyset$ e $n \cup \{n\}$ per ogni suo elemento n . Ma l'operazione di successore può essere definita per un qualsiasi ordinale α , in termini completamente insiemistici ponendo $\alpha + 1 = \alpha \cup \{\alpha\}$, quindi la sequenza degli ordinali si estende al transfinito:

$$\begin{aligned} &0, 1, 2, \dots \omega, \omega + 1, \omega + 2 \dots \omega + \omega = \\ &= 2\omega, 2\omega + 1 \dots 3\omega \dots \dots \omega^2 \dots \dots \omega^3 \dots \dots \omega^\omega \end{aligned}$$

(le operazioni di somma, prodotto ed esponente sugli ordinali si possono definire rigorosamente, in termini del tutto generali).

La nozione di ordinale mette in luce il legame profondo tra il concetto di insieme e quello di infinito. Un insieme in quanto tale permette di esprimere la nozione di totalità come unico oggetto. Nel caso di un insieme infinito quale $\mathbb{N}$, identificare l'insieme con un oggetto equivale ad esprimere compiutamente il processo infinito di generazione dei numeri, ovvero consente di concepire quello che i filosofi chiamano infinito in atto, come contrapposto all'infinito in potenza.

La classe Ω degli ordinali è una classe propria (non un insieme). Infatti, se Ω fosse un insieme, $\bigcup \Omega$ sarebbe il massimo tra gli ordinali. Ma ciò porterebbe immediatamente a una contraddizione:

Paradosso di Burali-Forti o del massimo ordinale *Se esistesse un ordinale massimo Ξ , allora $\Xi + 1$ sarebbe ancora un ordinale, che evidentemente sarebbe maggiore di Ξ ; quindi Ξ non sarebbe il massimo.*

La seguente proposizione mostra che gli ordinali si dispongono secondo un ordine lineare.

Proposizione 1.4 *L'inclusione (e quindi l'appartenenza) tra ordinali è un ordinamento totale.*

Dimostrazione Bisogna dimostrare che due ordinali α, β sono sempre confrontabili, cioè o sono uguali o uno è minore dell'altro. Consideriamo la loro intersezione $\gamma = \alpha \cap \beta$ essa è chiaramente un ordinale. Sicuramente γ è incluso in α e in β . Se $\gamma = \alpha$ o $\gamma = \beta$, allora la prova è conclusa. Se γ fosse strettamente incluso sia in α che in β , essendo tali insiemi degli ordinali, allora γ apparterrebbe ad entrambi, ovvero $\{\gamma\}$ sarebbe incluso in entrambi e quindi anche $\gamma \cup \{\gamma\}$ sarebbe incluso in entrambi. Ma ciò è assurdo poiché abbiamo supposto che $\alpha \cap \beta = \gamma$. ■

Ogni ordinale è bene ordinato rispetto alla relazione di appartenenza o di inclusione (indicata in tale contesto anche con $\leq$), e anche la classe Ω è bene ordinata rispetto all'appartenenza (o all'inclusione). Infatti, data una classe non vuota di ordinali, l'intersezione di tutti i suoi elementi è il minimo ordinale di tale classe.

Un ordinale che non è successore di nessun altro ordinale è un *ordinale limite*. Il primo ordinale limite, usualmente indicato con ω , è costituito dall'insieme degli ordinali finiti e quindi coincide essenzialmente con l'insieme dei naturali. Tutti gli ordinali definibili a partire da ω e dagli ordinali finiti tramite somme, prodotti ed esponenti sono numerabili. Il primo degli ordinali non numerabili è l'insieme degli ordinali numerabili, indicato con ω_1 ; dopo di questo parte un'altra serie di ordinali, enormemente più lunga, che porta a ω_2 , per proseguire fino a ω_ω e oltre, con un andamento vertiginoso. La teoria degli insiemi, nei suoi sviluppi più specialistici è rivolta a un'analisi di questi ordini "enormi" di infinito per cercare di sondarne i limiti più arditi.

Nonostante gli ordinali consentano una numerazione al transfinito, conservano un legame intrinseco con il finito: infatti, si verifica facilmente che, in quanto buoni ordini, non possono contenere catene discendenti infinite; quindi, a qualsiasi punto ci si ponga nella successione enumerativa di un ordinale, non si può mai tornare all'indietro con un regresso infinito.

Dimostriamo ora che ogni insieme può essere bene ordinato. Per una tale dimostrazione è necessario un principio insiemistico, noto come *assioma di scelta*, che è *non costruttivo* in quanto postula l'esistenza di un insieme senza specificare le condizioni che devono soddisfare i suoi elementi. Il suo ruolo è decisivo in moltissime dimostrazioni matematiche. La sua introduzione, nella dimostrazione che ogni insieme è bene ordinabile, è dovuta al matematico tedesco Ernst Zermelo (1904). La sua formulazione esplicita (1908) è la seguente.

Assioma di scelta *Per ogni insieme C di insiemi non vuoti esiste una funzione f , detta funzione di scelta, tale che $f(X) \in X$ per ogni $X \in C$.*

Proposizione 1.5 (buon ordinamento) *Ogni insieme può essere bene ordinato.*

Dimostrazione Sia A l'insieme da bene ordinare. Determineremo una corrispondenza biunivoca tra A e un ordinale, da ciò segue la buona ordinabilità di A . Si consideri l'ordinamento seguente su A definito attraverso una funzione di scelta f :

$$f(A) < f(A - \{f(A)\}) < f(A - \{f(A), f(A - \{f(A)\})\}) < \dots$$

Si continui a generare tale catena (bene ordinata) fino a quando non si “svuota” tutto l’insieme A . È da verificare che, indicizzando i passi con ordinali, per un qualche ordinale si riesce veramente a “svuotare” l’insieme A e quindi a bene ordinarlo. Sia γ un ordinale e consideriamo la famiglia $F_\gamma = (F_\beta \mid \beta < \gamma)$:

$$F_0 = A$$

$$F_\beta = A - \{f(F_\delta) \mid \delta < \beta\} \quad \text{per ogni } \beta < \gamma.$$

Diremo *F-famiglia* su A una famiglia F_γ di sottoinsiemi non vuoti di A , definita come sopra per qualche ordinale γ . Indichiamo con Γ la classe di ordinali γ per cui si possono definire *F-famiglie* F_γ su A . Se A è un insieme, allora Γ non può coincidere con la classe Ω di tutti gli ordinali, poiché altrimenti, in base all’assioma di rimpiazzamento ($\Gamma = F^{-1}[A]$), anche Ω sarebbe un insieme, e invece sappiamo che Ω è una classe propria. Sia quindi $\alpha = \bigcup \Gamma$, ovvero α è il massimo ordinale relativo a *F-famiglie* su A . Sicuramente F_α bene ordina tutto A , ovvero $A = \{f(F_\beta) \mid \beta < \alpha\}$. Infatti, supponiamo per assurdo che $\{f(F_\beta) \mid \beta < \alpha\} = B$ e $B \subset A$; allora, applicando la funzione di scelta a $A - B$, otterremmo una $F_{\alpha+1}$ famiglia su A per un ordinale maggiore di α , e ciò contraddice la definizione di α . ■

La dimostrazione precedente mostra che gli ordinali sono i prototipi dei buoni ordinamenti, nel senso che, un insieme A è sempre in corrispondenza biunivoca con qualche ordinale e pertanto può essere posto nella forma indicizzata $A = \{\alpha_\beta \mid \beta \leq \alpha\}$ per un qualche ordinale α . Il principio di induzione transfinita permette di estendere le prove induttive a insiemi bene ordinati, quindi, assumendo l’assioma di scelta, a qualsiasi insieme.

La nozione di ordinale consente in modo semplice la definizione di numero cardinale, permettendo di estendere rigorosamente al transfinito la nozione quantitativa di numero che è logicamente distinta da quella di numero d’ordine di una serie.

Due insiemi si dicono *equipotenti* se tra di essi esiste una corrispondenza biunivoca. Si dice *numero cardinale* o *cardinalità* di un insieme A il minimo ordinale equipotente ad A , che si indica con $|A|$.

Visto che ogni insieme può essere bene ordinato e che la classe degli ordinali è bene ordinata, un tale ordinale esiste sempre. Quindi due insiemi A e B sono equipotenti sse $|A| = |B|$. Il primo cardinale infinito, solitamente indicato con $\aleph_0$ individua la cardinalità dei naturali e degli insiemi numerabili (equipotenti con ω). (Il simbolo $\aleph$ indica “alef”, la prima lettera dell’alfabeto ebraico introdotta da Cantor per indicare i numeri cardinali nel suo fondamentale lavoro sui numeri transfiniti). Un cardinale strettamente maggiore a $\aleph_0$ è quello che fornisce la cardinalità delle parti dei naturali. Infatti, si dimostra il seguente risultato generale.

Proposizione 1.6 (diagonalizzazione di Cantor) *La cardinalità delle parti di un insieme A è sempre superiore alla cardinalità dell'insieme.*

Dimostrazione Supponiamo per assurdo che esista una corrispondenza biunivoca f da A a $\mathcal{P}(A)$. Si consideri il seguente sottoinsieme R di A :

$$R = \{a \in A \mid a \notin f(a)\}$$

Essendo f biunivoca deve esistere un elemento di A , diciamolo r , tale che $R = f(r)$. Ma l'esistenza di un tale r porta a un assurdo. Infatti, deve valere che: $r \in R$ oppure $r \notin R$. Nel primo caso, in base alla definizione di R , $r \notin R$, e nel secondo caso $r \in R$ (argomento del tutto analogo al paradosso di Russell). ■

Proposizione 1.7 (funzione di accoppiamento di Cantor) *L'insieme delle coppie di naturali è numerabile.*

Dimostrazione (cenno) Si utilizzi la seguente funzione di codifica. Si dispongano tutte le coppie dei naturali in una matrice infinita $(a_{ij} \mid i, j \in \omega)$, (fig. 1.1) con valori crescenti di j verso destra e valori crescenti di i verso il basso. Quindi si consideri la prima coppia in alto a sinistra, per la quale la somma degli indici vale 0, e la si associa a 0; si considerino quindi tutte le coppie la cui somma degli indici vale 1 ($a_{0,1}, a_{1,0}$) e si associno rispettivamente a 1, 2; quindi tutte le coppie la cui somma vale 2 ($a_{0,2}, a_{1,1}, a_{2,0}$) e si associno rispettivamente a 3, 4, 5. Proseguendo in tal modo si ottiene la corrispondenza biunivoca desiderata (la forma analitica di tale corrispondenza si ottiene osservando che il numero delle coppie la cui somma degli indici non supera un certo valore è un numero triangolare (del tipo $n(n + 1)/2$)). ■

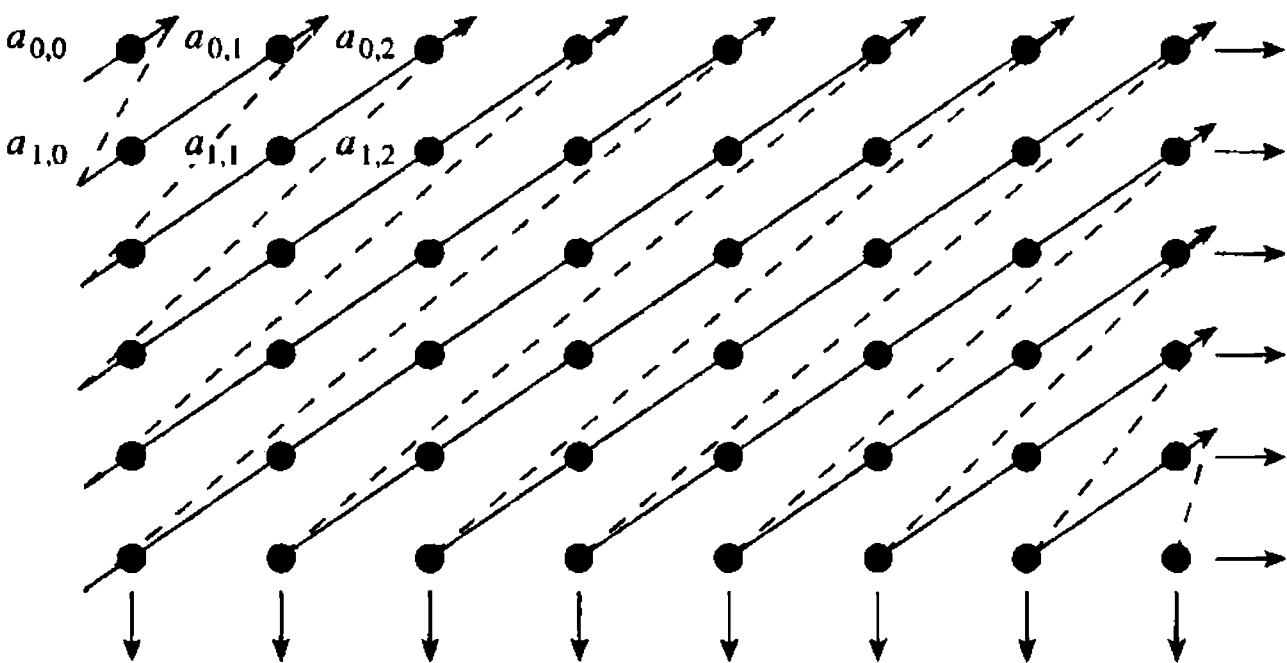


Figura 1.1
Quadro enumerativo di Cantor.

La seguente definizione stabilisce un quasi-ordinamento tra numeri cardinali (relazione binaria riflessiva e transitiva).

Definizione 1.1 *Dati due insiemi A, B , se esiste un sottoinsieme C di B tale che A è equipotente con C , scriviamo $|A| \leq |B|$ e diciamo che A è minore di B in potenza.*

Le seguenti proposizioni indicano che le operazioni di somma e prodotto tra cardinali, definite come cardinalità dell'unione e del prodotto cartesiano, non permettono di costruire cardinali più grandi dei loro argomenti.

Proposizione 1.8 *L'unione di un insieme con un altro insieme di cardinalità non superiore ad esso è equipotente all'insieme dato.*

Dimostrazione (cenno) Lo si dimostri prima nel caso numerabile; quindi lo si estenda utilizzando la buona ordinabilità di ogni insieme. ■

Proposizione 1.9 *Il prodotto cartesiano di un insieme con un altro insieme di cardinalità non superiore ad esso è equipotente all'insieme dato.*

Dimostrazione (cenno) Lo si dimostri prima nel caso numerabile; quindi lo si estenda utilizzando la buona ordinabilità di ogni insieme. ■

Proposizione 1.10 (ordinamento dei cardinali) *La relazione di quasi ordinamento in potenza è un ordinamento. Ovvero dati due insiemi A e B vale che:*

$$|A| \leq |B|, |B| \leq |A| \Rightarrow |A| = |B|.$$

Dimostrazione Si utilizza la proposizione precedente sulla equipotenza tra un insieme e l'unione di esso con un insieme minore in potenza. Infatti, poiché $|A| \leq |B|$, una parte C di B è equipotente con A . Se poniamo $B' = B - C$, allora $B = C \cup B'$ è equipotente con $A \cup B'$. L'insieme B' ha cardinalità non superiore ad A , in quanto per ipotesi dev'essere $|B| \leq |A|$, per cui $A \cup B'$ è equipotente con A e quindi per transitività A e B sono equipotenti. ■

Esercizio 1.12 *Dimostrare che dati due insiemi A, B , se vi è una funzione iniettiva da A in B , allora ve ne è una surgettiva da B in A e viceversa.*

Esercizio 1.13 *Si dimostri che ogni insieme infinito (non biunivoco con un segmento di naturali) include un sottoinsieme numerabile.*

Suggerimento Si usi l'assioma di scelta.

Esercizio 1.14 (paradosso di Galileo) *Si dimostri che l'insieme dei naturali è biunivoco con una sua parte propria.*

Suggerimento Si mandi ciascun numero nel suo doppio.

Esercizio 1.15 *Si dimostri che un insieme è infinito se e solo se è riflessivo, ovvero biunivoco con una sua parte propria.*

Suggerimento Si usino gli esercizi precedenti.

Esercizio 1.16 *Si dimostri che l'unione di una famiglia numerabile di insiemi finiti è numerabile.*

Suggerimento Prima si numerano, in qualsiasi ordine, tutti gli elementi del primo insieme, poi quelli del secondo insieme, poi quelli del terzo, e via di seguito.

Esercizio 1.17 *Si dimostri che l'insieme dei numeri razionali è numerabile.*

Suggerimento Si consideri l'enumerazione delle coppie di naturali.

Esercizio 1.18 *Si dimostri che l'unione di una famiglia numerabile di insiemi numerabili è numerabile.*

Suggerimento Si consideri l'enumerazione delle coppie di naturali.

Esercizio 1.19 *Si dimostri per induzione che l'insieme delle k -ple ($k \in \mathbb{N}$, $k > 2$) di naturali è equipotente con quello dei naturali.*

Esercizio 1.20 *Si dimostri che l'insieme delle stringhe di naturali è equipotente con quello dei naturali.*

Esercizio 1.21 *Si dimostri che l'insieme dei reali è equipotente con quello delle parti dei naturali.*

Suggerimenti

1. $(-\pi/2, \pi/2) \leftrightarrow \mathbb{R}$ (tramite la funzione tangente).
2. $(-\pi/2, \pi/2) \leftrightarrow (0, 1)$ (tramite la retta che congiunge i punti del piano $(-\pi/2, 0)$ e $(-\pi/2, 1)$).
3. $(0, 1) \leftrightarrow [0, 1]$ (ordinamento dei cardinali).
4. $[0, 1] \leftrightarrow (\{0, 1\} \rightarrow \omega)$ (tramite identificazione dei punti x di $[0, 1]$ con le funzioni f_x definite per dicotomie successive: se $x < 1/2$, allora $f_x(1) = 0$, altrimenti $f_x(1) = 1$. Nel primo caso, se $x < 1/4$, allora $f_x(2) = 0$, altrimenti $f_x(2) = 1$. Si prosegua in tal modo, dimezzando ad ogni passo l'intervallo in cui si trova il punto x).
5. $(\{0, 1\} \rightarrow \omega) \leftrightarrow \mathcal{P}(\omega)$ (tramite funzione caratteristica di un sottoinsieme di naturali, che vale 1 sui naturali che stanno nel sottoinsieme e 0 su quelli che non ci stanno).

Esercizio 1.22 *Si determini una numerazione di un insieme numerabile in cui ogni suo elemento è immagine di infiniti numeri naturali.*

Il seguente esercizio illustra l'origine del termine diagonalizzazione usato nel teorema di Cantor sulla non-equipotenza di un insieme con le sue parti.

Esercizio 1.23 *Si ricostruisca il procedimento originale di Cantor per dimostrare che l'insieme dei reali non è equipotente a quello dei naturali.*

Suggerimento Si consideri l'intervallo aperto $(0, 1)$ che è equipotente a tutti i numeri reali (si vede geometricamente). Si individui univocamente un reale non nullo minore di 1 con una successione infinita (utilizzando per i razionali la forma illimitata periodica). A questo punto si costruisca una matrice in cui ad ogni riga si pone un reale. Quindi si consideri un reale la cui rappresentazione ha come cifra di posto i -esimo una cifra diversa da quella presente nella posizione i -esima della riga i -esima. Tale reale non può, per costruzione, essere uguale a nessun reale che compare nella matrice, quindi tale matrice non può enumerare tutti i reali.

Esercizio 1.24 *Si dimostri in modo diretto che i reali sono equipotenti con le coppie di reali.*

Suggerimento Si individui univocamente un reale con una successione infinita (utilizzando per i razionali la forma illimitata periodica). A questo punto da una successione se ne producano due, una prendendo le cifre di posto dispari e una prendendo quelle di posto pari. Tale procedimento non porta ad una biunivocità completa poiché potrebbe capitare che una successione produca un razionale in rappresentazione non illimitata ($0,110203010\dots$ produce $0,1$ e $0,1231\dots$). Allora basta prelevare dalla prima successione gruppi di cifre tali che l'ultima cifra del gruppo sia diversa da 0 ($0,5307009\dots$ produce $0,507\dots$ e $0,3009\dots$).

Quest'ultimo esercizio equivale a stabilire che il quadrato unitario è equipotente con il segmento unitario. Illuminante, a questo proposito, è la ricostruzione storica di Fraenkel:²

Dopo aver dimostrato l'esistenza di due numeri cardinali diversi, nel 1873 Cantor si mise a cercare altri cardinali transfiniti e ritenne ovvio che avrebbe ottenuto il suo scopo passando dal continuo unidimensionale a continui di dimensione superiore. Il primo passo poteva essere quello di passare da un segmento di cardinale $\aleph$ a un quadrato di cardinale $\aleph \times \aleph$. A Cantor occorreva quindi dimostrare che l'insieme dei punti contenuti in un segmento non fosse equivalente a quello dei punti contenuti in un quadrato. Avendo incontrato varie difficoltà nella ricerca di questa dimostrazione, si consultò con diversi matematici a Berlino e Göttingen. Gli fu risposto che non era necessaria alcuna dimostrazione, essendo di per sé evidente che le coppie di coordinate (x, y) non si possono ridurre, cioè associare biunivocamente, a una singola coordinata [...] Già nel 1870 Cantor non faceva affidamento sul buon senso dei suoi famosi colleghi e finalmente, con sua grande sorpresa, trovò che era tutto il contrario di quanto pensava.

² A. A. Fraenkel, *Set Theory and Logic*, Addison-Wesley, Reading, Mass., 1966 [trad. it. *Teoria degli insiemi e logica*, Astrolabio, Roma 1970, pp. 70-71].

1.11. Principi di massimalità

Assumendo il buon ordinamento di ogni insieme si definisce facilmente una funzione di scelta per ogni famiglia di insiemi non vuoti. Infatti, per scegliere un elemento di un insieme della famiglia basta bene ordinarlo e sceglierne il minimo. Un principio, spesso utilizzato, equivalente a quello di scelta è il seguente.

Principio di massimalità di Hausdorff *In un insieme ordinato ogni catena è inclusa in una catena massimale (rispetto all'inclusione).*

Giustificiamo (informalmente) come attraverso una funzione di scelta si possa ottenere l'estendibilità massimale di ogni catena di un insieme ordinato. Data una catena C in un insieme A , si applichi una funzione di scelta f alla famiglia di insiemi $A - C, A - C - \{f(A - C)\}, \dots$. In altre parole, si scelga ad ogni passo un elemento che non è nella catena e lo si tolga dall'insieme, ottenendo un nuovo insieme a cui applicare la scelta del passo successivo. Se ad ogni passo l'elemento scelto è confrontabile con quelli della catena, si estenda la catena posizionandolo nel posto giusto, altrimenti lo si scarti, quindi si prosegua in modo analogo al passo successivo.

Strettamente collegato al principio di massimalità di Hausdorff è il seguente risultato, noto come *lemma di Zorn* e anch'esso equivalente all'assioma di scelta:

Lemma di Zorn *In un insieme ordinato in cui ogni catena ha estremo superiore nell'insieme, ogni elemento b ha un elemento massimale m tale che $m \geq b$.*

Il lemma di Zorn segue facilmente dal principio di massimalità di Hausdorff. Si consideri una catena comprendente b e la si estenda in modo massimale: tale catena massimale avrà un massimo e tale massimo è il massimale maggiore o uguale a b asserto dal lemma.

Utilizzando il lemma di Zorn si ottiene la buona ordinabilità di qualsiasi insieme (e quindi la definibilità delle funzioni di scelta). Infatti, basta ordinare tutti i buoni ordinamenti sull'insieme da bene ordinare (un buon ordine è maggiore di un altro se è definito in più coppie rispetto al primo e coincide con il primo laddove questo è definito). Si verifica che l'insieme di tali buoni ordinamenti verifica le ipotesi del lemma di Zorn. Quindi si consideri un massimale di tali buoni ordinamenti, come postulato dal lemma di Zorn; esso è un buon ordine dell'insieme dato.

Un insieme A che verifica le condizioni del lemma di Zorn (ogni catena di A ha estremo superiore in A) dicesi *induttivo*. Una funzione f su un insieme A tale che $f(x) \geq x$ per ogni $x \in A$ dicesi *accrescitiva*. Dal principio di massimalità di Hausdorff segue facilmente la seguente proposizione dovuta a Nicolas Bourbaki (la dimostrazione originale, notevolmente più complessa non utilizza alcun principio equivalente al principio di scelta).

Proposizione 1.11 *Sia A un insieme ordinato induttivo; allora ogni funzione f accrescitiva su A ha un punto fisso, ovvero un $a \in A$ per cui $f(a) = a$.*

Dimostrazione Consideriamo la catena $\{b, f(b), f(f(b)), \dots\}$, e sia m il suo estremo superiore in A . In base al principio di massimalità vi è una catena che la include e che contiene m . Allora $f(m) = m$ poiché $f(m) \geq m$ (f è accrescitiva) e nello stesso tempo $m \geq f(m)$ poiché m è il massimo della catena massimale. ■

Proposizione 1.12 *L'ordinamento in potenza tra cardinali coincide con quello precedentemente definito sugli ordinali.*

Dimostrazione Ricordiamo che la cardinalità di un insieme è il minimo ordinale equipotente ad esso. Per chiarezza indichiamo con α il cardinale $|A|$ considerato come ordinale e con β il cardinale $|B|$ considerato come ordinale. Ovviamente $\alpha = \beta$ se e solo se A e B sono equipotenti, ovvero se e solo se $|A| = |B|$.

Se $|A|$ è strettamente minore di $|B|$ in potenza, allora α può essere messo in corrispondenza solo con una parte dell'ordinale β , ma i due ordinali non possono essere uguali, altrimenti vi sarebbe equipotenza tra A e B ; in definitiva, essendo l'ordinamento tra ordinali un ordinamento totale, $\alpha < \beta$.

Viceversa, se $\alpha < \beta$, essendo i due ordinali i minimi ordinali equipotenti ai due insiemi, α deve essere equipotente a una parte propria di β , altrimenti sarebbe un ordinale inferiore a β equipotente con B , contro il fatto che β è il minimo ad essere equipotente con B ; in definitiva, $|A| < |B|$. ■

La proposizione precedente implica che l'ordinamento in potenza dato tra cardinali è un ordinamento totale.

Se A è un insieme di cardinalità $\aleph_i$, allora si indica con $2^{\aleph_i}$ la cardinalità di $\mathcal{P}(A)$. Esistono cardinali intermedi tra $\aleph_i$ e $2^{\aleph_i}$? Tale questione, nota come *ipotesi generalizzata del continuo* (IGC) e dibattuta per quasi un secolo, compariva al primo posto nella famosa lista dei grandi problemi che David Hilbert sottopose al Congresso internazionale dei matematici a Parigi nel 1900. Essa ha ricevuto una risposta definitiva nel 1963 ad opera di P. J. Cohen con

la scoperta che sono ugualmente concepibili una nozione insiemistica, detta cantoriana, in cui tali cardinali intermedi non esistono, e nozioni non cantoriane in cui vale il contrario. Più propriamente, estendendo alcuni risultati ottenuti da Gödel negli anni Quaranta, Cohen ha dimostrato che l'assioma di scelta è logicamente indipendente dagli altri assiomi insiemistici e che l'ipotesi generalizzata del continuo (IGC) è indipendente da ZFC (ZF + assioma di scelta). A sua volta, un precedente risultato di Sierpinski aveva stabilito che IGC implica AC.

Una corrispondenza biunivoca f tra due insiemi ordinati A, B si dice un *isomorfismo d'ordine* (e in tal caso A e B si dicono ordinatamente isomorfi) se, indicando con $\leq_1, \leq_2$ gli ordinamenti sui due insiemi, vale per ogni $x, y \in A$:

$$x \leq_1 y \Leftrightarrow f(x) \leq_2 f(y).$$

Si verifica che un insieme bene ordinato è (ordinatamente) isomorfo con un solo ordinale α che dicesi il suo *tipo d'ordine*.

Esercizio 1.25 *Si determini un isomorfismo d'ordine tra ω e $\omega \times \omega$.*

Esercizio 1.26 *Si dimostri che un isomorfismo d'ordine tra due ordinali deve coincidere con la funzione di identità.*

Suggerimento Si consideri l'immagine di 0; essa deve essere necessariamente 0, altrimenti l'isomorfismo non sarebbe corretto. Analogamente l'immagine di 1 deve essere 1 e così di seguito (si prosegua per induzione transfinita).

1.12. La costruzione del linguaggio matematico

L'aspetto fondazionale e quello di simbolizzazione matematica sono le motivazioni principali dei fondatori della logica matematica. Entrambi gli aspetti si possono ricondurre ai progetti leibniziani di una *Characteristica universalis* e di un *Calculus ratiocinator*, vale a dire a una ideografia universale dei concetti matematici e un relativo calcolo, analogo a quello aritmetico, per potere algoritmizzare il ragionamento. Nel *Formulario mathematico* di Giuseppe Peano (vol. 5, 1908) si possono trovare analisi, storia ed etimologia di simboli e termini matematici fondamentali. La nozione astratta di operazione è emersa gradualmente in matematica con lo svilupparsi dell'algebra astratta (non più relativa ai sistemi numerici, ma a entità del tutto generali: vettori, matrici, sistemi ipercomplessi, proposizioni, classi). La maturazione di una nozione generale di operazione si è avuta, a partire da F. Gauss (1777-1855), a opera degli algebristi dell'Ottocento (Hamilton, Cayley, Grassmann, De Morgan, Boole). La teoria astratta delle relazioni risale essenzialmente a A. De Morgan, Ch. S. Peirce e E. Schröder. La teo-

ria delle classi come teoria dell'inclusione risale essenzialmente a G. Boole; il suo studio assiomatico astratto costituisce la teoria delle cosiddette algebre di Boole. La teoria degli insiemi, come teoria dell'appartenenza, risale a Bolzano e soprattutto a Cantor e Frege. Il paradosso di Russell, comunicato da Russell a Frege in una famosa lettera del 1902, mise in crisi la teoria delle classi di Frege e di conseguenza la teoria fondazionale della matematica che a essa si richiamava. Esso è collegato a una serie di paradossi (di Burali-Forti, di Cantor, di Richard), alcuni risalenti alla logica greca, che scossero profondamente le intuizioni matematiche fondamentali postulando una revisione critica e rigorosa del linguaggio e dei concetti matematici di base; dalla crisi delle certezze matematiche prese le mosse la moderna logica matematica. Oltre a promuovere una rivoluzione concettuale nella logica e nella matematica, tali paradossi furono spesso fonte di ispirazione di nuove idee. Le dimostrazioni secondo il cosiddetto metodo diagonale non sono altro che argomenti basati sul ragionamento di Russell; ne è un esempio la famosa dimostrazione di Cantor sulla non-numerabilità dei numeri reali. Le prime teorie delle classi introdotte per superare il paradosso di Russell si basavano sulla nozione di tipo logico tramite cui si classificavano gli insiemi: se $A \in B$, allora B deve avere un tipo superiore a quello di A . Le più note teorie che caratterizzano la nozione di insieme attraverso sistemi di assiomi sono ZF e NBG. La prima si basa sul principio di separazione (lo schema di comprensione ristretto agli elementi di un insieme già dato) di Zermelo, Fraenkel e Skolem; la seconda sulla distinzione classe/insieme, introdotta da von Neumann, Gödel, Bernays. Entrambe studiano il concetto di insieme individuando assiomi che evitano paradossi del tipo di Russell e che possano consentire la costruzione di insiemi a un livello di astrazione sempre più alto (insiemi di insiemi di insiemi...). In tal senso la teoria degli insiemi si può qualificare come una sorta di studio dell'ontologia dell'astrazione matematica volta a stabilire fino a che punto le entità esistenti a un certo livello di astrazione possono essere considerate individui su cui basare ulteriori processi di astrazione. La teoria degli insiemi costituisce il quadro di riferimento per quasi tutte le teorie matematiche e la notazione insiemistica è il linguaggio base della pratica matematica corrente. Un gruppo di matematici francesi, riuniti sotto lo pseudonimo di Nicolas Bourbaki, ha intrapreso, intorno alla metà del Novecento, il progetto di esprimere in modo rigoroso qualsiasi concetto matematico in termini esclusivamente insiemistici. L'influenza di tale lavoro è stata notevole, infatti in quasi tutta la trattatistica matematica la nozione di operazione su un insieme A è ridotta a quella di un insieme di coppie (argomento, risultato) con la proprietà che non possono esservi due coppie distinte con ugual argomento. Tale punto di vista ha certamente il pregio di una grande economia concettuale, tuttavia in tal modo operazioni e relazioni presuppongono necessariamente le classi su cui agi-

scono. Spesso ciò risulta innaturale; per esempio, non occorre presupporre alcuna classe per definire l'operazione di identità. Inoltre spesso un'operazione è ben definita come regola di applicazione e produzione di valori, ma è difficile o inutilmente costoso definire a priori l'insieme di oggetti a cui essa è applicabile, soprattutto se tale insieme è infinito. Per questo motivo molte teorie matematiche costruttive partono da una nozione primitiva di operazione, indipendente da quella di insieme.

Le variabili furono usate, spesso in modo implicito e indiretto, già nelle prime trattazioni matematiche. La teoria aristotelica del sillogismo, nel presentare le figure valide di ragionamento, impiegava di fatto variabili di predicati unari. La geometria euclidea, tutte le volte che sviluppava argomenti generali su figure, punti, rette, segmenti e angoli, utilizzava variabili su tali entità geometriche.

L'uso delle variabili come incognite comparve sistematicamente a partire dalle formule risolutive delle equazioni, ad opera di matematici arabi intorno al xv secolo. Da tale uso discende anche la consuetudine di usare il simbolo x (prima lettera di *xei*, la trascrizione spagnola della lettera *shin* usata dagli arabi per indicare l'incognita). Nella matematica occidentale, a partire dalle opere del matematico francese François Viète (1540-1603), si giunse rapidamente a un impiego sempre più sistematico e complesso di simboli per variabili (indeterminate, parametri, incognite, letterali).

Le λ -espressioni hanno giocato un ruolo fondamentale nello studio dei formalismi logici. Esse furono introdotte da Alonzo Church intorno agli anni Trenta come base di una teoria fondazionale della matematica basata sul concetto di funzione. Più tardi il λ -calcolo si rivelò un formalismo adatto a rappresentare ogni tipo di algoritmo (dopo opportuna codifica dei dati tramite λ -espressioni). I λ -formalismi si collegano alla logica combinatoria, introdotta da M. Schöfinkel negli anni Venti e sviluppata in seguito da H. B. Curry, e agli schemi funzionali, introdotti da S. Eileberg e C. G. Elgot intorno agli anni Settanta, che esprimono in modo diretto le strutture per costruire funzioni complesse.

Le prime dimostrazioni in cui si può ravvisare uno schema induttivo furono usate da Pitagora e dalla sua scuola (vi sec. a. C.) nello studio di successioni numeriche. Altre dimostrazioni per induzione si ritrovano negli *Elementi* di Euclide (iii sec. a. C.) e successivamente in alcune opere di matematici arabi del Medioevo. Nel 1202 viene pubblicato il *Liber abbaci* di Leonardo Fibonacci nel quale viene presentata alla civiltà occidentale l'omonima successione induttiva. L'uso dell'induzione si trova nel *Arithmeticon libri duo* di Francesco Maurolico del 1575; però, nonostante sia largamente impiegato, nessun matematico cita esplicitamente il principio di induzione: il primo sarà Blaise Pascal nel *Traité du triangle arithmétique* del 1654 dove una forma primitiva di induzione è enunciata per dimostrare

proprietà riguardanti il cosiddetto triangolo di Tartaglia-Pascal. Il termine induzione compare successivamente e sotto l'influsso dell'induzione baconiana, secondo cui si possono trarre leggi generali dall'osservazione di casi particolari. In effetti le prime forme di induzione numerica consistevano nell'esaminare dei casi numerici e nell'arguire che le dimostrazioni fatte per particolari valori numerici seguivano uno schema applicabile a infiniti valori. Nel 1861 H. Grassmann definisce per induzione la somma e il prodotto. Nel 1888 Richard Dedekind nel suo trattato *Was sind und was sollen die Zahlen?* introduce il concetto di chiusura induttiva e dimostra la prima versione del teorema di *ricorsione*, ovvero l'esistenza di un'unica funzione g definita induttivamente su $\mathbb{N}$ tale che: $g(0) = k$, $g(n + 1) = f(g(n))$, dove f è una funzione totale sui naturali. L'anno successivo, riprendendo in parte e sviluppando gli studi di Grassmann e Dedekind, Peano enuncia il principio di induzione come uno degli assiomi che descrivono i numeri naturali. Il principio di induzione è di importanza incalcolabile per tutta la matematica costruttiva e discreta. Più della metà delle definizioni e dimostrazioni presentate in questo testo sono ottenute applicando tale principio.

Capitolo 2

Logica predicativa

Una *proposizione* è un'entità a cui, secondo una data interpretazione, è attribuibile un valore di verità vero o falso (1/0, V/F, tt/ff). Ogni teoria matematica è costituita da proposizioni che asseriscono proprietà o relazioni su *individui* di un certo universo (numeri, sequenze, punti, figure ecc.). Gran parte delle proposizioni matematiche può essere espressa utilizzando i seguenti *simboli logici* di *connettivi* e *quantificatori*:

$$\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists$$

da leggersi: *non*, *e*, *o*, *se allora*, *se e solo se* (*sse*), *per ogni*, *per qualche* (*esiste*). In inglese: *not*, *and*, *or*, *if then*, *if and only if* (*iff*), *for every*, *for some* (*there is*). Il simbolo $\neg$ esprime il connettivo di *negazione*, $\wedge$ esprime il connettivo di *congiunzione*, $\vee$ quello di *disgiunzione*, $\rightarrow$ quello di *implicazione*, $\leftrightarrow$ quello di *equivalenza*, $\forall$ quello di *quantificazione universale*, $\exists$ quello di *quantificazione esistenziale*.

La logica predicativa, detta anche *logica del primo ordine* (per distinguerla da logiche di ordine superiore in cui gli individui possono essere classi, funzioni o relazioni) definisce:

- la *sintassi predicativa*, e cioè le regole con cui i connettivi e i quantificatori si combinano per costruire formule predicative;
- la *semantica predicativa*, e cioè le regole secondo cui tali espressioni sono interpretate come proposizioni.

2.1. Sintassi predicativa

Diciamo *segnatura* (predicativa) un insieme di ~~simboli~~ Σ per denotare individui, funzioni, relazioni e proposizioni. Più precisamente, per definire

una segnatura Σ occorre specificare un insieme di simboli e suddividerli in *funzionali* e *relazionali*, associando a ciascuno un numero naturale detto *arietà* del simbolo. I simboli funzionali di arietà 0 sono simboli di *costanti* (individuali), i simboli relazionali di arietà 0 sono simboli *proposizionali* e i simboli relazionali di arietà k (con $k > 0$) si dicono anche *predicati*. Una Σ -struttura o un Σ -modello $\mathcal{M}$ è una struttura relazionale in cui vi è una relazione k -argomentale per ogni simbolo relazionale di arietà k di Σ e una funzione k -argomentale per ogni simbolo funzionale di arietà k di Σ . In particolare, ai simboli di costante di Σ è associato un elemento del dominio di $\mathcal{M}$ e ad ogni simbolo proposizionale un valore di verità.

La sintassi della logica predicativa è relativa a una prefissata *segnatura* Σ e a un insieme V di *variabili*, che nel seguito indicheremo con $x, y, z, \dots$ (o altri simboli di volta in volta, esplicitamente o implicitamente specificati). Primo compito della sintassi predicativa è la definizione degli insiemi di termini e di formule costruibili a partire dai simboli di una segnatura Σ e da un insieme di variabili V .

Nel seguito le lettere maiuscole $P, Q, R, \dots$ indicheranno simboli proposizionali o relazionali e le lettere minuscole: $a, b, c, f, g, \dots$ indicheranno simboli di costante o di funzione. Si useranno anche scritture del tipo $P_$, $Q_$, $f_$, ... per indicare con il numero di trattini l'arietà del simbolo.

Assumiamo oltre ai simboli di Σ e V due simboli di parentesi e un simbolo di virgola (che indicheremo con i soliti simboli tipografici per le parentesi tonde e la virgola).

L'insieme $T_\Sigma(V)$ dei *termini* sulla segnatura Σ e sulle variabili V è definito induttivamente ponendo per ogni generica variabile x , generica costante c e generico funtore (k -ario) f :

$$x \in T_\Sigma(V)$$

$$c \in T_\Sigma(V)$$

$$t_1, \dots, t_k \in T_\Sigma(V) \Rightarrow f(t_1, \dots, t_k) \in T_\Sigma(V).$$

L'insieme delle Σ -formule atomiche è costituito:

- dai simboli proposizionali;
- dalle sequenze $P(t_1, \dots, t_k)$ in cui P è un predicato k -ario della segnatura e $t_1, \dots, t_k$ termini in $T_\Sigma(V)$;
- dalle sequenze $(t_1 = t_2)$ per ogni coppia $t_1, t_2 \in T_\Sigma(V)$.

L'insieme $F_\Sigma(V)$ delle Σ -formule è definito per induzione:

Le Σ -formule atomiche sono Σ -formule predicative.

Se φ, ψ sono Σ -formule predicative e x una variabile, allora le seguenti sono Σ -formule predicative:

$$(\neg \varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi), (\forall x \varphi), (\exists x \varphi).$$

Spesso, quando la cosa non ingenera confusione, si omettono virgole e parentesi scrivendo per esempio Px, Rxy, fx in luogo di $P(x), R(x,y), f(x)$. Inoltre le quantificazioni ripetute dello stesso tipo saranno indicate una sola volta; per esempio $(\forall x(\forall y \dots))$ si abbrevia con $\forall xy \dots$ e analogamente $(\exists x(\exists y \dots))$ si abbrevia con $\exists xy \dots$.

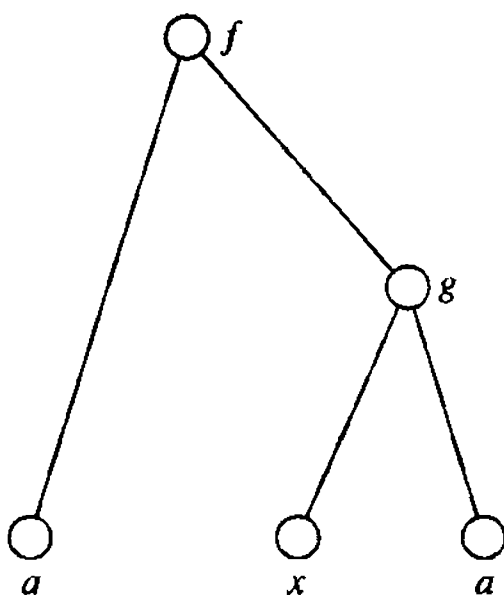
Esempio 2.1 Costruiamo a passi il termine

$$f(a, g(x, a))$$

sulla segnatura $\{a, f_, g_\}$ e variabile x .

1. x variabile;
2. a costante;
3. $g(x, a)$ termine: da 1, 2 e $g_\$;
4. $f(a, g(x, a))$ termine: da 2, 3 e $f_\$.

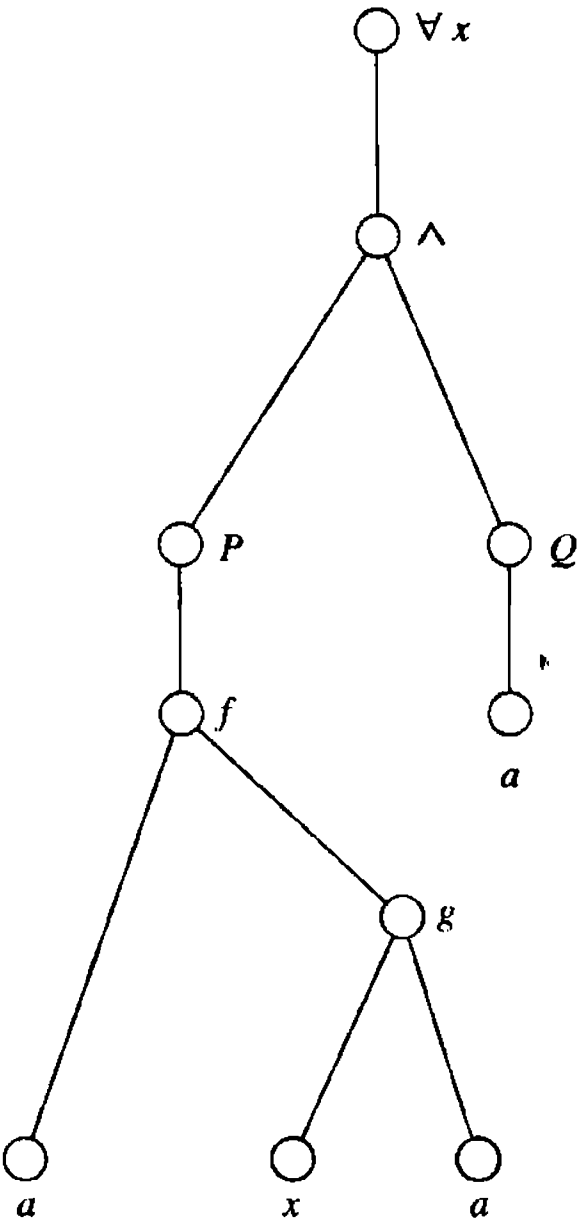
Ricordiamo che un termine su una segnatura individua un albero ai cui nodi sono associati i simboli della segnatura. L'albero per il termine appena costruito è il seguente:



In modo del tutto analogo si costruiscono alberi che rappresentano formule. Il seguente albero individua la sintassi della formula

$$\forall x(P(f(a, g(x, a))) \wedge Q(a))$$

dove P, Q sono due predicati binari, mentre gli altri simboli sono come nell'albero precedente, e $\forall x$ è considerato come un unico simbolo:



Nelle formule $(\forall x \varphi)$, $(\exists x \varphi)$ la variabile x si dice *vincolata* o *quantificata*, poiché la variabilità di x è eliminata dai quantificatori. Una variabile che occorre non quantificata in una formula si dice che vi occorre *libera*. Spesso si scrive $\varphi(x)$ per mettere in evidenza l'eventuale occorrenza della variabile libera x nella formula φ .

Gli insiemi $\text{var}(t)$ e $\text{free}(\varphi)$ determinano rispettivamente le *variabili del termine* t e le *variabili libere della formula* φ . La loro definizione induttiva è molto semplice (le variabili libere di $\varphi * \psi$ sono quelle di φ unite a quelle di ψ , quelle di $\neg \varphi$ sono le stesse di φ e quelle di $Qx \varphi$ sono quelle di φ , eccetto x , ove $*$ indica un connettivo binario e Q un quantificatore).

Data una formula $\varphi(x)$ e un termine t , il termine si dice *liberamente sostituibile* a x in $\varphi(x)$ se, sostituendo t in tutte le occorrenze libere di x in $\varphi(x)$, nessuna variabile di t risulta quantificata dopo la sostituzione. Vedremo in seguito che una regola deduttiva fondamentale consiste nell'ottenere, da una formula del tipo $\forall x \varphi(x)$, una formula in cui la quantificazione è eliminata e la variabile x è sostituita da un termine. Affinché una tale regola sia corretta, ovvero non conduca da una formula vera a una falsa, è necessario richiedere che il termine sostituito sia liberamente sostituibile a x in $\varphi(x)$. Consideriamo per esempio la formula $\exists y (\neg x = y)$; in tale formula il termine

y non è liberamente sostituibile a x . Se sostituissimo y al posto di x otterremmo infatti $\exists y(\neg y = y)$ che è sempre falsa nonostante $\forall x \exists y(\neg x = y)$ sia vera se riferita a due individui distinti.

Nel seguito scriveremo $\varphi(t)$ per indicare la formula ottenuta da $\varphi(x)$ dopo avere ivi sostituito t a tutte le occorrenze libere di x , assumendo che t sia liberamente sostituibile a x in $\varphi(x)$.

Spesso si usano punti piuttosto che parentesi, o anche punti e parentesi insieme. Per esempio, $\forall x.Px \rightarrow Qx$ sta per $\forall x(Px \rightarrow Qx)$, mentre $\forall x Px \rightarrow Qx$ sta per $(\forall x Px) \rightarrow Qx$; ed anche $\forall x.(Px \rightarrow Qx) \vee Rx$ sta per $\forall x((Px \rightarrow Qx) \vee Rx)$ o $\forall x: Px \rightarrow Qx. \vee Rx$ (più punti separano di più, e parentesi più interne aggregano prima).

La *complessità* logica $\text{comp}(\varphi)$ di una formula φ è un numero naturale. Si definisce per induzione ponendola nulla per le formule atomiche e ponendo per ogni connettivo binario $*$ e per ogni quantificatore Q : $\text{comp}(\varphi * \psi) = \max(\{\text{comp}(\varphi), \text{comp}(\psi)\}) + 1$ e $\text{comp}(Qx\varphi) = \text{comp}(\neg \varphi) = \text{comp}(\varphi) + 1$.

Definizione 2.1 *Un Σ -termine senza variabili dicesi Σ -termine chiuso. Una formula predicativa φ senza variabili libere, ovvero per cui $\text{free}(\varphi) = \emptyset$, dicesi Σ -formula chiusa o Σ -proposizione (o Σ -enunciato).*

I Σ -termini chiusi e le Σ -proposizioni si indicano rispettivamente con T_Σ e F_Σ .

Per evitare l'uso di troppe parentesi si utilizza in genere una *convenzione* che stabilisce la seguente priorità nell'applicazione di connettivi e quantificatori: la *negazione e le quantificazioni precedono i connettivi binari*; e tra i connettivi binari $\wedge, \vee$ precedono $\rightarrow$ e $\leftrightarrow$.

Quando si adoperano i quantificatori è essenziale considerare la loro portata, ovvero la sottoformula a cui si riferiscono, indicata tramite parentesi. Spesso nel linguaggio matematico la quantificazione universale è espressa implicitamente, ovvero quando si asserisce una formula in cui compaiono delle variabili si intende che vale ogni proposizione ottenuta da essa assegnando valori alle variabili (si asserisce $x + y = y + x$ per intendere che vale la sua quantificazione universale). La forma usuale delle proposizioni matematiche fondamentali è di tipo universale. Nel linguaggio naturale vi sono vari modi di esprimere il contenuto di una proposizione universale. Ecco alcuni modi con cui si può esprimere la famosa *congettura di Goldbach* (matematico del Settecento).

1. Tutti i numeri pari diversi da 2 sono somma di due primi.
2. Ogni numero pari diverso da 2 è somma di due primi.
3. Se un numero pari è diverso da 2, allora è somma di due primi.
4. Un numero pari che è diverso da 2 è anche somma di due primi.

Indichiamo con $P(x, y)$ la relazione x è padre di y . In tal caso

$$\forall y \exists x P(x, y)$$

esprime il fatto biologicamente vero che *ogni uomo ha un padre*; se scambiamo l'ordine dei due quantificatori otteniamo:

$$\exists x \forall y P(x, y)$$

che afferma che *esiste un padre di tutti gli uomini*, fatto la cui validità è tutt'altro che reale. Tale esempio mostra che *l'ordine delle quantificazioni* è essenziale nella determinazione del senso di una proposizione, cioè le due quantificazioni non sono commutative.

Spesso è utile il seguente quantificatore $\exists!$ che indica l'*esistenza di un unico valore* che soddisfa una formula a cui si applica. Esso è una semplice abbreviazione poiché può essere sempre espresso tramite quantificazione esistenziale e uguaglianza:

$$\exists! x \varphi(x) \equiv \exists x (\varphi(x) \wedge \forall y (\varphi(y) \rightarrow x = y)).$$

Esercizio 2.1 Si consideri la segnatura $\{P_, R_, a, b, f_, R_-\}$. Dare esempi di formule predicative corrette in tale segnatura, e determinare i passi dettagliati di costruzione delle formule e la loro complessità.

Esercizio 2.2 Una formula predicativa dicesi buona se nessuna sua variabile libera occorre vincolata in una sua sottoformula. Si definisca per induzione la classe delle formule predicative buone su un prefissato alfabeto predicativo.

2.2. Semantica predicativa

Definiamo ora matematicamente il significato delle proposizioni predicative. Fissiamo innanzitutto un *universo* D . Interpretare una proposizione su D significa essenzialmente leggere su tale universo i simboli funzionali e relazionali che occorrono nella proposizione, assumere che le variabili varino sullo stesso universo e dare a connettivi e quantificatori il loro significato usuale.

Consideriamo una segnatura Σ . Per dare semantica alle proposizioni di Σ , estenderemo tale segnatura con gli elementi dell'universo D come ulteriori costanti, dando significato alla classe più ampia delle proposizioni su tale segnatura estesa. Procederemo in tre fasi successive.

Semantica dei simboli di Σ

Si consideri una Σ -struttura $\mathcal{M}$ di dominio D e indichiamo con $f^{\mathcal{M}}$, $P^{\mathcal{M}}$, $c^{\mathcal{M}}$ e $Q^{\mathcal{M}}$ la denotazione in $\mathcal{M}$ di un generico simbolo funzionale (n -ario) f , di un

generico simbolo relazionale (n -ario) P , di un generico simbolo di costante individuale c , e di un generico simbolo proposizionale Q . Le loro *interpretazioni* o denotazioni in $\mathcal{M}$ sono rispettivamente: una funzione di arietà n , una relazione di arietà n (un insieme di n -ple), un elemento di D , e un valore di verità rappresentabile con 1 (*vero*) o 0 (*falso*).

Semantica dei termini su Σ e D

Dopo aver dato significato ai simboli della segnatura, daremo significato ai termini chiusi e alle proposizioni. A tal fine bisogna *estendere la nozione di termine chiuso e di proposizione*.

Data una segnatura Σ e un insieme D , l'insieme $T_{\Sigma, D}$, dei *termini chiusi su Σ e D* , coincide con l'insieme di termini chiusi della segnatura Σ_D in cui tutti gli elementi di D sono considerati come ulteriori costanti individuali da aggiungere a Σ . L'insieme $F_{\Sigma, D}$ è l'insieme di proposizioni (formule senza variabili libere) sulla segnatura Σ_D .

Definiamo per induzione l'interpretazione $()^{\mathcal{M}}$ sui termini $T_{\Sigma, D}$. Poniamo per ogni costante $c \in \Sigma$, per ogni $d \in D$ e per ogni $t_i \in T_{\Sigma, D}$ con $i = 1, \dots, n$:

$$(c)^{\mathcal{M}} = c^{\mathcal{M}}$$

$$(d)^{\mathcal{M}} = d$$

$$(f(t_1, \dots, t_n))^{\mathcal{M}} = f^{\mathcal{M}}((t_1)^{\mathcal{M}}, \dots, (t_n)^{\mathcal{M}}).$$

Semantica delle proposizioni su Σ e D

Scriviamo

$$\mathcal{M} \models \varphi$$

per indicare che *la proposizione φ vale nel modello $\mathcal{M}$* o che il modello $\mathcal{M}$ soddisfa la proposizione φ viceversa scriviamo

$$\mathcal{M} \not\models \varphi$$

in caso contrario. La relazione $\models$ dicesi di *validità*.

Se Φ è un insieme di proposizioni scriviamo

$$\mathcal{M} \models \Phi$$

per indicare che *tutte le proposizioni di Φ valgono in $\mathcal{M}$* ; e scriviamo

$$\mathcal{M} \not\models \Phi$$

per indicare che *tutte le proposizioni di Φ non valgono in $\mathcal{M}$* .

La relazione $\models$ è definita per induzione nel modo seguente:

$$1. \mathcal{M} \models P(t_1, \dots, t_n) \Leftrightarrow ((t_1)^{\mathcal{M}}, \dots, (t_n)^{\mathcal{M}}) \in P^{\mathcal{M}}.$$

- 2. Se $\mathcal{M} \models \varphi$ e $\mathcal{M} \models \psi$, allora $\mathcal{M} \models \varphi \wedge \psi$, altrimenti $\mathcal{M} \not\models \varphi \wedge \psi$.
- 3. Se $\mathcal{M} \not\models \varphi$ e $\mathcal{M} \not\models \psi$, allora $\mathcal{M} \not\models \varphi \vee \psi$, altrimenti $\mathcal{M} \models \varphi \vee \psi$.
- 4. Se $\mathcal{M} \models \varphi$ e $\mathcal{M} \not\models \psi$, allora $\mathcal{M} \not\models \varphi \rightarrow \psi$, altrimenti $\mathcal{M} \models \varphi \rightarrow \psi$.
- 5. Se $\mathcal{M} \not\models \varphi$, allora $\mathcal{M} \models \neg \varphi$, altrimenti $\mathcal{M} \not\models \neg \varphi$.
- 6. Se $\mathcal{M} \models \varphi \leftrightarrow \psi$, allora $\mathcal{M} \models \varphi \leftrightarrow \psi$, altrimenti $\mathcal{M} \not\models \varphi \leftrightarrow \psi$.
- 7. Se $\mathcal{M} \models \{\varphi(d) \mid d \in D\}$, allora $\mathcal{M} \models \forall x \varphi(x)$, altrimenti $\mathcal{M} \not\models \forall x \varphi(x)$.
- 8. Se $\mathcal{M} \not\models \{\varphi(d) \mid d \in D\}$, allora $\mathcal{M} \not\models \exists x \varphi(x)$, altrimenti $\mathcal{M} \models \exists x \varphi(x)$.

La semantica dei connettivi si esprime usualmente con delle *tavole di verità* del tipo seguente (tab. 2.1) in cui si indica il valore di verità delle formule composte, in funzione del valore di verità delle formule componenti.

Tabella 2.1 Tavole di verità dei connettivi

φ	ψ	$\neg \varphi$	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \rightarrow \psi$	$\varphi \leftrightarrow \psi$
1	1	0	1	1	1	1
1	0		0	1	0	0
0	1	1	0	1	1	0
0	0		0	0	1	1

Indichiamo con Mod_Σ la classe di tutti i Σ -modelli, $\text{Mod}_\Sigma(\varphi)$ è la classe di tutti i Σ -modelli in cui vale φ e, dato un insieme Φ di Σ -proposizioni, $\text{Mod}_\Sigma(\Phi)$ è la classe di tutti i Σ -modelli che soddisfano contemporaneamente tutte le formule di Φ .

Lo stesso simbolo $\models$ esprime anche la relazione di *conseguenza logica* definita nel modo seguente.

Definizione 2.2 Se $\text{Mod}_\Sigma(\Phi) \subseteq \text{Mod}_\Sigma(\varphi)$ si pone:

$$\Phi \models \varphi$$

e si dice che φ è *conseguenza logica* di Φ , cioè che φ vale in tutti i modelli in cui valgono tutte le formule di Φ . Se $\Phi \models \{\varphi_1, \dots, \varphi_n\}$ si scrive semplicemente:

$$\varphi_1, \dots, \varphi_n \models \varphi.$$

Un insieme Φ di Σ -proposizioni si dice *soddisfacibile* se $\text{Mod}_\Sigma(\Phi)$ non è un insieme vuoto, ovvero se tutte le formule di Φ sono soddisfatte da qualche Σ -modello; sinteticamente indicheremo questo fatto scrivendo

$$\Phi \not\models \perp$$

ove il simbolo $\perp$ indica l'assurdo, ovvero la congiunzione di una qualsiasi proposizione con la sua negata ($\text{Mod}_\Sigma(\perp) = \emptyset$).

In caso contrario si dice che Φ è *insoddisfacibile* e si scrive

$$\Phi \models \perp.$$

Dato un insieme Φ di Σ -proposizioni e una Σ -proposizione φ abbrevieremo spesso $\Phi \cup \{\varphi\}$ scrivendo semplicemente Φ, φ . Dalle definizioni precedenti segue facilmente il seguente criterio di *dimostrazione per assurdo*.

Proposizione 2.1 (principio di dimostrazione per assurdo)

$$\Phi \models \varphi \Leftrightarrow \Phi, \neg \varphi \models \perp.$$

Dimostrazione Se non vi è alcun modello di $\Phi \cup \{\neg \varphi\}$, allora in ogni modello di Φ non può valere $\neg \varphi$, quindi deve valere φ , ovvero per la definizione di $\models$ si ha $\Phi \models \varphi$. Il viceversa è ovvio. ■

Definizione 2.3 Una Σ -teoria è un insieme Φ di Σ -proposizioni tale che se $\Phi \models \varphi$, allora $\varphi \in \Phi$.

In senso lato comunque si intende per Σ -teoria un qualsiasi insieme di Σ -proposizioni.

Definizione 2.4 Una formula proposizionale è una formula costruita solo con simboli proposizionali e connettivi. Una formula proposizionale che è una verità logica predicativa si dice *tautologia*. Una teoria proposizionale è un insieme di formule proposizionali.

Definizione 2.5 Una Σ -proposizione φ si dice logicamente valida o verità logica (della logica predicativa) se essa è valida in ogni Σ -struttura. In tal caso si pone:

$$\models \varphi.$$

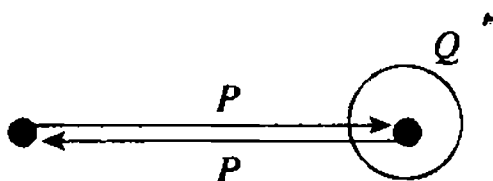
Una proposizione logicamente valida è concepibile come una proposizione che è conseguenza logica di una teoria vuota (e quindi che vale in tutti i modelli), ovvero:

$$\models \varphi \Leftrightarrow \emptyset \models \varphi.$$

Un *letterale* è una formula atomica o la negazione di una formula atomica. Sia $\mathcal{M}$ un Σ -modello di dominio D . Il *diagramma* $\text{Diag}(\mathcal{M})$ di $\mathcal{M}$ è costituito dall'insieme dei letterali di $F_{\Sigma, D}$, che valgono nel modello $\mathcal{M}$. Si constata facilmente che una interpretazione predicativa su un modello $\mathcal{M}$ di dominio D è completamente determinata dal suo diagramma. Un Σ -modello $\mathcal{M}$ di dominio D può essere sempre considerato come un modello nella segna-

tura Σ_D in cui tutti gli elementi del dominio D sono aggiunti a Σ come costanti interpretate in se stesse. Quando si vuole considerare $\mathcal{M}$ come modello in tale segnatura estesa lo si indica con $\mathcal{M}_\Delta$. La Σ -teoria $Th(\mathcal{M})$ è costituita da tutte le proposizioni F_Σ che valgono nel modello $\mathcal{M}$, mentre $Th(\mathcal{M}_\Delta)$ è la teoria delle proposizioni di $F_{\Sigma,D}$ che valgono in $\mathcal{M}_\Delta$ (si noti la differenza).

I *modelli finiti* la cui segnatura ha solamente simboli predicativi binari o unari possono essere rappresentati in modo sintetico con formulazioni grafiche in cui gli elementi sono dei nodi, le relazioni binarie frecce che colleghino le coppie di elementi in relazione e le proprietà dei cerchi che includono i nodi che le verificano. Si consideri, per esempio, il seguente modello sulla segnatura $\{P-- , Q-\}$:



Esercizio 2.3 Si dica, giustificando le risposte, quali delle seguenti formule sono vere e quali sono false nel modello sopra raffigurato:

1. $\forall xy (P(x, y) \rightarrow Q(x))$
2. $\forall x (\neg P(x, y) \vee Q(x))$
3. $\forall xy (P(x, y) \vee Q(x))$.

Si determini inoltre quali sono le proposizioni di complessità 1 sulla segnatura considerata che valgono nel modello.

Esercizio 2.4 Si dia una teoria che abbia solo modelli infiniti.

Suggerimento Si consideri una relazione binaria connessa irreflessiva e transitiva.

Ogni modello è *equivalente* a un modello avente lo stesso dominio, la cui segnatura è costituita solo da simboli di predicati. Tale equivalenza va intesa nel modo seguente: ogni simbolo di funzione n -aria f può essere tradotta in un predicato $P_f(x_1, \dots, x_n, x_{n+1})$ con $n+1$ variabili libere tale che, per ogni $(n+1)$ -upla del dominio, $P_f(a_1, \dots, a_n, a_{n+1})$ vale sul secondo modello se $f(a_1, \dots, a_n) = a_{n+1}$ sul primo. Infine per ogni costante individuale c vi è un predicato $P_c(x)$ con una variabile libera tale che, per ogni a del dominio, $P_c(a)$ vale sul secondo modello se sul primo vale $c = a$.

Inoltre, un modello su una segnatura costituita solo da predicati può essere rappresentato in un modello con soli predicati unari e binari a patto di estendere il dominio del primo modello. Consideriamo per esempio un modello con un predicato ternario P . Estendiamo il dominio introducendo per ogni terna (a_1, a_2, a_3) del dominio originale un nuovo individuo s e definiamo

nel nuovo modello i seguenti predicati binari C_1, C_2, C_3 tali che $C_1(s, a_1), C_2(s, a_2), C_3(s, a_3)$; infine definiamo nel nuovo modello il predicato unario Q tale che $Q(s)$ se e solo se vale $P(a_1, a_2, a_3)$ nel modello di partenza. Dalla definizione data del nuovo modello segue che nel primo vale $P(a_1, a_2, a_3)$ se e solo se in questo vale la formula $C_1(s, a_1) \wedge C_2(s, a_2) \wedge C_3(s, a_3) \wedge Q(s)$. In tal senso il modello appena definito rappresenta quello di partenza tramite congiunzione di predicati binari e unari.

Infine, poiché un predicato unario P può essere facilmente rappresentato con un predicato binario R , ponendo $R(a, a) \leftrightarrow P(a)$ (per ogni individuo a del dominio), possiamo concludere che ogni modello è completamente rappresentabile tramite un opportuno modello su una segnatura costituita solo da predicati binari, ovvero tramite un multigrafo orientato ed etichettato. Tale universalità rappresentativa delle relazioni binarie spiega l'importanza di tali relazioni, che del resto non deve sorprendere, visto che tutti i modelli sono definibili in termini insiemistici e che la teoria degli insiemi può essere costruita usando solamente il predicato binario di appartenenza.

Sulla nozione di modello si basano le *dimostrazioni di indipendenza*. Per dimostrare che da certe proposizioni $P_1, \dots, P_k$ non consegue la proposizione P , ovvero che P è logicamente indipendente da $P_1, \dots, P_k$ basta trovare un modello di $P_1, \dots, P_k$ che non è modello di P . Le origini di tale metodo risalgono ai modelli di geometrie non euclidee per dimostrare l'indipendenza del postulato delle parallele dagli altri assiomi euclidei. Nel primo libro di Euclide vi sono 23 definizioni (*oroi*) e 5 postulati (*aitemata*), più 9 assiomi (*axiomata*) del tutto generali. La proposizione 29 è la prima in cui si usa il postulato 5 e dimostra l'unicità della parallela a una retta per un punto. Il problema del quinto postulato era quello di provare la proposizione 29 indipendentemente dalle prime 28. Tale problema rimasto insoluto per secoli fu risolto introducendo per la prima volta (e in modo del tutto informale) la nozione di interpretazione di un sistema assiomatico. Il modo più semplice per spiegare l'indipendenza del quinto postulato, nei confronti degli altri postulati euclidei, consiste nel modello piano di Felix Klein il cui dominio è costituito dai punti interni a una circonferenza (che verificano il predicato *punto*) e dalle corde interne a tale circonferenza (che verificano il predicato *retta*) mentre le relazioni di appartenenza di un punto e di stare tra due punti sono quelle usuali ristrette ai punti delle corde considerate. In tal modo si perviene a un modello della geometria *iperbolica* di Lobačevskij in cui vi sono infinite rette "parallele" a una retta data che passano per un punto esterno alla retta.

Esempio 2.2 Si consideri una segnatura con 4 predicati: P, R entrambi unari e $\in, \perp$ binario il primo e ternario il secondo. Essi esprimono le proprietà e relazioni geometriche di punto, retta, appartenenza (di un punto a

una retta) e di stare-tra due punti ($\perp a b c$ se b sta tra a e c). Esprimiamo con proposizioni, in tale segnatura, le condizioni geometriche considerate.

1. Per ogni due punti distinti esiste una e una sola retta che passa per entrambi:

$$\forall xy(Px \wedge Py \wedge x \neq y \rightarrow \exists! z(Rz \wedge x \in z \wedge y \in z)).$$

2. Ogni retta contiene almeno due punti distinti:

$$\forall z(Rz \rightarrow \exists xy(Px \wedge Py \wedge x \neq y \wedge x \in z \wedge y \in z)).$$

3. Esistono una retta e un punto fuori di essa:

$$\exists xz(Px \wedge Rz \wedge \neg x \in z).$$

4. La relazione $\perp$ è simmetrica rispetto al primo e terzo argomento:

$$\forall xyu(\perp xyu \rightarrow \perp uyx).$$

5. Dati tre punti distinti allineati, uno di questi è sempre tra gli altri due:

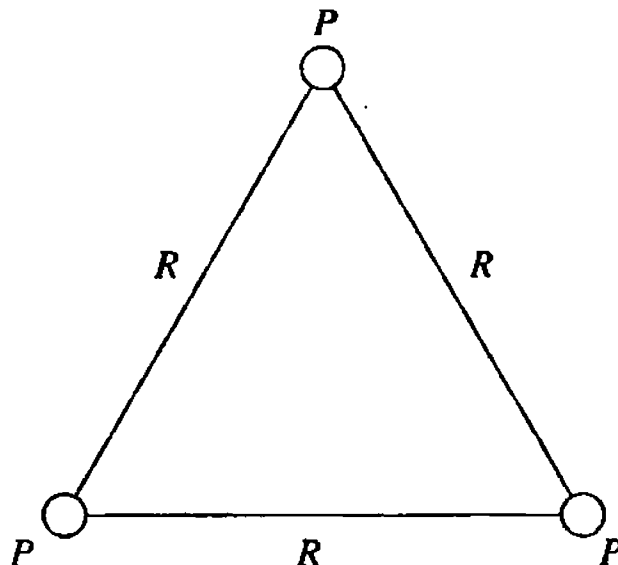
$$\forall xyuz(Px \wedge Py \wedge Pu \wedge Rz \wedge x \in z \wedge y \in z \wedge u \in z \rightarrow \perp xuy \vee \perp uxy \vee \perp xyu).$$

6. Data una retta e un punto fuori di essa, vi è sempre una e una sola retta che passa per il punto e non ha punti in comune con la prima retta:

$$\forall x(Px \wedge Rz \wedge \neg x \in z \rightarrow \exists! w(x \in w \wedge \neg \exists u(u \in z \wedge u \in w))).$$

Esempio 2.3 Dimostriamo che l'ultima proposizione dell'esempio precedente non è conseguenza logica delle altre.

Basta prendere come modello i tre vertici di un triangolo, che verificano il predicato P , e i tre lati del triangolo che verificano il predicato R , imponendo inoltre che ciascun vertice appartenga ai lati di cui è estremo (il predicato di "stare-tra" non vale per nessuna terna di punti):



Tale modello verifica tutte le proposizioni dell'esempio precedente, tranne l'ultima.

Esempio 2.4 Esprimiamo in logica predicativa, usando i predicati G , M , F (binario il primo e unari gli altri), le seguenti proposizioni sui rapporti di parentela:

1. Nessuno è genitore di se stesso:

$$\neg \exists x (Gxx).$$

2. Nessuno è sia maschio che femmina:

$$\neg \exists x (Mx \wedge Fx).$$

3. Ognuno è o maschio o femmina:

$$\forall x (Mx \vee Fx).$$

4. Ognuno ha un genitore:

$$\forall x \exists y Gyx.$$

5. Nessuno è genitore di tutti:

$$\neg \exists x \forall y Gxy.$$

6. Ognuno ha due genitori di sesso differente:

$$\forall x \exists yz (Gyx \wedge Gzx \wedge My \wedge Fz).$$

7. Ognuno ha un solo padre:

$$\forall x \exists y (Gyx \wedge My).$$

Esempio 2.5 Dimostriamo che dalle prime sei proposizioni dell'esempio precedente non segue logicamente l'ultima. A tal fine basta interpretare i predicati M , F , G sul dominio dei numeri naturali non nulli associando a M la proprietà di essere pari, a F quella di essere dispari, e a Gxy quella di essere multiplo proprio (x di y).

Uno *schema predicativo* è costruito con variabili sintattiche di formule e termini. Si usano schemi predicativi, piuttosto che formule predicative, quando non si intende fissare una specifica segnatura. Il seguente è uno schema predicativo, ove $\varphi(x)$ indica una generica formula con x come variabile libera e ψ indica una qualsiasi formula in cui x non occorre libera;

dimostriamo più avanti che esso è logicamente valido, i.e. ogni sua istanza determina una formula predicativa logicamente valida:

$$(\exists x \varphi(x) \rightarrow \psi) \leftrightarrow \forall x(\varphi(x) \rightarrow \psi).$$

Una formula predicativa può essere sempre vista come l'istanza di uno schema predicativo, e d'altra parte essa individua uno schema predicativo se i suoi simboli sono considerati come variabili sintattiche. Per tale motivo, ambigualmente, non si distingue tra schemi e formule predicative; il contesto indicherà il senso con cui tali espressioni simboliche sono usate.

Uno *schema proposizionale* è un particolare schema predicativo costruito tramite connettivi, a partire da variabili sintattiche per proposizioni, che si dicono anche *variabili proposizionali*. Per esempio

$$(\varphi \wedge \psi \rightarrow \chi) \rightarrow (\varphi \rightarrow (\psi \rightarrow \chi))$$

è uno schema proposizionale. Una formula proposizionale può essere sempre vista come l'istanza di uno schema proposizionale; viceversa essa individua uno schema se i suoi simboli proposizionali sono considerati come variabili proposizionali.

Diamo nel seguito una lista di schemi predicativi logicamente validi. Il lettore è invitato a esaminarli con attenzione. Alcuni di essi sono intuitivamente del tutto chiari, altri nascondono delle sottigliezze logiche che a prima vista possono sfuggire, ma che sono alla base di caratteristiche fondamentali della logica predicativa. Per secoli, l'attività basilare dei logici è consistita nello *scoprire leggi logiche* alla stregua di uno scienziato che scopre leggi naturali.

Esempio 2.6 Leggi logiche ($* \in \{\wedge, \vee\}$, $Q \in \{\forall, \exists\}$)

- | | |
|---|---------------------------------|
| 1. $(\varphi * \psi) \leftrightarrow (\psi * \varphi)$ | (commutatività) |
| 2. $(\varphi * (\psi * \chi)) \leftrightarrow ((\varphi * \psi) * \chi)$ | (associatività) |
| 3. $(\varphi \wedge (\psi \vee \chi)) \leftrightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \chi))$ | (distributività $\wedge \vee$) |
| 4. $(\varphi \vee (\psi \wedge \chi)) \leftrightarrow ((\varphi \vee \psi) \wedge (\varphi \vee \chi))$ | (distributività $\vee \wedge$) |
| 5. $(\varphi \wedge \psi) \vee \varphi \leftrightarrow \varphi$ | (assorbimento $\wedge \vee$) |
| 6. $(\varphi \vee \psi) \wedge \varphi \leftrightarrow \varphi$ | (assorbimento $\vee \wedge$) |
| 7. $\varphi * \varphi \leftrightarrow \varphi$ | (idempotenza) |
| 8. $\neg \neg \varphi \leftrightarrow \varphi$ | (doppia negazione) |
| 9. $\varphi \vee \neg \varphi$ | (terzo escluso) |
| 10. $\varphi \wedge \psi \leftrightarrow \neg(\neg \varphi \vee \neg \psi)$ | (De Morgan) |
| 11. $\varphi \vee \psi \leftrightarrow \neg(\neg \varphi \wedge \neg \psi)$ | (De Morgan) |
| 12. $\varphi \wedge (\varphi \rightarrow \psi) \rightarrow \psi$ | (modus ponens) |

13. $(\varphi \rightarrow \psi) \leftrightarrow (\neg \psi \rightarrow \neg \varphi)$	(contropositiva)
14. $(\varphi \rightarrow (\psi \rightarrow \chi)) \leftrightarrow (\varphi \wedge \psi \rightarrow \chi)$	(esportazione)
15. $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \chi)) \rightarrow (\varphi \rightarrow \chi)$	(sillogismo)
16. $((\varphi \vee \psi) \wedge (\neg \varphi \vee \chi)) \rightarrow (\psi \vee \chi)$	(risoluzione)
17. $\varphi \rightarrow (\psi \rightarrow \varphi)$	(antecedente onniconseguente)
18. $(\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta))$	(distributività $\rightarrow \rightarrow$)
19. $(\varphi \wedge \neg \varphi) \rightarrow \psi$	(tutto dall'assurdo)
20. $(\varphi \rightarrow \psi) \leftrightarrow \neg \varphi \vee \psi$	(implicazione con $\vee, \neg$)
21. $(\varphi \leftrightarrow \psi) \leftrightarrow (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$	(equivalenza con $\rightarrow, \wedge$)
22. $\neg \forall x \varphi \leftrightarrow \exists x \neg \varphi$	(negazione $\forall$)
23. $\forall x \varphi(x) \rightarrow \varphi(t)$	(eliminazione $\forall$)
24. $\varphi(t) \rightarrow \exists x \varphi(x)$	(introduzione $\exists$)
25. $QxQy\varphi \leftrightarrow QyQx\varphi$	(scambio Q)
26. $Qx\varphi(x) \leftrightarrow Qy\varphi(y)$	(ridenominazione Q)
27. $(Qx\varphi(x) * \psi) \leftrightarrow Qx(\varphi(x) * \psi)$	(prefisso $Q *$, $x \notin \text{var}(\psi)$)
28. $(\forall x \varphi \rightarrow \psi) \leftrightarrow \exists x(\varphi \rightarrow \psi)$	(prefisso $\forall \rightarrow$, $x \notin \text{var}(\psi)$)
29. $(\exists x \varphi \rightarrow \psi) \leftrightarrow \forall x(\varphi \rightarrow \psi)$	(prefisso $\exists \rightarrow$, $x \notin \text{var}(\psi)$)
30. $(\psi \rightarrow \forall x \varphi) \leftrightarrow \forall x(\psi \rightarrow \varphi)$	(prefisso $\rightarrow \forall$, $x \notin \text{var}(\psi)$)
31. $(\psi \rightarrow \exists x \varphi) \leftrightarrow \exists x(\psi \rightarrow \varphi)$	(prefisso $\rightarrow \exists$, $x \notin \text{var}(\psi)$).

Diamo ora altri modi per dare semantica alle formule predicative che mettono in luce aspetti importanti.

Semantica insiemistica delle proposizioni su Σ e D

Definiamo ora per induzione, per ogni $\varphi \in F_{\Sigma, D}$, l'insieme

$$\text{Mod}_{\Sigma, D}(\varphi)$$

che rappresenta l'insieme dei Σ -modelli di dominio D in cui vale φ . Indichiamo con $\text{Mod}_{\Sigma, D}$ la classe di tutti i Σ -modelli di dominio D . Ricordiamo che una relazione k -aria si identifica con un insieme di k -ple, quindi scriveremo che una k -pla gli appartiene, per dire che essa vale sulla k -pla.

$$\text{Mod}_{\Sigma, D}(t_1 = t_2) = \{\mathcal{M} \in \text{Mod}_{\Sigma, D} \mid (t_1)^{\mathcal{M}} = (t_2)^{\mathcal{M}}\}$$

$$\text{Mod}_{\Sigma, D}(P(t_1, \dots, t_k)) = \{\mathcal{M} \in \text{Mod}_{\Sigma, D} \mid \langle (t_1)^{\mathcal{M}}, \dots, (t_k)^{\mathcal{M}} \rangle \in P^{\mathcal{M}}\}$$

$$\text{Mod}_{\Sigma, D}(Q) = \{\mathcal{M} \in \text{Mod}_{\Sigma, D} \mid Q^{\mathcal{M}} = 1\}$$

$$\text{Mod}_{\Sigma, D}(\varphi \wedge \psi) = \text{Mod}_{\Sigma, D}(\varphi) \cap \text{Mod}_{\Sigma, D}(\psi)$$

$$\text{Mod}_{\Sigma, D}(\varphi \vee \psi) = \text{Mod}_{\Sigma, D}(\varphi) \cup \text{Mod}_{\Sigma, D}(\psi)$$

$$\text{Mod}_{\Sigma, D}(\neg \varphi) = \text{Mod}_{\Sigma, D} - \text{Mod}_{\Sigma, D}(\varphi)$$

$$\text{Mod}_{\Sigma, D}(\forall x \varphi(x)) = \bigcap_{a \in d} \text{Mod}_{\Sigma, D}(\varphi(a))$$

$$\text{Mod}_{\Sigma, D}(\exists x \varphi(x)) = \bigcup_{a \in d} \text{Mod}_{\Sigma, D}(\varphi(a))$$

La semantica dell'implicazione e della doppia implicazione è ricondotta a quella dei connettivi booleani ($\neg$, $\wedge$, $\vee$):

$$\text{Mod}_{\Sigma, D}(\varphi \rightarrow \psi) = \text{Mod}_{\Sigma, D}(\neg \varphi \vee \psi)$$

$$\text{Mod}_{\Sigma, D}(\varphi \leftrightarrow \psi) = \text{Mod}_{\Sigma, D}((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)).$$

Invitiamo il lettore a riflettere sul senso profondo della semantica appena data di connettivi e quantificatori. Il loro significato era chiaro fin dal principio. Cosa hanno aggiunto le equazioni di sopra, che oltretutto non sono sempre di comprensione immediata? Una prima risposta del lettore potrebbe essere: "Dire in modo complicato quanto si diceva in modo semplice". La risposta è in un certo senso ragionevole, ma non dice tutto, ovvero non coglie lo spirito del discorso. Il senso riposto delle equazioni semantiche permea tutto il progetto della semantica tarskiana, anche se nelle formulazioni correnti spesso sfugge per un eccesso di semplificazione: *ridurre alla teoria degli insiemi il significato del linguaggio logico predicativo*. Si era già capito negli anni Trenta che tutta la matematica si poteva esprimere entro teorie predicative (era lo spirito delle ricerche di Frege, Peano e Hilbert); il progetto di Tarski era quindi rivolto a portare nel "paradiso di Cantor" lo stesso linguaggio della matematica dimostrando l'universalità espressiva della teoria degli insiemi.

Semantica mediante assegnamenti alle variabili

Diciamo *assegnamento* una funzione ρ da un insieme V di variabili a un dominio D . Dato un assegnamento ρ , indichiamo con $\rho_{x=a}$ l'assegnamento che coincide con ρ su tutte le variabili tranne che su x , ove assume il valore a . Definiamo come segue l'interpretazione $(t)_{\rho}^{\mathcal{M}}$ dei termini di $T_{\Sigma}(V)$ in D :

$$(x)_{\rho}^{\mathcal{M}} = \rho(x)$$

$$(c)_{\rho}^{\mathcal{M}} = c^{\mathcal{M}}$$

$$(f(t_1, \dots, t_k))_{\rho}^{\mathcal{M}} = f^{\mathcal{M}}((t_1)_{\rho}^{\mathcal{M}}, \dots, (t_k)_{\rho}^{\mathcal{M}}).$$

A questo punto definiamo la semantica di una formula atomica in un dato assegnamento ponendo:

$$\mathcal{M} \models P(t_1, \dots, t_k)_{\rho} \Leftrightarrow ((t_1)_{\rho}^{\mathcal{M}}, \dots, (t_k)_{\rho}^{\mathcal{M}}) \in P^{\mathcal{M}}$$

utilizzando le tavole di verità tale metodo si estende a tutte le formule composte con connettivi. La semantica dei quantificatori si definisce ponendo:

$$\mathcal{M} \models (\forall x \varphi(x))_\rho \Leftrightarrow \{a \in D \mid \mathcal{M} \models \varphi(x)_{\rho_{x=a}}\} = D$$

$$\mathcal{M} \models (\exists x \varphi(x))_\rho \Leftrightarrow \{a \in D \mid \mathcal{M} \models \varphi(x)_{\rho_{x=a}}\} \neq \emptyset.$$

In tale metodo la semantica di una formula dipende dall'assegnamento con cui questa viene considerata. Una formula che vale rispetto ad ogni possibile assegnamento si dice valida nel modello.

Semantica generale delle proposizioni

Questo metodo si pone a un livello più generale. Fissiamo un insieme Γ di assegnamenti (funzioni di *variabili* in *valori*). Una proposizione, relativa a Γ , è una funzione da Γ in valori di verità $\{0, 1\}$, ovvero una proprietà definita su Γ . La semantica di una formula predicativa atomica, definita con il metodo precedente, è una proposizione nel senso appena detto. A questo punto, diamo la semantica di connettivi e quantificatori sulle proposizioni considerate come proprietà di assegnamenti. Indichiamo con γ, δ delle proposizioni in tal senso, con $\bar{v}$ il valore di verità complementare a v , e con $\min, \max$ il minimo e massimo nell'insieme $\{0, 1\}$ dei valori di verità ($0 < 1$); poniamo quindi

$$(\llbracket \neg \rrbracket(\gamma))(\rho) = \overline{\gamma(\rho)}$$

$$(\gamma \llbracket \wedge \rrbracket \delta)(\rho) = \min\{\gamma(\rho), \delta(\rho)\}$$

$$(\gamma \llbracket \vee \rrbracket \delta)(\rho) = \max\{\gamma(\rho), \delta(\rho)\}$$

$$\llbracket \forall x \rrbracket_\rho(\gamma)(\rho) = \min\{\gamma(\rho_{x=a}) \mid a \in D\}$$

$$\llbracket \exists x \rrbracket_\rho(\gamma)(\rho) = \max\{\gamma(\rho_{x=a}) \mid a \in D\}.$$

Utilizzando tali equazioni, dalla semantica delle formule atomiche ottenuta secondo il metodo precedente si ottiene facilmente la semantica di ogni formula predicativa; ovviamente una formula vale in un modello se in tale modello il suo valore di verità, rispetto a un dato assegnamento, è 1.

2.3. Logica proposizionale

Un assegnamento di valori di verità ai simboli di una teoria proposizionale è un'interpretazione che più propriamente si dice una *valutazione booleana*. Data una formula proposizionale φ indichiamo con $\varphi(P)$ una formula proposizionale in cui occorre la formula P e in tal caso, se ψ è un'altra formula proposizionale, indichiamo con $\varphi(\psi)$ la formula ottenuta da $\varphi(P)$ sostituendo in essa tutte le occorrenze di P con la formula ψ . Dalla nozione di interpretazione seguono immediatamente le seguenti proposizioni.

Proposizione 2.2 (principio di sostituzione proposizionale)

$$\models \varphi(P) \Leftrightarrow \models \varphi(\psi).$$

Esercizio 2.5 *Dimostrare che ciascuna delle due formule di De Morgan:*

$$\neg(\varphi \wedge \psi) \Leftrightarrow (\neg \varphi \vee \neg \psi)$$

$$\neg(\varphi \vee \psi) \Leftrightarrow (\neg \varphi \wedge \neg \psi)$$

è conseguenza dell'altra tramite il principio di sostituzione.

Proposizione 2.3 (principio di congruenza proposizionale)

$$\models \psi \Leftrightarrow \chi \Leftrightarrow \models \varphi(\psi) \Leftrightarrow \varphi(\chi).$$

Data una formula proposizionale φ in cui occorrono solo i connettivi $\wedge$, $\vee$, $\neg$ indichiamo con φ^* la formula duale ottenuta rimpiazzando in essa tutte le occorrenze di $\wedge$ con $\vee$ e viceversa. Indichiamo inoltre con $\varphi(\neg)$ la formula proposizionale ottenuta da φ rimpiazzando ogni atomica che vi occorre con la sua negazione (si definiscano per induzione φ^* e $\varphi(\neg)$). Si ha la seguente proposizione.

Proposizione 2.4 (principio di dualità proposizionale)

$$\models \varphi^* \Leftrightarrow \neg \varphi(\neg).$$

Dimostrazione (per induzione)

1. $\varphi = \psi \vee \chi \Rightarrow \varphi^* = \psi^* \wedge \chi^* \Leftrightarrow \neg \psi(\neg) \wedge \neg \chi(\neg) \Leftrightarrow \neg(\psi(\neg) \vee \chi(\neg)) = \neg \varphi(\neg)$
2. $\varphi = \psi \wedge \chi \Rightarrow \varphi^* = \psi^* \vee \chi^* \Leftrightarrow \neg \psi(\neg) \vee \neg \chi(\neg) \Leftrightarrow \neg(\psi(\neg) \wedge \chi(\neg)) = \neg \varphi(\neg)$
3. $\varphi = \neg \psi \Rightarrow \varphi^* = \neg \psi^* \Leftrightarrow \neg \neg \psi(\neg) = \neg \varphi(\neg)$ ■

Definizione 2.6 *Due formule proposizionali si dicono equivalenti se hanno le stesse variabili proposizionali e se, in corrispondenza degli stessi valori delle loro variabili, assumono gli stessi valori di verità.*

Le proposizioni (“metaproposizioni”, in quanto parlano di proposizioni!) che seguono sono una conseguenza diretta della precedente definizione, della definizione di tautologia e della semantica dei connettivi $\leftrightarrow$, $\rightarrow$.

Proposizione 2.5 (principio di equivalenza proposizionale) *Due formule proposizionali φ , ψ sono equivalenti sse $\varphi \leftrightarrow \psi$ è una tautologia.*

Proposizione 2.6 (principio di deduzione proposizionale) *Date due formule proposizionali $\varphi \models \psi$ sse $\varphi \rightarrow \psi$ è una tautologia.*

Ricordiamo che un letterale è una formula atomica o la negazione di una formula atomica.

Definizione 2.7 *Una forma normale disgiuntiva è una formula proposizionale costituita dalla disgiunzione di congiunzioni di letterali. Una forma normale congiuntiva è invece la congiunzione di disgiunzioni di letterali.*

Proposizione 2.7 (forme disgiuntive e congiuntive) *Ogni formula proposizionale è equivalente a una forma normale disgiuntiva.*

Dimostrazione Consideriamo la tavola proposizionale di una formula φ e in essa selezioniamo tutte le righe in corrispondenza delle quali la formula è vera. Supponiamo siano le prime m . Dato un simbolo proposizionale P , è comodo, per quanto scriveremo fra poco, scrivere 1 P per P e 0 P per $\neg P$. Siano $P_1, \dots, P_k$ le formule atomiche di φ e siano $x_{i,1}, \dots, x_{i,k}$ per $i \in \{1, \dots, m\}$ i valori delle m righe della tavola di verità in corrispondenza ai quali φ risulta vera, allora si ha

$$\varphi \leftrightarrow (x_{1,1}P_1 \wedge \dots \wedge x_{1,k}P_k) \vee \dots \vee (x_{m,1}P_1 \wedge \dots \wedge x_{m,k}P_k).$$

Analogamente si dimostra che ogni formula proposizionale è equivalente a una forma normale congiuntiva (basta scambiare i ruoli dei due connettivi $\wedge, \vee$ e di 0, 1). ■

Un interessante risultato della logica proposizionale mostra che la nozione di tautologia può essere determinata con un calcolo algebrico simile a quello aritmetico. A tal fine introduciamo la caratterizzazione assiomatica delle algebre di Boole. Gli *assiomi dell'algebra di Boole* sono definiti in una qualsiasi algebra con due operazioni binarie $\wedge, \vee$, un'operazione unaria $\neg$ e due costanti 0, 1:

- Associatività di $\wedge$.
- Associatività di $\vee$.
- Commutatività di $\wedge$.
- Commutatività di $\vee$.
- Distributività di $\wedge$ rispetto a $\vee$.
- Distributività di $\vee$ rispetto a $\wedge$.
- Assorbimento di $\vee$ rispetto a $\wedge$.

- Assorbimento di $\wedge$ rispetto a $\vee$.
- Indifferenza: $\varphi \wedge 0 = 0$, $\varphi \vee 1 = 1$.

Definizione 2.8 Due formule proposizionali φ , ψ sono equivalenti secondo il calcolo di Boole se, partendo dalla formula φ , in cui i connettivi $\rightarrow$, $\leftrightarrow$ sono espressi in termini di $\wedge$, $\vee$, $\neg$, vi è una successione finita di rimpiazzamenti, di sottoformule con formule uguali secondo gli assiomi di Boole, che termina con la formula ψ .

Esempio 2.7

$$\varphi \rightarrow (\psi \rightarrow \theta) = \neg \varphi \vee (\neg \psi \vee \theta) = (\neg \varphi \vee \neg \psi) \vee \theta \stackrel{*}{=} \neg(\varphi \wedge \psi) \vee \theta = \varphi \wedge \psi \rightarrow \theta.$$

Esercizio 2.6 Si verifichi che gli assiomi di Boole sono soddisfatti dalla classe di tutti i sottoinsiemi di un prefissato insieme detto universo, laddove 1 si interpreti come l'universo, 0 come l'insieme vuoto, $\wedge$ come intersezione, $\vee$ come unione e $\neg$ come complementazione.

Un notevole risultato, noto come teorema di Stone, afferma che ogni algebra di Boole è sempre isomorfa a qualche algebra di insiemi, ovvero una opportuna classe di insiemi con le operazioni di unione, intersezione, complementazione, insieme vuoto e insieme universale (non è detto che la classe sia costituita da *tutti* i sottoinsiemi di un insieme). Il seguente teorema dimostra che il calcolo di Boole è intrinsecamente connesso alla nozione di tautologia stabilita secondo le tavole di verità dei connettivi.

Proposizione 2.8 (completezza proposizionale del calcolo di Boole) *Nel calcolo sulle formule proposizionali, determinato dagli assiomi booleani, si deriva $\varphi = \psi$ sse $\models \varphi \leftrightarrow \psi$, ovvero se le formule φ , ψ sono equivalenti e si deriva $\varphi = 1$ sse $\models \varphi$, ovvero sse φ è una tautologia.*

Dimostrazione (cenno) Basta osservare che gli assiomi di Boole sono sufficienti a trasformare ogni formula proposizionale nella sua forma normale disgiuntiva e che tali forme normali individuano completamente la tavola di verità della formula. ■

Esempio 2.8 Si definisca la relazione binaria che vale tra due formule proposizionali se queste sono equivalenti (secondo il calcolo di Boole o le tavole di verità). Tale relazione è un'equivalenza. Sul suo insieme quoziente si definiscano due operazioni binarie e un'operazione unaria rispetto alla quale siano verificati gli assiomi di algebra di Boole. L'algebra ottenuta dicesi *algebra di Lindenbaum*.

I connettivi considerati si dicono *verofunzionali* in quanto, in base alla semantica data, il valore di verità delle proposizioni con essi composte è determinato dal valore di verità delle proposizioni componenti. La disgiunzione considerata si dice inclusiva poiché non esclude che entrambe le formule disgiunte siano vere. Essa presenta una certa discrepanza con l'idea di proposizione del linguaggio ordinario: infatti, una proposizione del tipo

$(2 = 3) \vee \text{ogni numero ha un successore}$

è vera dal nostro punto di vista, laddove da un punto di vista intuitivo sembra poco sensata, poiché mette insieme due fatti che non hanno alcuna relazione. Tale discrepanza appare in maniera ancora più evidente nella definizione dell'implicazione. Infatti, risulta che un'implicazione $\varphi \rightarrow \psi$ è vera non appena l'antecedente φ risulti falso o il conseguente ψ risulti vero, e ciò è completamente in contrasto con l'intuizione sottostante alla nozione intuitiva di implicazione: infatti è del tutto controintuitivo accettare la sensatezza di proposizioni quali "se $4 = 5$, allora vi sono infiniti primi". L'implicazione verofunzionale è una caratterizzazione specifica e limitata di implicazione e individua un requisito minimale di tutte le forme implicative: nessuna implicazione può essere valida se l'antecedente è vero e il conseguente falso.

L'implicazione verofunzionale $\rightarrow$ è diversa dall'implicazione delle dimostrazioni matematiche. Si ha che se $P \Rightarrow Q$, allora $P \rightarrow Q$ è vera; però non sempre, quando vale $P \rightarrow Q$, l'asserto $P \Rightarrow Q$ esprime un'implicazione matematica ragionevole. Consideriamo un esempio. Una delle due proposizioni $P \rightarrow Q$, $Q \rightarrow P$ è vera per qualsiasi coppia di proposizioni P , Q . Infatti si hanno due casi: 1) P è vera, oppure 2) $\neg P$ è vera. Nel primo caso è vera $Q \rightarrow P$, nel secondo è vera $P \rightarrow Q$. Tuttavia non è assolutamente detto che si possa stabilire una delle due implicazioni matematiche $P \Rightarrow Q$ o $Q \Rightarrow P$. Per esempio, non è detto che assumendo come sua la proposizione "17 è un numero primo" si riesca a derivare la proposizione "esiste un cubo che è somma di due cubi", oppure, viceversa, che la primalità del 17 possa essere derivata dall'esistenza di due cubi la cui somma è un cubo.

A proposito dei comportamenti controintuitivi dell'implicazione verofunzionale nei confronti del "se allora" matematico si è parlato talvolta di *paradossi dell'implicazione* e si è distinta l'implicazione verofunzionale, detta anche *materiale*, dalla relazione di conseguenza $\models$, specificata in termini di modelli e detta anche *formale*.

La differenza tra *implicazione materiale* e *implicazione formale* è strettamente legata alla fondamentale differenza tra *vero* e *dimostrabile*.

I due concetti non si equivalgono, ed è stato un merito fondamentale della logica matematica avere chiarito i loro rapporti reciproci. Data una proposizione e la sua negazione, almeno una delle due deve essere vera; tut-

tavia non è detto che almeno una delle due sia dimostrabile. Come vedremo, vi sono teorie in cui, per qualche proposizione P , né P né $\neg P$ sono dimostrabili nella teoria, benché ovviamente, in base al classico principio del *tertium non datur*, una delle due sia sicuramente vera in ogni interpretazione. La *logica matematica intuizionista* originata dai lavori di Brouwer (1881-1966), a differenza della logica classica, ha elaborato una nozione di proposizione secondo cui la validità si identifica con la dimostrabilità in un opportuno sistema deduttivo.

Nonostante tutto, il connettivo $\rightarrow$ è una caratterizzazione formale per cui valgono varie caratteristiche essenziali del “se allora” matematico. Per esempio, in base alla sua semantica verofunzionale, se, in una data interpretazione, sia una proposizione P che una proposizione $P \rightarrow Q$ risultano vere, allora si può asserire anche la verità di Q . Così pure, molte fondamentali regole logiche dell’implicazione individuate dai logici greci e medievali seguono facilmente dalla definizione verofunzionale del connettivo logico $\rightarrow$. Utilizzando la nozione di validità in un modello si stabilisce facilmente che

$$(\mathcal{M} \models \varphi \rightarrow \psi) \Leftrightarrow (\mathcal{M} \models \varphi \Rightarrow \mathcal{M} \models \psi).$$

Diciamo *funzione booleana* di n variabili una funzione da $\{0, 1\}^n$ in $\{0, 1\}$. Poiché la cardinalità di $\{0, 1\}^n$ è 2^n , il numero di tali funzioni è 2^{2^n} . Vi sono quindi 16 connettivi binari.

Esercizio 2.7 *Si enumerino tutte le funzioni booleane binarie.*

Suggerimento Si considerino oltre ai quattro connettivi noti il connettivo di implicazione inversa, le due proiezioni, i connettivi costanti (sempre 0, sempre 1) e le complementazioni delle funzioni considerate.

Esercizio 2.8 *Un insieme di funzioni booleane è una base funzionalmente completa se ogni funzione booleana, di un qualsiasi numero di variabili, può essere espressa componendo le funzioni di tale insieme. I teoremi precedenti implicano che i connettivi $\wedge, \vee, \neg$ determinano una base funzionalmente completa. Si esibiscano altre basi funzionalmente complete.*

Esercizio 2.9 *Si dimostri che il connettivo binario che produce il vero solo se i suoi argomenti sono entrambi falsi, da solo costituisce una base funzionalmente completa. Si dimostri che il connettivo binario che produce il falso solo se i suoi argomenti sono entrambi falsi, da solo costituisce una base funzionalmente completa.*

Esercizio 2.10 *Si consideri un circuito composto da fili conduttori, commutatori, connessioni in parallelo e in serie e dei punti terminali su cui agiscono variabili booleane. In un terminale si ha passaggio di corrente se*

la variabile che vi agisce vale 1. Un commutatore scambia il valore di una variabile booleana. In una connessione parallela si ha passaggio di corrente se almeno in uno dei due circuiti componenti si ha passaggio, mentre in una connessione in serie si ha passaggio di corrente se in entrambi i circuiti componenti si ha passaggio. Si rappresenti un circuito indicando i commutatori con $\neg$, le connessioni in parallelo e in serie come le usuali connessioni elettriche di conduttori e le variabili booleane che agiscono nel circuito con delle lettere poste nei punti terminali. Data una formula costruita con i connettivi $\neg$, $\wedge$, $\vee$, si disegni un circuito in cui, assegnando dei valori alle variabili, si ha passaggio di corrente sse la formula proposizionale corrispondente è vera.

Concludiamo l'analisi della logica proposizionale con un teorema fondamentale che sarà generalizzato in seguito a tutta la logica predicativa e che costituisce l'essenza dei più importanti risultati della logica predicativa. Spieghiamo prima in modo informale l'enunciato del teorema. Supponiamo di avere infinite proposizioni Γ , ma supponiamo contemporaneamente che ogniquale volta ne selezioniamo un numero finito riusciamo a trovare un modello per le proposizioni selezionate. Siano $\Gamma_1, \Gamma_2, \Gamma_3, \dots$ la lista di tutti i sottoinsiemi finiti di Γ (un insieme numerabile se tale è Γ). Supponiamo ancora che per ciascun sottoinsieme considerato riusciamo a trovare un modello e siano $M_1, M_2, M_3, \dots$ tali modelli che diremo parziali, in quanto soddisfano solo parti di Γ (per di più finite). Essendo tali insiemi diversi tra loro, in genere i relativi modelli possono essere diversi. La compattezza della logica proposizionale afferma che l'esistenza di tali modelli garantisce l'esistenza di un modello unico che soddisfa tutte le formule di Γ (e che potrebbe differire da ciascuno dei modelli parziali).

Il seguente diagramma cerca di visualizzare il fenomeno (fig. 2.1):

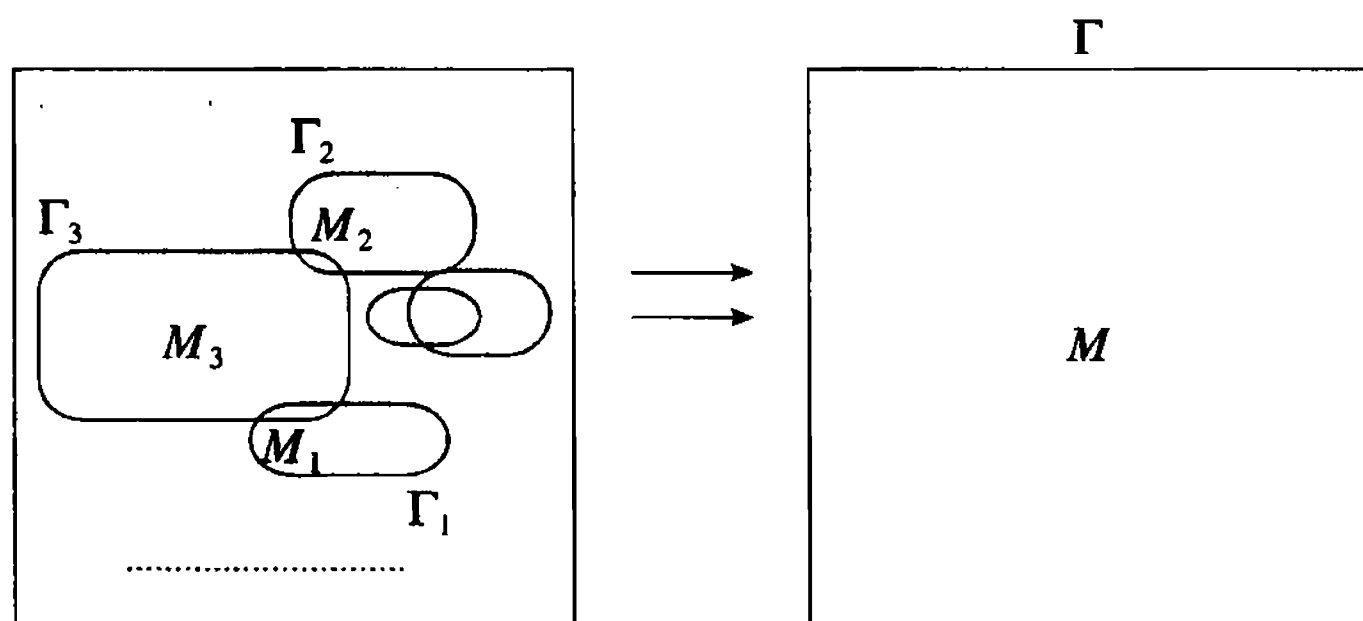


Figura 2.1

Compattezza della logica predicativa.

Proposizione 2.9 (compattezza proposizionale) *Un insieme numerabile Φ di formule proposizionali è soddisfacibile sse lo è ogni suo sottoinsieme finito.*

Dimostrazione Se Φ è soddisfacibile, allora ovviamente ogni suo sottoinsieme è tale. Quindi rimane da dimostrare solo l'implicazione inversa. Assumiamo allora che ogni sottoinsieme finito di Φ sia soddisfacibile. Supponiamo dapprima che in Φ occorran solo un insieme finito di simboli proposizionali. In tal caso le possibili valutazioni booleane, che assegnano valori di verità ai simboli proposizionali, sono un numero finito $\{f_1, \dots, f_k\}$. Affermiamo che una di esse deve necessariamente soddisfare Φ . Infatti, se così non fosse, dovrebbe esistere per ogni $1 \leq i \leq k$ almeno una formula ψ_i che non è soddisfatta da f_i ; ma allora $\{\psi_1, \dots, \psi_k\}$ sarebbe un sottoinsieme finito insoddisfacibile, e ciò contraddice le ipotesi.

Consideriamo ora il caso in cui anche i simboli proposizionali di Φ siano un insieme numerabile $P_1, P_2, \dots, P_n, \dots$. Sia $\varphi_1, \varphi_2, \dots, \varphi_n, \dots$ una numerazione di Φ . Costruiamo un albero la cui radice è etichettata con la valutazione vuota; quindi poniamo al primo livello due nodi: uno etichettato con l'assegnamento di valore di verità $P_1 = 1$ (P_1 vero) e l'altro in cui $P_1 = 0$ (P_1 falso). Se tali assegnamenti rendono vera φ_1 li lasciamo e generiamo per entrambi i nodi due figli etichettati con le due possibili valutazioni di P_2 . Se invece uno di tali assegnamenti rende falsa φ_1 , cancelliamo il nodo relativo. In generale, giunti al livello n , consideriamo tutti i nodi presenti a quel livello e per ciascuno di essi generiamo due figli etichettati con $P_{n+1} = 1, P_{n+1} = 0$. Se uno di tali assegnamenti, insieme a quelli del ramo in cui si trova, soddisfa $\varphi_1, \varphi_2, \dots, \varphi_n, \varphi_{n+1}$, allora manteniamo il nodo relativo; altrimenti lo cancelliamo. In base all'ipotesi che tutti i sottoinsiemi finiti di Φ sono soddisfacibili, sappiamo che il processo di generazione di tale albero può proseguire all'infinito. Quindi l'albero è un albero finitario infinito. A questo punto, il lemma di König ci dice che esso ha un ramo infinito. Tale ramo è evidentemente una valutazione booleana dei simboli atomici di Φ che soddisfa tutte le formule di Φ . ■

2.4. Tableau analitici

Una delle tematiche logiche fondamentali consiste nell'individuare forme di ragionamento logicamente valide, la cui validità cioè non dipenda dal contenuto delle singole proposizioni con cui il ragionamento è costruito, ma dallo schema formale sottostante. Mostriamo nel seguito un metodo, detto dei *tableau analitici*, che consente di determinare algebricamente tutte le verità logiche della logica predicativa. Gli alberi che seguono individuano delle re-

gole, il cui funzionamento è spiegato più avanti. La lettura intuitiva di queste regole è la seguente: se in un modello vale la formula che si trova alla radice, allora in tale modello devono valere tutte le formule associate ai nodi di almeno un ramo, o del ramo, se l'albero ne ha uno solo. Il lettore può verificare, caso per caso, che una tale situazione si verifica, in base alla semantica dei connettivi e dei quantificatori, per tutti gli alberi che seguono (vedi fig. 2.2).

Notiamo che per ogni connettivo binario e per ogni quantificatore vi sono due alberi: uno in cui l'operatore logico è quello esterno e uno in cui adesso è premessa una negazione. Si hanno pertanto 12 regole che possiamo sinteticamente siglare come nella tabella 2.2:

Tabella 2.2 Regole tableau

$T_{\wedge}$	$T_{\neg\wedge}$
$T_{\vee}$	$T_{\neg\vee}$
$T_{\rightarrow}$	$T_{\neg\rightarrow}$
$T_{\leftrightarrow}$	$T_{\neg\leftrightarrow}$
$T_{\forall}$	$T_{\neg\forall}$
$T_{\exists}$	$T_{\neg\exists}$

Data una teoria Φ , un Φ -tableau è un albero i cui nodi sono etichettati con formule o con il simbolo speciale $\perp$, costruito nel modo seguente (data una formula $\chi(t)$ in cui occorre il termine t , si indica con $\chi(t')$ la formula in cui qualche occorrenza di t è rimpiazzata da t').

All'inizio si produce un nodo e lo si etichetta con una formula di Φ . Ad ogni passo ci si posiziona su una foglia f dell'albero e si prosegue con una delle seguenti alternative:

1. *Regola di introduzione*: si genera un figlio di f etichettandolo con una formula di Φ .
2. *Regola di ricopiatura*: si genera un figlio di f etichettandolo con una formula che è etichetta di un antenato di f .
3. *Regole tableau*: si applica all'etichetta φ di f una regola tableau, ovvero, se φ coincide con l'etichetta della radice di una regola, allora si rimpiazza f con l'albero di tale regola.
4. *Regola di doppia negazione*: se f è etichettata con $\neg\neg\psi$, si genera un figlio di f con etichetta ψ .
5. *Regola di congruenza*: se f è etichettata con la formula $t_1 = t_2$ e nel ramo di f vi è un nodo etichettato con una formula $\chi(t_i)$, $i \in \{1, 2\}$, si genera un figlio di f con un'etichetta del tipo $\chi(t_j)$, $j \in \{1, 2\}$, $j \neq i$.
6. *Regola di chiusura*: se f è etichettata con una formula ψ e la negata $\neg\psi$ è etichetta di un antenato di f , si genera un figlio di f con etichetta $\perp$.

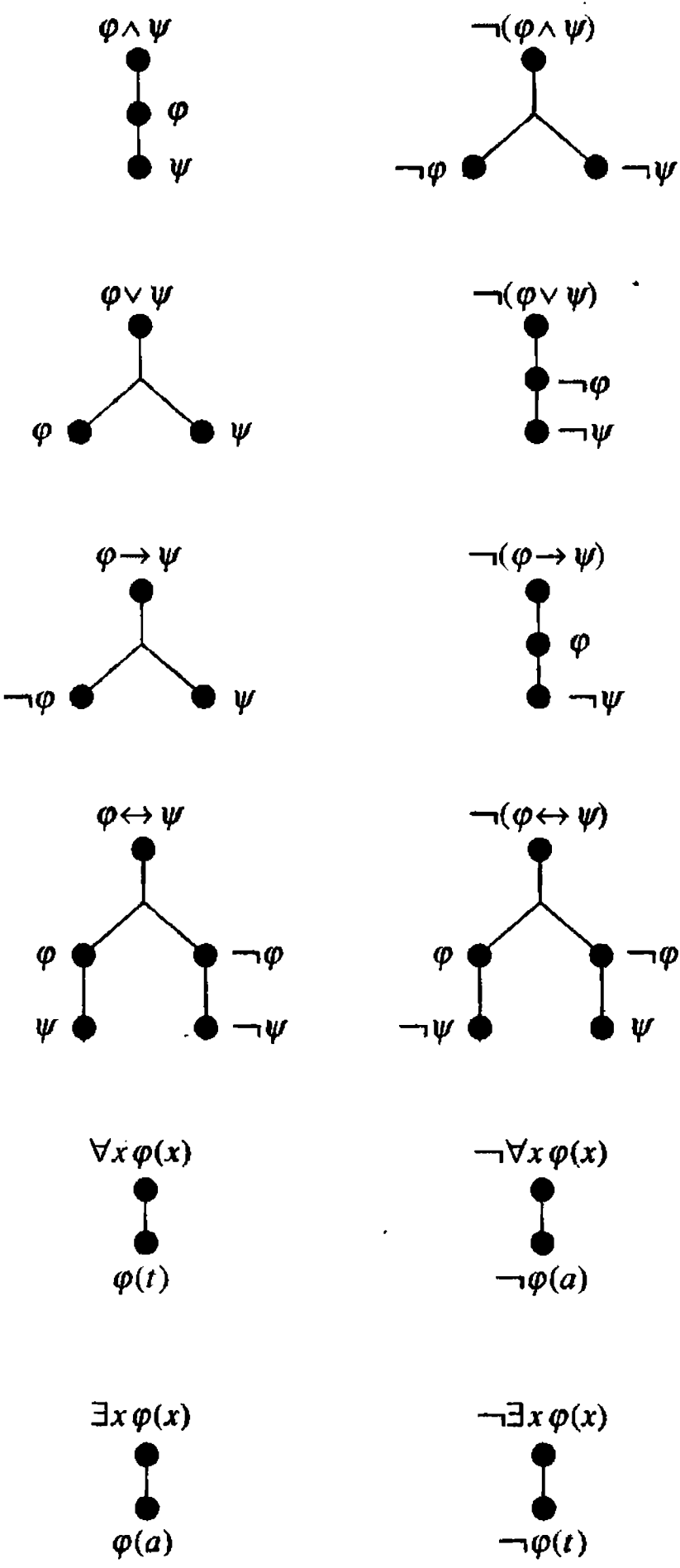


Figura 2.2
Alberi tableau.

Nei tableau, t, t_1, t_2 indicano termini chiusi qualsiasi, mentre a indica una costante individuale univocamente determinata dalla formula in cui viene sostituita (al posto della variabile la cui quantificazione viene rimossa).
Tale costante dicesi *testimone* della formula o anche *costante di Henkin* della formula.

Definizione 2.9 *Un tableau si dice chiuso se in esso tutte le foglie sono etichettate con $\perp$.*

Il fatto che nelle regole di tipo $\exists$ e $\neg\forall$ la costante introdotta dipenda univocamente dalla formula, implica che a tali formule una regola si può applicare di fatto una sola volta, nel senso che ogni altra applicazione produrrebbe sempre lo stesso risultato. Invece le regole $\forall$ e $\neg\exists$ possono essere applicate varie volte producendo risultati diversi.

Nella pratica, si può evitare di ricopiare una formula già apparsa in un ramo, purché si capisca quando l'applicazione di una regola si riferisce a tale formula.

La deducibilità secondo il metodo dei tableau può essere resa più efficiente aggiungendo le seguenti regole che sono ovviamente corrette. Ad ogni nodo può essere posta come etichetta: 1) una tautologia; 2) una formula che è conseguenza logica della teoria considerata; 3) la formula ψ se le formule φ e $\varphi \rightarrow \psi$ sono già nel ramo.

Definizione 2.10 *Si dice che da una teoria Φ si deduce, secondo il metodo dei tableau, la formula φ e si pone (omettendo l'indice T , quando è arguibile)*

$$\Phi \vdash_T \varphi,$$

quando esiste un $\Phi \cup \{\neg \varphi\}$ -tableau chiuso.

Esempio 2.9 Dimostriamo che

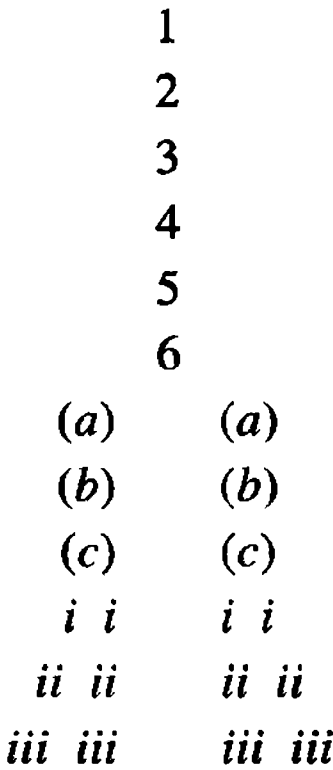
$$\vdash (P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P).$$

Rappresentiamo l'albero del relativo tableau in maniera tabellare, secondo le notazioni originali a cui si deve il nome di tale metodo: una regola che genera due figli corrisponde al suddividersi della tabella in due sottotabelle (*tavole analitiche* sarebbe un nome altrettanto adeguato).

Tabella 2.3 Esempio di tableau

$\neg((P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P))$ (introduzione)	
$(P \rightarrow Q)$	
$\neg(\neg Q \rightarrow \neg P)$	
$\neg Q$	
$\neg\neg P$	
P	
$P \rightarrow Q$ (ricopiatura)	
$\neg P$	Q
P (ricopiatura)	$\neg Q$ (ricopiatura)
$\perp$	$\perp$

Nel seguito indicheremo i rami di un tableau tramite indentazione delle formule, etichettando i nodi con numeri o lettere. Per esempio, l'albero associato alla deduzione del prossimo esempio è il seguente:



Esempio 2.10

- $\vdash P \wedge (Q \vee R) \rightarrow (P \wedge Q) \vee (P \wedge R).$
1. $\neg(P \wedge (Q \vee R) \rightarrow (P \wedge Q) \vee (P \wedge R))$

(introduzione)
2. $P \wedge (Q \vee R)$
3. $\neg((P \wedge Q) \vee (P \wedge R))$
4. $P \wedge (Q \vee R)$

(ricopiatura)
5. P
6. $Q \vee R$

(a) Q

(b) $\neg((P \wedge Q) \vee (P \wedge R))$

(ricopiatura)

(c) $\neg(P \wedge Q)$

i. $\neg P$

ii. P

(ricopiatura)

iii. $\bot$

i. $\neg Q$

ii. Q

(ricopiatura)

iii. $\bot$

- (a) R
 (b) $\neg((P \wedge Q) \vee (P \wedge R))$ (ricopiatura)
 (c) $\neg(P \wedge R)$
 i. $\neg P$
 ii. P (ricopiatura)
 iii. $\perp$
 i. $\neg R$
 ii. R (ricopiatura)
 iii. $\perp$

Negli esempi che seguono sottintenderemo le regole di ricopiatura.

Esempio 2.11 Dimostriamo con i tableau che dalla teoria

$$\forall xyz(Ixz \wedge Iyz \rightarrow Vxy)$$

$$\forall x Ixx$$

si deduce

$$\forall xy(Ixy \rightarrow Vxy).$$

1. $\neg \forall xy(Ixy \rightarrow Vxy)$
2. $\neg(Iab \rightarrow Vab)$
3. Iab
4. $\neg Vab$
5. $\forall xyz(Ixz \wedge Iyz \rightarrow Vxy)$ (introduzione)
6. $Iab \wedge Ibb \rightarrow Vab$
 - (a) $\neg(Iab \wedge Ibb)$
 - i.* $\neg Iab$
 - ii.* $\perp$
 - i.* $\neg Ibb$
 - ii.* $\forall x Ixx$ (introduzione)
 - iii.* Ibb
 - iv.* $\perp$

$$(a) Vab$$

$$(b) \perp$$

Esempio 2.12

$$\vdash (\exists x \varphi(x) \rightarrow \psi) \leftrightarrow \forall x (\varphi(x) \rightarrow \psi)$$

in cui in ψ la variabile x non occorre libera.

$$1. \neg((\exists x \varphi(x) \rightarrow \psi) \leftrightarrow \forall x (\varphi(x) \rightarrow \psi))$$

$$(a) \exists x \varphi(x) \rightarrow \psi$$

$$(b) \neg \forall x (\varphi(x) \rightarrow \psi)$$

$$(c) \neg(\varphi(a) \rightarrow \psi)$$

$$(d) \varphi(a)$$

$$(e) \neg \psi$$

$$i. \neg \exists x \varphi(x)$$

$$ii. \neg \varphi(a)$$

$$iii. \perp$$

$$i. \psi$$

$$ii. \perp$$

$$(a) \neg(\exists x \varphi(x) \rightarrow \psi)$$

$$(b) \forall x (\varphi(x) \rightarrow \psi)$$

$$(c) \exists x \varphi(x)$$

$$(d) \neg \psi$$

$$(e) \varphi(a)$$

$$(f) \varphi(a) \rightarrow \psi$$

$$i. \neg \varphi(a)$$

$$ii. \perp$$

$$i. \psi$$

$$ii. \perp$$

Esempio 2.13

$$\forall xy(Pxy \rightarrow Qx), \forall xy(Pxy \rightarrow Pyx) \vdash \forall xy(Pxy \rightarrow Qx \wedge Qy).$$

$$1. \neg \forall xy(Pxy \rightarrow Qx \wedge Qy)$$

$$2. \neg(Pab \rightarrow Qa \wedge Qb)$$

$$3. Pab$$

4. $\neg(Qa \wedge Qb)$

(a) $\neg Qa$

(b) $\forall xy(Pxy \rightarrow Qx)$ (introduzione)

(c) $Pab \rightarrow Qa$

i. $\neg Pab$

ii. $\perp$

i. Qa

ii. $\perp$

(a) $\neg Qb$

(b) $\forall xy(Pxy \rightarrow Pyx)$ (introduzione)

(c) $Pab \rightarrow Pba$

i. $\neg Pab$

ii. $\perp$

i. Pba

ii. $\neg \forall xy(Pxy \rightarrow Qx \wedge Qy)$ (introduzione)

iii. $Pba \rightarrow Qb \wedge Qa$

A. $\neg Pba$

B. $\perp$

A. $Qb \wedge Qa$

B. Qb

C. $\perp$

Esempio 2.14 Paradosso del cappello: “Esiste qualcuno tale che se lui è C (con il cappello), allora tutti sono C ”:

$\vdash \exists x(Cx \rightarrow \forall yCy).$

1. $\neg \exists x(Cx \rightarrow \forall yCy)$ (introduzione)

2. $\neg(Ca \rightarrow \forall yCy)$

3. Ca

4. $\neg \forall yCy$

5. $\neg Cb$

6. $\neg(Cb \rightarrow \forall yCy)$

7. Cb

8. $\neg \forall yCy$

9. $\perp$

Esempio 2.15

$$\forall x(Px \rightarrow Qx \vee Rx), \neg \forall x Qx \vdash \exists x(Px \rightarrow Rx).$$

1. $\neg \forall x Qx$ (introduzione)
2. $\neg Qa$
3. $\neg \exists x(Px \rightarrow Rx)$ (introduzione)
4. $\neg(Pa \rightarrow Ra)$
5. Pa
6. $\neg Ra$
7. $\forall x(Px \rightarrow Qx \vee Rx)$ (introduzione)
8. $(Pa \rightarrow Qa \vee Ra)$
 - (a) $\neg Pa$
 - (b) $\perp$
 - (a) $Qa \vee Ra$
 - i. Qa
 - ii. $\perp$
 - i. Ra
 - ii. $\perp$

Esercizio 2.11 Si dia un esempio di tableau infinito.

Suggerimento Si consideri un $\{\forall x \exists y P(x, y)\}$ -tableau.

Notiamo che un tableau *concluso*, ovvero in cui non si può procedere oltre, non è necessariamente chiuso. La proposizione seguente mostra che la chiusura di un Φ -tableau implica l'insoddisfacibilità di Φ .

Proposizione 2.10 *Se vi è un Φ -tableau chiuso, allora Φ è insoddisfacibile.*

Dimostrazione In ogni modello in cui vale la formula che etichetta la radice di una regola, devono valere tutte le formule di almeno un ramo della regola. Se tutti i rami di un tableau hanno per foglia $\perp$, allora in ogni modello in cui valgono le formule di Φ si deve valere una formula e la sua negata, ma un tale modello non può esistere e quindi Φ è insoddisfacibile. ■

Proposizione 2.11 (correttezza del metodo deduttivo dei tableau)

$$\Phi \vdash_T \varphi \Rightarrow \Phi \models \varphi.$$

Dimostrazione Dalla definizione di $\vdash_T$, e in base alla proposizione precedente, se $\Phi \vdash_T \varphi$, allora $\Phi \cup \{\neg\varphi\}$ è insoddisfacibile, quindi $\Phi \models \varphi$. ■

Dimostreremo tra poco che il metodo dei tableau permette sempre di scoprire quando $\Phi \models \varphi$; tuttavia, finché un tableau non si chiude nessuna delle due possibilità (chiusura/non chiusura) può essere determinata. Può darsi che dopo pochi passi si giunga alla chiusura, ma può darsi che tutti i tentativi di chiudere il tableau risultino vani, e non si riesca nemmeno a stabilire se la chiusura sia impossibile. Un tale fenomeno è dovuto a un limite intrinseco della logica predicativa che sarà dimostrato in seguito, per cui la validità logica è, in generale, *semidecidibile*, ma non *decidibile*. Infatti, in generale, alla domanda: “Il tableau T si chiude?” si può rispondere “sì” quando T si chiude, ma non si può rispondere “no” se T non si chiude. Ciò non esclude che in certi casi particolari una tale domanda possa ammettere una risposta definitiva, positiva o negativa. L’esercizio che segue fornisce un esempio in proposito.

Esercizio 2.12 *Si dimostri che un tableau relativo a una formula proposizionale è sempre finito e quindi si può sempre decidere se è chiuso o meno.*

Esercizio 2.13 *Si dimostri il teorema di compattezza proposizionale come conseguenza dell’esercizio precedente e del lemma di König.*

A volte la non chiusura di un tableau suggerisce la definizione di un *contromodello*, ovvero un modello in cui una data proposizione non vale. Il seguente è un esempio in proposito. Si consideri la proposizione

$$(\forall xPx \rightarrow \forall xQx) \rightarrow \forall x(Px \rightarrow Qx).$$

Cerchiamo di provare che tale formula è logicamente valida.

Tabella 2.4 Tableau non chiuso

$\neg((\forall xPx \rightarrow \forall xQx) \rightarrow \forall x(Px \rightarrow Qx))$ (introduzione)	
$(\forall xPx \rightarrow \forall xQx)$	
$\neg(\forall x(Px \rightarrow Qx))$	
$\neg(Pa \rightarrow Qa)$	
Pa	
$\neg Qa$	
$(\forall xPx \rightarrow \forall xQx)$	
$\forall xPx$	$\neg(\forall xQx)$
Pb	$\neg Qb$

Il tableau non si chiude. Un contromodello, suggerito dalla non chiusura dell’albero precedente, ha come dominio $\{a, b\}$ e il seguente diagramma:

$\{Pa, Pb, \neg Qa, \neg Qb\}$. Infatti, si verifica subito che in tale modello l'antecedente dell'implicazione è vero e il conseguente è falso.

Esercizio 2.14 *Si considerino le proposizioni seguenti:*

1. $\forall x(Px \rightarrow Qx) \rightarrow (\forall xPx \rightarrow \forall xQx)$
2. $\exists x(Px \rightarrow Qx) \rightarrow (\exists xPx \rightarrow \exists xQx)$
3. $(\exists xPx \rightarrow \exists xQx) \rightarrow \exists x(Px \rightarrow Qx)$.

si dimostri, utilizzando i tableau, quale delle proposizioni precedenti è logicamente valida. A partire dai tableau che non si chiudono si costruiscano dei contromodelli per le proposizioni relative.

2.5. Completezza e compattezza

La prima proposizione di questa sezione costituisce il cuore di tutta la logica predicativa. Ne esistono varie dimostrazioni, qui ne presenteremo una secondo la linea di Beth e Hintikka. Cominciamo con una definizione.

Definizione 2.11 *Sia Σ una segnatura e D un insieme. Un insieme H di formule predicative di $F_{\Sigma, D}$ si dice insieme di Hintikka di dominio D se tale dominio D include tutte le costanti di Σ e inoltre valgono le seguenti condizioni:*

1. *non esiste alcuna formula φ che stia in H con la sua negata;*
2. *se $\varphi \wedge \psi \in H$, allora entrambe φ, ψ appartengono ad H ;*
3. *se $\neg(\varphi \vee \psi) \in H$, allora entrambe $\neg\varphi, \neg\psi$ appartengono ad H ;*
4. *se $\varphi \vee \psi \in H$, allora almeno una tra φ, ψ appartiene ad H ;*
5. *se $\neg(\varphi \wedge \psi) \in H$, allora almeno una tra $\neg\varphi, \neg\psi$ appartiene ad H ;*
6. *se $\exists x\varphi(x) \in H$, allora, per qualche $a \in D$, $\varphi(a) \in H$;*
7. *se $\neg\forall x\varphi(x) \in H$, allora, per qualche $a \in D$, $\neg\varphi(a) \in H$;*
8. *se $\forall x\varphi(x) \in H$, allora, per ogni $a \in D$, $\varphi(a) \in H$;*
9. *se $\neg\exists x\varphi(x) \in H$, allora, per ogni $a \in D$, $\neg\varphi(a) \in H$;*
10. *se $t_1 = t_2$, $\varphi(t_i) \in H$, $i \in \{1, 2\}$, allora ogni formula del tipo $\varphi(t_j) \in H$, con $j \in \{1, 2\}$, $j \neq i$.*

La proprietà fondamentale di un insieme di Hintikka su un dominio D è quella di avere sempre un modello.

Lemma 2.1 *Sia H un insieme di Hintikka di dominio D ; allora esiste un modello di H di dominio D .*

Dimostrazione Assumiamo dapprima che H sia una Σ -teoria ove non occorran né simboli di funzione né di uguaglianza.

Definiamo un Σ -modello di H di dominio D ove ogni costante è interpretata in se stessa e ogni simbolo di relazione n -aria P è interpretato nella relazione n -aria $\llbracket P \rrbracket$ tale che $\langle d_1, \dots, d_k \rangle \in \llbracket P \rrbracket$ se la formula atomica $P(d_1, \dots, d_k)$ si trova in H .

Verifichiamo che in tale modello sono vere tutte le proposizioni di H . Procediamo per induzione sul numero delle occorrenze di $\wedge, \vee, \exists, \rightarrow, \leftrightarrow$.

Una formula atomica $\varphi \in H$ è vera in base all'interpretazione appena data dei simboli di relazione.

Se $\varphi = \neg\psi$ e ψ è atomica, allora ψ non può occorrere in H , altrimenti H non verificherebbe la consistenza richiesta a un insieme di Hintikka; quindi ψ è falsa e di conseguenza φ è vera.

Se $\varphi \wedge \psi \in H$, allora, poiché H è di Hintikka, $\varphi \in H$ e $\psi \in H$; quindi per ipotesi induttiva sia φ che ψ sono vere e quindi anche $\varphi \wedge \psi$ lo è.

Se $\neg(\varphi \wedge \psi) \in H$, allora almeno una tra le due formule $\neg\varphi, \neg\psi$ deve stare in H ; quindi per induzione almeno una delle due è vera, ovvero o φ è falsa o ψ è falsa, e in conclusione $\neg(\varphi \wedge \psi)$ è vera.

Se $\forall x \varphi(x) \in H$, allora, poiché H è di Hintikka, $\varphi(d) \in H$ per ogni $d \in D$; quindi, per ipotesi di induzione, $\varphi(d)$ è vera per ogni individuo $d \in D$, ma questo equivale a dire che $\forall x \varphi(x)$ è vera nel modello considerato.

Se $\neg\forall x \varphi(x) \in H$, allora esiste un individuo d tale che $\neg\varphi(d) \in H$; quindi, per ipotesi di induzione, $\varphi(d)$ è falsa, ovvero $\forall x \varphi(x)$ è falsa e $\neg\forall x \varphi(x)$ è vera.

In modo analogo si procede nei casi $\vee, \exists, \rightarrow, \leftrightarrow$.

Se in Φ occorrono simboli di uguaglianza e di funzioni, il modello precedente va modificato definendo su D la seguente relazione di equivalenza $\equiv$ tale che $d \equiv d'$ sse $(d = d') \in H$. In tal modo, il dominio del modello è l'insieme $D/\equiv$ delle classi di equivalenza.

Inoltre: I) ogni costante c viene interpretata nella sua classe di equivalenza $[c]$, ovvero $\llbracket c \rrbracket = [c]$; II) ogni simbolo di funzione n -aria si interpreta nella funzione $\llbracket f \rrbracket$ tale che per ogni $d_1, \dots, d_n$ del dominio

$$\llbracket f \rrbracket(\llbracket d_1 \rrbracket, \dots, \llbracket d_n \rrbracket) = [f(d_1, \dots, d_n)];$$

III) ogni simbolo di relazione n -aria P si interpreta nella relazione n -aria $\llbracket P \rrbracket$ tale che, per ogni $d_1, \dots, d_n$ del dominio:

$$\langle \llbracket d_1 \rrbracket, \dots, \llbracket d_n \rrbracket \rangle \in \llbracket P \rrbracket \Leftrightarrow P(d_1, \dots, d_n) \in H.$$

In tal modo la prova data può essere estesa al caso generale. ■

Vediamo ora che, dato un Φ -tableau non chiuso, riusciamo a produrre un Φ -tableau, che diremo *sistematico*, in cui almeno un ramo H è un insieme di Hintikka che include Φ e ha come dominio l'insieme dei termini chiusi che occorrono in H . Intuitivamente un tableau sistematico è ottenuto applicando le regole in modo esaustivo, senza dimenticare alcuna istanza delle regole riapplicabili ($T_{\forall}$, $T_{\neg\exists}$ e congruenza).

Costruzione del tableau sistematico Data una teoria Φ , un Φ -tableau sistematico può essere costruito nel modo seguente. Si segua la normale procedura per costruire tableau, tuttavia ad ogni passo quando a un nodo dell'albero si applica una regola, si *marchi* come *usata* la formula. Se un tableau è chiuso o tutte le formule non atomiche sono marcate, allora la procedura di costruzione del tableau sistematico è conclusa. Altrimenti, si consideri la foglia di un ramo non chiuso e si consideri una formula di profondità minima (che si trova il più in alto possibile) tra quelle non marcate che appartengono al ramo e la si marchi come usata, la si ricopi sotto la foglia considerata, si applichi la relativa regola e si marchi come usata la formula ricopiata, tranne che nei seguenti casi in cui le formule ricopiate non si marcano e si soddisfano le seguenti ulteriori condizioni:

1. se la formula è del tipo $\forall x \varphi(x)$ si aggiungano al ramo i nodi con le formule $\varphi(t)$ per tutti i termini chiusi t tale che $\varphi(t)$ non occorre nel ramo;
2. se la formula è del tipo $\neg\exists x \varphi(x)$ si aggiungano al ramo i nodi con le formule $\neg\varphi(t)$ per tutti i termini chiusi t tale che $\neg\varphi(t)$ non occorre nel ramo;
3. se la formula è del tipo $t_1 = t_2$ (con t_1, t_2 termini chiusi), si aggiungano al ramo tutte le formule del tipo $\varphi(t_j)$, $j \in \{1, 2\}$, $j \neq i$ per ogni formula $\varphi(t_i)$, $i \in \{1, 2\}$ che occorre già nel ramo.

Nei tre casi precedenti, non marcare come usate le formule aggiunte ci assicura che, nel caso si introducano in seguito nuovi termini, prima o poi si introdurranno anche le nuove istanze delle regole $\forall$ e $\neg\exists$ e $t_1 = t_2$ postulate dalle condizioni di Hintikka.

Si verifica facilmente che un ramo non chiuso di un Φ -tableau sistematico è un insieme di Hintikka che include Φ e il cui dominio coincide con i termini chiusi che occorrono nel ramo.

Definizione 2.12 Diciamo che una teoria Φ è (tableau)-consistente se non esistono Φ -tableau chiusi.

Il seguente può essere considerato per molti versi come il *teorema fondamentale* della logica predicativa.

Proposizione 2.12 (completezza predicativa) *Ogni teoria, finita o numerabile, che sia consistente è anche soddisfacibile.*

Dimostrazione Consideriamo un Φ -tableau sistematico, esso è non chiuso, altrimenti Φ non sarebbe consistente, quindi esso ha un ramo non chiuso H che, per quanto detto precedentemente, è un insieme di Hintikka avente come dominio l'insieme dei termini chiusi del ramo. A questo punto dal lemma segue l'esistenza di un modello di H e quindi di Φ avente come dominio i termini chiusi che occorrono in H , o più in generale classi di equivalenza di tali termini. ■

Il teorema di completezza si può generalizzare a una teoria tableau consistente di qualsiasi cardinalità (si ordini bene e si generalizzi la dimostrazione del caso numerabile).

Dal teorema di completezza è facile dedurre facilmente l'equivalenza tra la relazione di conseguenza logica e quella di tableau-deducibilità, come mostra la proposizione seguente.

Proposizione 2.13 (equivalenza tra $\models$ e $\vdash$)

$$\Phi \models \varphi \Leftrightarrow \Phi \vdash \varphi.$$

Dimostrazione Il verso $\Leftarrow$ segue dalla correttezza del metodo dei tableau. Il verso $\Rightarrow$ segue facilmente per contropositiva dal teorema di completezza. Infatti, se assumiamo che

$$\Phi \not\models \varphi$$

allora, per definizione di tableau-deducibilità, ogni $\Phi \cup \{\neg\varphi\}$ -tableau non è chiuso, ovvero la teoria $\Phi \cup \{\neg\varphi\}$ è tableau-consistente. Quindi, per il teorema di completezza, tale teoria è soddisfacibile, e quindi

$$\Phi \models \varphi$$

perché se valesse $\Phi \not\models \varphi$ la teoria $\Phi \cup \{\neg\varphi\}$ sarebbe insoddisfacibile. ■

Spesso la completezza della logica predicativa viene identificata con il verso $\Rightarrow$ della proposizione precedente: infatti, assumendo che, per ogni Σ -teoria e Σ -proposizione φ , valga $\Phi \models \varphi \Rightarrow \Phi \vdash \varphi$; si dimostra immediatamente, per contropositiva, che ogni teoria tableau consistente è anche soddisfacibile.

La completezza del sistema deduttivo dei tableau ci consente la dimostrazione di altre proprietà fondamentali della logica predicativa.

Proposizione 2.14 (finitzza della logica predicativa)

$$\Phi \models \varphi \Leftrightarrow \Delta \models \varphi$$

per qualche sottoinsieme finito Δ di Φ .

Dimostrazione Per il teorema precedente:

$$\Phi \models \varphi \Leftrightarrow \Phi \vdash_T \varphi.$$

Ma $\Phi \vdash_T \varphi$ sse vi è un $\Phi \cup \{\neg\varphi\}$ -tableau chiuso; un tale tableau è finito, quindi in esso occorrono solo un numero finito di formule di Φ , quindi φ è conseguenza logica di tali formule. ■

Proposizione 2.15 (compattezza della logica predicativa) *Una teoria predicativa Φ è soddisfacibile sse lo è ogni suo sottoinsieme finito di formule.*

Dimostrazione Se ogni insieme finito di formule è soddisfacibile, allora, per la correttezza dei tableau, non può esistere un Φ -tableau chiuso, perché un tableau chiuso è sempre finito. Quindi la teoria è consistente, ovvero per il teorema di completezza è soddisfacibile. ■

Una conseguenza diretta della compattezza è l'esistenza di modelli non standard dei numeri reali (e dei numeri naturali). Consideriamo il modello $\mathcal{R}$ dei numeri reali e sia $\text{Th}(\mathcal{R})$ la teoria delle proposizioni che valgono in tale modello. Aggiungiamo a tale teoria l'insieme infinito di proposizioni $\Phi = \{\exists x (nx \leq 1) \mid n \in \omega\}$. Il modello $\mathcal{R}$ non soddisfa Φ , tuttavia, per ogni naturale non nullo m , $\mathcal{R}$ soddisfa $\{\exists x (nx \leq 1) \mid n \leq m\}$. Quindi, per il teorema di compattezza, $\text{Th}(\mathcal{R}) \cup \Phi$ ha un modello. In tale modello esiste un numero, detto *iperreale*, che non è nullo, ma è minore di qualsiasi numero reale positivo. Un tale numero rappresenta quindi un infinitesimo. Un'estensione del modello dei reali con iperreali che rappresentano infinitesimi e infiniti (inversi di infinitesimi) è la base della cosiddetta *analisi non standard* introdotta da A. Robinson negli anni Sessanta. Per dare un'idea della potenza di tale metodo, dimostriamo in modo non standard il teorema di derivazione delle funzioni composte. Si dimostra che ogni numero iperreale r non infinito è la somma di un reale $\text{st}(r)$, la sua parte standard, e di un infinitesimo. Una funzione g si dice continua in x (x numero reale) se per ogni infinitesimo ε (positivo o negativo) si ha $\text{st}(g(x + \varepsilon)) = g(x)$, ovvero se esiste un altro infinitesimo δ per cui $g(x + \varepsilon) = g(x) + \delta$. La derivata $f'(x)$ di una funzione f in un punto x si definisce come il numero reale che verifica la seguente equazione per ogni infinitesimo ε :

$$f'(x) = \text{st} \frac{f(x + \varepsilon) - f(x)}{\varepsilon}.$$

Se $f'(x)$ esiste, vale che $f(x + \varepsilon) - f(x) = f'(x)\varepsilon$ (per qualche infinitesimo γ , vale $f'(x) = (f(x + \varepsilon) - f(x))/\varepsilon + \gamma$). Questo implica che una funzione derivabile in x è continua in x , in quanto il prodotto tra un reale e un infinitesimo è un infinitesimo. Consideriamo la funzione composta $f \circ g$ e supponiamo che esistano $g'(x)$ e $f'(g(x))$; è possibile dimostrare che

$$(f \circ g)'(x) = f'(g(x)) \cdot g'(x).$$

Infatti, utilizzando la continuità di g in x , ovvero che $g(x + \varepsilon) = g(x) + \delta$, si ottiene (riferendo le uguaglianze solo alle parti standard):

$$\begin{aligned} \frac{(f \circ g)(x + \varepsilon) - (f \circ g)(x)}{\varepsilon} &= \frac{f(g(x + \varepsilon)) - f(g(x))}{\varepsilon} = \\ &= \frac{f(g(x) + \delta) - f(g(x))}{\varepsilon} = \frac{f'(g(x)) \cdot \delta}{\varepsilon} = \frac{f'(g(x)) \cdot [g(x + \varepsilon) - g(x)]}{\varepsilon} = \\ &= f'(g(x)) \cdot g'(x). \end{aligned}$$

2.6. Forme di Skolem ed espansione di Herbrand

In questa sezione mostreremo dei risultati notevoli di normalizzazione, secondo i quali ogni formula (o teoria) predicativa è logicamente equivalente o equisoddisfacibile a una formula (o a una teoria) avente una forma particolare.

Proposizione 2.16 *Data una formula predicativa φ , vi è una formula ad essa equivalente in forma prenessa del tipo*

$$Q_1 x_1 Q_2 x_2 \dots Q_k x_k \mu$$

ove $Q_1, Q_2, \dots, Q_k$ è una sequenza di quantificatori che dicesi prefisso e μ è una formula proposizionale che dicesi matrice.

Dimostrazione La dimostrazione si ottiene per induzione sulla complessità delle formule una volta verificata la validità logica delle seguenti equivalenze in cui ψ è una formula ove non occorre libera x , Q indica un qualsiasi quantificatore, Q' indica l'altro quantificatore diverso da Q e $*$ indica uno dei due connettivi $\wedge, \vee$:

$$\neg \forall x \varphi \leftrightarrow \exists x \neg \varphi$$

$$\neg \exists x \varphi \leftrightarrow \forall x \neg \varphi$$

$$Qx \varphi(x) \leftrightarrow Qy \varphi(y)$$

$$(Qx\varphi * \psi) \leftrightarrow Qx(\varphi * \psi)$$

$$(\psi * Qx\varphi) \leftrightarrow Qx(\psi * \varphi)$$

$$(Qx\varphi \rightarrow \psi) \leftrightarrow Q'x(\varphi \rightarrow \psi)$$

$$(\psi \rightarrow Qx\varphi) \leftrightarrow Qx(\psi \rightarrow \varphi)$$

$$(Qx\varphi(x) \leftrightarrow \psi) \leftrightarrow Q'xQy((\varphi(x) \rightarrow \psi) \wedge (\psi \rightarrow \varphi(y))).$$

In tal modo, applicando le equivalenze considerate i quantificatori possono essere spostati tutti all'inizio della formula. ■

Esempio 2.16

$$\neg [\forall x(\varphi(x) \rightarrow \psi) \rightarrow (\exists x\varphi(x) \rightarrow \psi)]$$

$$\neg \exists x((\varphi(x) \rightarrow \psi) \rightarrow \forall x(\varphi(x) \rightarrow \psi))$$

$$\neg \exists x\forall y((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(y) \rightarrow \psi))$$

$$\forall x\neg\forall y((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(y) \rightarrow \psi))$$

$$\forall x\exists y\neg((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(y) \rightarrow \psi)).$$

Proposizione 2.17 *Dato un enunciato φ in forma prenessa se ne può determinare un altro, che indicheremo con $\text{Skolem}(\varphi)$, che è soddisfacibile sse lo è anche φ , e in cui compaiono solo quantificatori universali.*

Dimostrazione (cenno) L'intuizione sottostante è la seguente. La proposizione $\forall x\exists yP(x, y)$ esprime, in un dato modello, che per ogni valore di x esiste un valore di y che soddisfa il predicato $P(x, y)$. Allora si può associare a ciascun valore di x il corrispondente valore di y che rende vera la proposizione, ma tale corrispondenza è una funzione e quindi possiamo introdurre un simbolo funzionale f che la denota. In tal modo $P(x, f(x))$ vale per costruzione, nel modello esteso per denotare f , quando nel modello di partenza vale $\forall x\exists yP(x, y)$. In generale si può procedere nel modo seguente. Se nella forma prenessa il quantificatore di posto i è esistenziale, lo si rimuove rimpiazzando contemporaneamente la variabile i -esima x_i con il termine $f_i(x, y, \dots)$, ove f_i è un nuovo simbolo di funzione e $x, y, \dots$ sono le variabili quantificate universalmente che nel prefisso precedono la variabile x_i (se $i = 1$, e quindi nessuna variabile universale la precede, f_1 è una costante individuale). ■

Per esempio, dalla forma prenessa sopra ottenuta si giunge alla seguente forma di Skolem:

$$\forall x\neg((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(fx) \rightarrow \psi)).$$

Dato che i quantificatori di una forma di Skolem sono solo universali, si può omettere di indicarli, intendendo che tutte le variabili libere di una tale formula sono da considerarsi universalmente quantificate. La formula precedente si indica quindi usualmente nel modo seguente:

$$\neg((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(fx) \rightarrow \psi)).$$

Inoltre, se si pone in forma normale congiuntiva la matrice di una forma di Skolem, si vede facilmente che essa risulta equivalente a una teoria le cui formule sono le disgiunzioni che compongono tale matrice. Per esempio, nella formula precedente, esprimendo il connettivo di implicazione tramite disgiunzione e negazione si ottiene in due passi:

$$(\varphi(x) \rightarrow \psi) \wedge \neg(\varphi(fx) \rightarrow \psi)$$

$$(\neg\varphi(x) \vee \psi) \wedge (\varphi(fx) \wedge \neg\psi).$$

Indicando quindi tali disgiunzioni con l'insieme dei letterali che le compongono, si ottiene la cosiddetta *rappresentazione a clausole* di una formula, in cui tutti i letterali di una disgiunzione costituiscono una clausola e la formula è individuata da tutte le clausole che in tal modo risultano. La formula precedente è per esempio rappresentata dalle seguenti tre clausole:

$$\{\neg\varphi(x), \psi\}$$

$$\{\varphi(fx)\}$$

$$\{\neg\psi\}.$$

Definizione 2.13 Dato un insieme Φ di formule predicative indichiamo con $\text{Skolem}(\Phi)$ l'insieme delle forme di Skolem di tutte le forme prenesse ottenute da formule di Φ .

Per quanto visto prima tale insieme è soddisfacibile se tale è Φ . Data una teoria Φ , indichiamo con Σ_Φ^* la segnatura della teoria $\text{Skolem}(\Phi)$ estesa con un simbolo di costante individuale nel caso in cui nessun simbolo del genere dovesse occorrere in $\text{Skolem}(\Phi)$.

Definizione 2.14 Diciamo universo di Herbrand della teoria Φ l'insieme dei termini chiusi sulla segnatura Σ_Φ^* .

Definizione 2.15 Diciamo espansione di Herbrand della teoria Φ la teoria proposizionale $\text{Herbrand}(\Phi)$ ottenuta istanziando, in tutti i modi possibili, le variabili delle formule di $\text{Skolem}(\Phi)$ con i termini dell'universo di Herbrand di Φ .

Esempio 2.17 Si consideri la seguente formula:

$$\neg[\forall x(\varphi(x) \rightarrow \psi) \rightarrow (\exists x \varphi(x) \rightarrow \psi)]$$

la cui forma di Skolem determinata precedentemente è

$$\neg((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(fx) \rightarrow \psi)).$$

L'universo di Herbrand relativo è

$$\{a, fa, ffa, fffa, \dots\}$$

e la sua espansione di Herbrand contiene formule del tipo

$$\begin{aligned} &\neg((\varphi(a) \rightarrow \psi) \rightarrow (\varphi(fa) \rightarrow \psi)) \\ &\neg((\varphi(fa) \rightarrow \psi) \rightarrow (\varphi(ffa) \rightarrow \psi)) \\ &\neg((\varphi(ffa) \rightarrow \psi) \rightarrow (\varphi(fffa) \rightarrow \psi)) \\ &\dots\dots\dots \end{aligned}$$

Proposizione 2.18 (espansione di Herbrand) *Una teoria Φ è soddisfacibile sse lo è $\text{Herbrand}(\Phi)$.*

Dimostrazione Dalle definizioni e proposizioni precedenti segue che Φ è equisoddisfacibile con $\text{Skolem}(\Phi)$. Ma tale teoria è soddisfacibile sse vi è un ramo non chiuso, e quindi soddisfacibile, dello $\text{Skolem}(\Phi)$ -tableau sistematico. Ma tale ramo coincide proprio con $\text{Herbrand}(\Phi)$. ■

2.7. Teoremi di Löwenheim-Skolem

Dalla compattezza discendono conseguenze molto importanti per le strutture che possono essere descritte nella logica predicativa.

Proposizione 2.19 *Se una teoria predicativa Φ ha modelli finiti di qualsiasi cardinalità finita, allora ha un modello infinito.*

Dimostrazione Indichiamo con ψ_n una formula che asserisce l'esistenza di almeno n individui (si costruisce immediatamente utilizzando $\exists$, $\neg$, $=$ e n variabili individuali). Consideriamo la teoria $\Psi = \{\psi_n | n \in \mathbb{N}\}$ del dominio numerabile e $\Phi' = \Phi \cup \Psi$. Se Φ' ha un modello esso è ovviamente infinito. Ma ogni suo sottoinsieme finito ha un modello poiché Φ ha modelli di qualsiasi cardinalità finita, quindi per il teorema di compattezza Φ' ha un modello e quindi Φ ha un modello infinito. ■

Corollario 2.1 *Non esiste alcuna teoria soddisfatta da tutti e soli i modelli finiti.*

Proposizione 2.20 *Non esiste alcuna proposizione χ tale che*

$$\mathcal{M} \models \chi \Leftrightarrow \mathcal{M} \text{ è infinito.}$$

Dimostrazione Supponiamo che una tale proposizione χ esista. Si consideri la teoria Ψ del dominio numerabile:

$$\mathcal{M} \models \Psi \Rightarrow \mathcal{M} \models \chi;$$

quindi

$$\Psi \models \chi$$

e per il teorema di finitezza ciò è assurdo. ■

Proposizione 2.21 *La teoria degli ordinamenti ben fondati non può essere espressa in logica predicativa.*

Dimostrazione Sia Φ tale ipotetica teoria. Si consideri la teoria $\Lambda = \{c_{n+1} < c_n \mid n \in \mathbb{N}\}$. Allora $\Phi' = \Phi \cup \Lambda$, per la proprietà di compattezza, deve avere un modello (visto che esistono insiemi ben fondati di qualsiasi cardinalità finita). Tuttavia un tale modello, che sarebbe anche modello di Φ , non sarebbe ben fondato in quanto soddisfa Λ . ■

Abbiamo visto che una teoria con modelli di cardinalità finita grande a piacere ha un modello infinito. Possiamo ulteriormente precisare tale asserito con un teorema (vedi sotto). Premettiamo un lemma che discende immediatamente dal fatto che i termini di una segnatura sono particolari sequenze finite di simboli.

Lemma 2.2 *Una teoria finita o numerabile ha un insieme di termini chiusi al più numerabile.*

Il teorema che segue ha un significato profondissimo e insieme alla compattezza caratterizza l'essenza della logica predicativa (la cosa è stabilita in modo del tutto rigoroso in un risultato dovuto a Lindström, 1969). Detto semplicemente, le strutture che si possono descrivere con teorie predicative finite o numerabili non sono altro che strutture sul dominio dei numeri naturali, ovvero, le usuali teorie logiche predicative sono essenzialmente teorie interpretabili sui numeri naturali.

Proposizione 2.22 (teorema di Löwenheim-Skolem, o Skolem-downward) *Se una teoria Φ finita o numerabile ha modelli infiniti, allora ha un modello numerabile.*

Dimostrazione Consideriamo $\Phi' = \Phi \cup \Psi$, ove Ψ è la teoria del dominio numerabile. La teoria Φ' ha un modello poiché Φ ha un modello infinito. Si consideri quindi il modello di Φ' individuato da un ramo H non chiuso di un Φ' -tableau. Φ' e quindi Φ hanno un modello il cui dominio sono i termini chiusi (o loro classi di equivalenza) che occorrono in H . Ma tale insieme è al più numerabile per il lemma precedente, ed è esattamente numerabile in base a quanto espresso dalla teoria Ψ . ■

Tale teorema si generalizza al caso di una teoria più che numerabile: se una teoria più che numerabile ha modelli infiniti, allora ha un modello avente la stessa cardinalità della teoria.

Il teorema precedente è responsabile del seguente famoso *paradosso di Skolem*. Si consideri una teoria assiomatica degli insiemi in logica predicativa. Tale teoria afferma l'esistenza di insiemi più che numerabili, eppure essa ha un modello numerabile. Come può avvenire un fatto del genere? Basta distinguere due livelli. L'ambiente insiemistico interno è diverso da quello insiemistico esterno entro cui si è definito il modello, quindi non è detto che gli insiemi del livello esterno siano tutti presenti all'interno, e sicuramente ciò è falso poiché nel modello non esistono insiemi che stabiliscono la corrispondenza tra un insieme del modello e l'insieme delle sue parti. Detto altrimenti, l'insieme delle parti del modello non coincide con il vero insieme delle parti della teoria degli insiemi entro cui il modello è definito.

Vale infine un risultato simmetrico rispetto al precedente teorema di Löwenheim-Skolem.

Proposizione 2.23 (teorema di Löwenheim-Skolem-Tarski, o Skolem-upward) *Se una teoria ha un modello di una data cardinalità infinita, allora ha modelli di qualsiasi cardinalità infinita maggiore.*

Dimostrazione (cenno) Basta aggiungere un numero di costanti pari alla cardinalità voluta e proposizioni che asseriscono la diversità di ciascuna costante da ogni altra. Per la compattezza la teoria estesa è soddisfacibile, quindi ha un modello $\mathcal{M}$ con la cardinalità voluta. A questo punto basta estrarre da $\mathcal{M}$ un modello della teoria iniziale trascurando di dare interpretazione alle costanti aggiunte. ■

Il teorema precedente implica l'esistenza di modelli aritmetici non standard: infatti in base ad esso vi sono modelli degli assiomi di Peano, espressi in logica predicativa, il cui dominio è più che numerabile.

Capitolo 3

Calcoli logici

Un calcolo logico è un procedimento algoritmico, in base a cui è possibile stabilire una relazione di *deducibilità* $\Phi \vdash \varphi$ tra una Σ -teoria Φ e una Σ -proposizione φ . I primi calcoli, risalenti a Hilbert, ma prima ancora a Frege, erano *assiomatici*, ovvero si proponevano di individuare le formule logicamente valide partendo da pochi *assiomi* e derivando quindi tutte le altre come *teoremi*, tramite regole deduttive. Una formulazione succinta di tale calcolo (non considerando l'uguaglianza e utilizzando solo gli operatori logici $\rightarrow, \neg, \forall$) è la seguente (basata su quella presentata in Church, 1956):

Assiomi HF

$$\varphi \rightarrow (\psi \rightarrow \varphi)$$

$$(\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta))$$

$$(\neg \varphi \rightarrow \neg \psi) \rightarrow (\psi \rightarrow \varphi)$$

$$\forall x \varphi(x) \rightarrow \varphi(t) \quad (t \text{ termine liberamente sostituibile a } x)$$

$$(\psi \rightarrow \varphi(x)) \rightarrow (\psi \rightarrow \forall x \varphi(x)) \quad (x \notin \text{var}(\psi))$$

Regola di inferenza HF Modus ponens:

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi}$$

(se si derivano le formule sopra la linea orizzontale si può derivare la formula sottostante).

Una *deduzione HF* della proposizione φ dalla teoria Φ è una sequenza finita di formule in cui ad ogni passo occorrono o assiomi o formule di Φ , oppure una formula ottenuta per modus ponens da formule che occorrono in passi precedenti.

La relazione di deducibilità $\vdash_{HF}$ di tale calcolo può essere definita dicendo che:

$$\Phi \vdash_{HF} \varphi$$

se esiste una deduzione HF di φ dalla teoria Φ ; $\vdash_{HF} \varphi$ indica che φ è ottenuto utilizzando solo gli assiomi; il tal caso φ si dice *teorema HF*.

Anche se la formulazione di una tale deducibilità è semplice ed elegante, risulta di fatto estremamente difficile svolgere deduzioni formali di una certa complessità. Un grande passo in avanti, per una comprensione della natura stessa delle dimostrazioni formali, fu il cosiddetto *teorema di deduzione* dimostrato nel 1930 da Herbrand e, indipendentemente, da Tarski.

Lemma 3.1

$$\vdash \varphi \rightarrow \varphi.$$

Dimostrazione

1. $(\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)) \rightarrow ((\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi))$ (assioma 2)
2. $\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)$ (assioma 1)
3. $(\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi)$ (modus ponens 1, 2)
4. $\varphi \rightarrow (\varphi \rightarrow \varphi)$ (assioma 1)
5. $\varphi \rightarrow \varphi$ (modus ponens 4, 3) ■

Proposizione 3.1 (teorema di deduzione)

$$\Phi, \varphi \vdash_{HF} \psi \Rightarrow \Phi \vdash \varphi \rightarrow \psi.$$

Dimostrazione Data una deduzione $\Phi, \varphi \vdash_{HF} \psi$ si costruisca la sua $(\varphi \rightarrow)$ -trasformata sostituendo ogni formula θ che vi occorre con la formula $\varphi \rightarrow \theta$. Quello che si ottiene in tal modo non è più una deduzione, ma mostreremo che aggiungendo dei passi deduttivi intermedi, in cui sono essenziali gli assiomi HF , si ottiene una deduzione HF di $\varphi \rightarrow \psi$ a partire da Φ e $\varphi \rightarrow \varphi$. Ma, in base al lemma, $\varphi \rightarrow \varphi$ è un teorema HF , quindi in definitiva si ottiene $\Phi \vdash \varphi \rightarrow \psi$. Rimane quindi da aggiungere i passi intermedi per rendere la $(\varphi \rightarrow)$ -trasformata una deduzione HF .

Procediamo per induzione sui passi della deduzione. Al primo passo si può avere o φ , o una proposizione δ che è un assioma o una proposizione di Φ . Nella $(\varphi \rightarrow)$ -trasformata questi diventano rispettivamente: 1) $\varphi \rightarrow \varphi$ e

ii) $\varphi \rightarrow \delta$. Nel primo caso, per il lemma la $\varphi \rightarrow \varphi$ è *HF*-deducibile; nel secondo caso poiché $\delta \rightarrow (\varphi \rightarrow \delta)$ è un assioma, e per ipotesi δ è un assioma o una formula di Φ , allora anche $\varphi \rightarrow \delta$ è *HF*-deducibile da Φ . Supponiamo ora di aver dimostrato che tutte le formule $(\varphi \rightarrow)$ -trasformate, fino a un certo passo della deduzione originale, sono *HF*-deducibili da Φ , dimostriamo che anche la formula $(\varphi \rightarrow)$ -trasformata del passo successivo è tale. Se al passo successivo della deduzione originale si ha un assioma, allora si procede come sopra; se non è questo il caso; allora si ha una formula γ ottenuta per modus ponens da formule di passi precedenti, diciamo ζ e $\zeta \rightarrow \gamma$. Pertanto sono già deducibili le $(\varphi \rightarrow)$ -trasformate $\varphi \rightarrow \zeta$ e $\varphi \rightarrow (\zeta \rightarrow \gamma)$. A questo punto utilizzando l'assioma

$$(\varphi \rightarrow (\zeta \rightarrow \gamma)) \rightarrow ((\varphi \rightarrow \zeta) \rightarrow (\varphi \rightarrow \gamma))$$

e applicando due volte il modus ponens si ottiene che anche $\varphi \rightarrow \gamma$ è deducibile. ■

Presenteremo ora brevemente altri calcoli logici. Per semplicità non considereremo il connettivo di doppia implicazione e il predicato di uguaglianza.

3.1. Deduzione naturale

Il teorema di deduzione costituì il punto di partenza delle ricerche di Gentzen sulla teoria della dimostrazione, che portarono a una nuova idea di dimostrazione formale, molto più vicina ai meccanismi basilari delle dimostrazioni della matematica. Per questo motivo tale calcolo si chiama calcolo di *deduzione naturale*. Un suo sviluppo è costituito dal calcolo dei *sequent* di Gentzen, che si è poi dimostrato essenzialmente equivalente a una variante del calcolo dei tableau. Tutti i calcoli menzionati sono completi nel senso che la deducibilità ad essi associata coincide con la relazione di conseguenza logica.

Diamo una sintetica presentazione del calcolo di deduzione naturale.

Regole di deduzione naturale

$$E_{\wedge} : \frac{\varphi \wedge \psi}{\varphi}$$

$$E_{\wedge} : \frac{\varphi \wedge \psi}{\psi}$$

$$I_{\wedge} : \frac{\varphi, \psi}{\varphi \wedge \psi}$$

$$E\vee : \frac{\varphi, \rightarrow\chi, \psi, \rightarrow\chi, \varphi \vee \psi}{\chi}$$

$$I\vee : \frac{\varphi}{\varphi \vee \psi}$$

$$I\vee : \frac{\psi}{\varphi \vee \psi}$$

$$E\rightarrow : \frac{\varphi, \varphi \rightarrow \psi}{\psi}$$

$$I\rightarrow : \frac{\psi}{\varphi \rightarrow \psi}$$

$$E\neg : \frac{\neg\varphi \rightarrow \perp}{\varphi}$$

$$I\neg : \frac{\varphi \rightarrow \perp}{\neg\varphi}$$

$$E\perp : \frac{\perp}{\varphi}$$

$$I\perp : \frac{\varphi, \neg\varphi}{\perp}$$

$$E\forall : \frac{\forall x\varphi(x)}{\varphi(t)}$$

$$I\forall : \frac{\varphi(y)}{\forall x\varphi(x)}$$

$$E\exists : \frac{\varphi(y) \rightarrow \psi, \exists x\varphi(x)}{\psi}$$

$$I\exists : \frac{\varphi(t)}{\exists x\varphi(x)}$$

Le formule sopra la linea orizzontale si dicono *premesse*, quelle al di sotto della linea si dicono *conclusioni*. Ogni operatore logico è fornito di due tipi di regole: quelle siglate con *E*, in cui l'operatore che si trova nelle premesse è eliminato nella conclusione, e quelle siglate con *I*, in cui l'operatore, che non è presente nelle premesse, viene introdotto nella conclusione.

Una deduzione naturale è una sequenza di passi, in ciascuno dei quali si può alternativamente:

1. Porre una formula qualsiasi, detta *ipotesi* della deduzione.

2. Porre la *conclusione* di una regola le cui premesse sono state ottenute in passi precedenti e non sono state ancora bloccate in accordo alla condizione successiva.
3. Porre l'implicazione $\varphi \rightarrow \psi$ (introduzione di $\rightarrow$), se al passo precedente si è ottenuta ψ . Contemporaneamente, se φ è un'ipotesi posta a un passo precedente, essa viene *eliminata* e vengono *bloccate* tutte le formule della deduzione che vanno dall'ipotesi eliminata fino alla formula precedente l'implicazione $\varphi \rightarrow \psi$. Le formule bloccate non possono essere utilizzate nei passi successivi.

Le ipotesi necessarie per dedurre una formula si dicono *assunzioni* della formula; in tal caso si dice anche che la formula *dipende* da tali ipotesi. Nelle regole $I\forall$ e $E\exists$, la variabile y non deve occorrere libera né in ψ né in alcuna assunzione di $\varphi(y)$. L'ultima formula di una deduzione costituisce la sua *tesi*. Una deduzione naturale la cui tesi è ψ e in cui le ipotesi non eliminate sono $\varphi_1, \dots, \varphi_n$ si indica con:

$$\varphi_1, \dots, \varphi_n \vdash \psi.$$

Nella costruzione delle deduzioni naturali, la regola di terzo tipo (eliminazione di ipotesi) determina un ruolo privilegiato per il connettivo di implicazione. Come si vede facilmente, tale regola discende direttamente dal teorema di deduzione.

Diamo alcuni esempi di deduzione naturale. Ogni linea è numerata ponendo a lato la formula dedotta e alternativamente: I) la sigla *hp* se essa è un'ipotesi; II) la sigla della regola applicata, con i numeri delle linee delle premesse. Quando si pone un'ipotesi si apre una parentesi quadra che si chiude quando l'ipotesi viene eliminata, in modo che le formule bloccate rimangano racchiuse tra le parentesi quadre; inoltre si pone a lato la sigla $-hp\ n$ se n è la linea dell'ipotesi eliminata.

Esempio 3.1 $P \rightarrow Q \vdash \neg Q \rightarrow \neg P$.

1.	$P \rightarrow Q$	hp
[2.	$\neg Q$	hp
[3.	P	hp
4.	Q	$E \rightarrow 1, 3$
5.	$\perp$	$I \perp 4, 2$
]6.	$P \rightarrow \perp$	$-hp3$
7.	$\neg P$	$I \neg 6$
]8.	$\neg Q \rightarrow \neg P$	$-hp2$

Esempio 3.2 $\vdash \neg P \wedge (P \vee Q) \rightarrow Q$.

-	[1. $\neg P \wedge (P \vee Q)$		hp
	2. $\neg P$	$E \wedge 1$	
	3. $P \vee Q$	$E \wedge 1$	hp
	[4. P		hp
	5. $\perp$	$I \perp 4, 2$	
	6. Q	$E \perp 5$	
	]7. $P \rightarrow Q$	$I \rightarrow 6$	- hp4
	[8. Q		hp
	]9. $Q \rightarrow Q$	$I \rightarrow 8$	- hp8
	10. Q	$E \vee 3, 7, 9$	
-	]11. $\neg P \wedge (P \vee Q) \rightarrow Q$	$I \rightarrow 10$	- hp1

Esempio 3.3 $\vdash P \vee \neg P$.

-	[1. $\neg(P \vee \neg P)$		hp
	[2. P		hp
	3. $P \vee \neg P$	$I \vee 2$	
	4. $\perp$	$I \perp 3, 1$	
	]5. $P \rightarrow \perp$	$I \rightarrow 4$	- hp2
	6. $\neg P$	$I \neg 5$	
	7. $P \vee \neg P$	$I \vee 6$	
	8. $\perp$	$I \perp 7, 1$	
	]9. $\neg(P \vee \neg P) \rightarrow \perp$	$I \rightarrow 8$	- hp1
-	10. $P \vee \neg P$	$E \neg 9$	

Esempio 3.4 $\forall x(Px \wedge Qx) \vdash \forall x Px \wedge \forall x Qx$.

1. $\forall x(Px \wedge Qx)$		hp
2. $Px \wedge Qx$	$E \forall 1$	
3. Px	$E \wedge 2$	
4. Qx	$E \wedge 2$	
5. $\forall x Px$	$I \forall 3$	
6. $\forall x Qx$	$I \forall 4$	
7. $\forall x Px \wedge \forall x Qx$	$I \wedge 5, 6$	

Esempio 3.5 $\exists x \forall y Pxy \vdash \forall y \exists x Pxy$.

1.	$\exists x \forall y Pxy$		hp
[2.	$\forall y Pxy$		hp
3.	Pxy	$E \forall 2$	
4.	$\exists x Pxy$	$I \forall 3$	
5.	$\forall y \exists x Pxy$	$I \forall 4$	
]6.	$\forall y Pxy \rightarrow \forall y \exists x Pxy$		— hp2
7.	$\forall y \exists x Pxy$	$E \exists 6, 1$	

Esempio 3.6 $P \wedge (Q \vee R) \vdash (P \wedge Q) \vee (P \wedge R)$.

1.	$P \wedge (Q \vee R)$		hp
2.	P	$E \wedge 1$	
3.	$Q \vee R$	$E \wedge 1$	
[4.	Q		hp
5.	$P \wedge Q$	$I \wedge 2, 4$	
6.	$(P \wedge Q) \vee (P \wedge R)$	$E \vee 5$	
]7.	$Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	$I \rightarrow 6$	— hp4
[8.	R		hp
9.	$P \wedge R$	$I \wedge 2, 8$	
10.	$(P \wedge Q) \vee (P \wedge R)$	$I \vee 9$	
]11.	$R \rightarrow (P \wedge Q) \vee (P \wedge R)$	$I \rightarrow 10$	— hp8
12.	$(P \wedge Q) \vee (P \wedge R)$	$E \vee 3, 7, 11$	

Esempio 3.7 $\forall x Qx \vdash \neg \exists x \neg Qx$.

1.	$\forall x Qx$		hp
[2.	$\exists x \neg Qx$		hp
[3.	$\neg Qy$		hp
4.	Qy	$E \forall 1$	
5.	$\perp$	$I \perp 3, 4$	
]6.	$\neg Qy \rightarrow \perp$	$I \rightarrow 5$	— hp3
7.	$\perp$	$E \exists 2, 6$	
]8.	$\exists x \neg Qx \rightarrow \perp$	$I \rightarrow 7$	— hp2
9.	$\neg \exists x \neg Qx$	$I \neg 8$	

Esempio 3.8 $\neg \exists x \neg Qx \vdash \forall x Qx$.

1. $\neg \exists x \neg Qx$		hp
[2. $\neg Qy$		hp
3. $\exists x \neg Qx$	$I \exists 2$	
4. $\perp$	$I \perp 1, 3$	
]5. $\neg Qy \rightarrow \perp$	$I \rightarrow 4$	— hp2
6. Qy	$E \neg 5$	
7. $\forall x Qx$	$I \forall 6$	

Esempio 3.9 $\forall xy(Pxy \rightarrow Qx), \forall xy(Pxy \rightarrow Pyx) \vdash \forall xy(Pxy \rightarrow Qx \wedge Qy)$.

1. $\forall xy(Pxy \rightarrow Qx)$		hp
2. $\forall xy(Pxy \rightarrow Pyx)$		hp
3. $Pxy \rightarrow Qx$	$E \forall 1$	
[4. Pxy		hp
5. Qx	$E \rightarrow 4, 3$	
6. $Pxy \rightarrow Pyx$	$E \forall 2$	
7. Pyx	$E \rightarrow 4, 6$	
8. $Pyx \rightarrow Qy$	$E \forall 1$	
9. Qy	$E \rightarrow 7, 8$	
10. $Qx \wedge Qy$	$I \wedge 5, 9$	
]11. $Pxy \rightarrow Qx \wedge Qy$	$I \rightarrow 10$	— hp4
12. $\forall xy(Pxy \rightarrow Qx \wedge Qy)$	$I \forall 11$	

Esempio 3.10 $\exists x(Px \vee Qx) \vdash \exists x Px \vee \exists x Qx$.

1. $\exists x(Px \vee Qx)$		hp
[2. $Py \vee Qy$		hp
[3. Py		hp
4. $\exists x Px$	$I \exists 3$	
5. $\exists x Px \vee \exists x Qx$	$I \vee 4$	
]6. $Py \rightarrow \exists x Px \vee \exists x Qx$	$I \rightarrow 5$	— hp3
[7. Qy		hp
8. $\exists x Qx$	$I \exists 7$	
9. $\exists x Px \vee \exists x Qx$	$I \vee 8$	
]10. $Qy \rightarrow \exists x Px \vee \exists x Qx$	$I \rightarrow 9$	— hp7
11. $\exists x Px \vee \exists x Qx$	$E \vee 6, 10, 2$	
]12. $Py \vee Qy \rightarrow \exists x Px \vee \exists x Qx$	$I \rightarrow 11$	— hp2
13. $\exists x Px \vee \exists x Qx$	$I \exists 12, 1$	

Osserviamo che in una deduzione naturale non si possono applicare regole di ricopiatura, o, detto altrimenti, se si copia una formula si devono prima ricopiare anche tutte le sue assunzioni. Per esempio, potremmo essere tentati di concludere la deduzione precedente già al passo 11, ma se ci fermassimo a quel punto avremmo ottenuto la formula sotto l'ipotesi 1 e 2; l'ipotesi 2 viene eliminata al passo 12 e quindi, se potessimo ricopiare quanto ottenuto al passo 11 (senza ricopiare prima le sue assunzioni) potremmo concludere. Tuttavia, ciò non sarebbe corretto: ecco perché è stata utilizzata la regola di eliminazione del quantificatore esistenziale utilizzando come premesse le formule dei passi 12 e 1.

Principi generali da seguire nella deduzione naturale sono i seguenti: I) per dedurre un'implicazione, si assuma come ipotesi l'antecedente e si cerchi di dimostrare il conseguente; II) per dimostrare una congiunzione si cerchi di dimostrare entrambe le formule componenti; III) per dimostrare una disgiunzione si cerchi di dimostrare una delle sue componenti. Negli altri casi, si assuma la negazione della formula e si cerchi di ottenere un assurdo.

Nell'eliminare le ipotesi si deve seguire l'ordine inverso con cui sono state introdotte, eliminando quindi l'ultima ipotesi fatta o la più recente ancora non eliminata.

La deduzione naturale consente di distinguere con chiarezza il ragionamento logico costruttivo, proprio della logica intuizionista, da quello della logica classica. Infatti, basta eliminare la regola $E \neg$, indicata anche con RAA (*reductio ad absurdum*), per ottenere un calcolo logico che esprime i principi deduttivi della logica intuizionista.

Una caratteristica importante del metodo di deduzione naturale consiste nella sua intrinseca modularità. Infatti, una volta ottenuta la deduzione $\varphi_1, \dots, \varphi_n \vdash \psi$, si può aggiungere al metodo la regola derivata R :

$$R: \frac{\varphi_1, \dots, \varphi_n}{\psi}.$$

In tal modo si possono strutturare deduzioni di notevole complessità. Il testo di Kalish-Montague,¹ in cui si introduce un metodo di deduzione naturale molto simile al nostro, contiene parecchi esempi di deduzioni naturali in cui, utilizzando regole derivate, si riescono a formalizzare dimostrazioni molto articolate in teorie matematiche interessanti (teoria dei campi ordinati, dei reali, della convergenza).

¹ D. Kalish e R. Montague, *Logic: Techniques of Formal Reasoning*, Harcourt Brace & Co., London - New York 1964.

3.2. Deducibilità secondo Herbrand-Skolem

Un altro metodo deduttivo, che risale essenzialmente a Herbrand, è basato sul teorema di compattezza proposizionale e sulla equisoddisfacibilità tra una teoria e la sua espansione di Herbrand.

Deducibilità secondo Herbrand-Skolem

Per dimostrare che $\Phi \models \varphi$ si considera la teoria $\Phi \cup \{\neg \varphi\}$ e si dimostra che essa è insoddisfacibile considerando la teoria $\Phi' = \text{Herbrand}(\Phi \cup \{\neg \varphi\})$ che è equisoddisfacibile con $\Phi \cup \{\neg \varphi\}$. In base alla compattezza proposizionale, tale teoria è insoddisfacibile se e solo se lo è un suo sottoinsieme finito. A tal fine, basta numerare tutte le proposizioni di Φ' , diciamole $\{\varphi_1, \varphi_2, \dots, \varphi_n, \dots\}$, e verificare, tramite tavole di verità, la soddisfacibilità di $\{\varphi_1, \varphi_1 \wedge \varphi_2, \dots, \varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n, \dots\}$. La teoria proposizionale Φ' è insoddisfacibile se almeno una di tali proposizioni è sempre falsa per qualsiasi assegnamento di valori di verità. Quando ciò avviene (e deve avvenire se $\Phi \cup \{\neg \varphi\}$ è insoddisfacibile) si può concludere che $\Phi \models \varphi$.

3.3. Metodo di risoluzione

Un metodo più efficiente, basato sempre sulle forme di Skolem e sulla espansione di Herbrand, è il cosiddetto *metodo di risoluzione*. Questo dimostra l'insoddisfacibilità di un insieme di clausole aggiungendovi altre clausole deducibili con due regole (che potrebbero essere conglobate in una sola). Il procedimento prosegue fino a quando non si aggiunge la clausola vuota (che in tale contesto si indica con $\perp$). A quel punto si può concludere che l'insieme iniziale di clausole è insoddisfacibile. Indichiamo con σ una sostituzione, ovvero una funzione che associa ad ogni variabile un termine.

Sostituzione Se vi è una clausola Γ si può aggiungere Γ_σ , intendendo con ciò la sostituzione in Γ di ogni variabile x con il termine $\sigma(x)$.

Risoluzione Se vi sono due clausole del tipo

$$\begin{array}{l} \Gamma \cup \delta \\ \Psi \cup \neg \delta \end{array}$$

allora si può aggiungere la clausola detta *risolvente* delle due clausole precedenti:

$$\Gamma \cup \Psi.$$

La completezza del metodo è conseguenza del metodo di Herbrand-Skolem e della completezza del principio di risoluzione per la logica proposizionale.

Esempio 3.11 Dimostriamo con il principio di risoluzione che:

$$\models \forall x(\varphi(x) \rightarrow \psi) \rightarrow (\exists x\varphi(x) \rightarrow \psi) \\ (x \notin \text{free}(\psi)).$$

Poniamo la proposizione negata in forma prenessa e poi di Skolem:

$$\begin{aligned} & \neg [\forall x(\varphi(x) \rightarrow \psi) \rightarrow (\exists x\varphi(x) \rightarrow \psi)] \\ & \neg \exists x((\varphi(x) \rightarrow \psi) \rightarrow (\forall x(\varphi(x) \rightarrow \psi))) \\ & \neg \exists x\forall y((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(y) \rightarrow \psi)) \\ & \forall x\neg\forall y((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(y) \rightarrow \psi)) \\ & \forall x\exists y\neg((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(y) \rightarrow \psi)) \\ & \neg((\varphi(x) \rightarrow \psi) \rightarrow (\varphi(fx) \rightarrow \psi)) \\ & (\varphi(x) \rightarrow \psi) \wedge \neg(\varphi(fx) \rightarrow \psi) \\ & (\neg\varphi(x) \vee \psi) \wedge (\varphi(fx) \wedge \neg\psi). \end{aligned}$$

La forma a clausole è quindi

$$C_1 = \{\neg\varphi(x), \psi\}$$

$$C_2 = \{\varphi(fx)\}$$

$$C_3 = \{\neg\psi\};$$

sostituendo x con fx in C_1 si ottiene

$$C_4 = \{\neg\varphi(fx), \psi\};$$

risolvendo C_2 e C_4 si ottiene

$$C_5 = \{\psi\}.$$

Infine, risolvendo la terza con la quinta clausola si determina la clausola vuota.

Un caso particolare di forma a clausole si ha quando in una clausola si ha un solo letterale positivo e tutti gli altri negativi. Tali clausole si dicono più propriamente formule di tipo Horn ed equivalgono ovviamente a formule condizionali. Sulle *formule di Horn* è basata la *programmazione logica*: infatti si può dimostrare che tramite formule di questa specie si possono esprimere tutte le funzioni calcolabili (vedi più avanti la rappresentazione logica di mac-

chine di Turing). Data la grande efficienza raggiunta dagli algoritmi che realizzano la risoluzione, soprattutto in alcuni casi di formule Horn, tale principio è fondamentale negli attuali sistemi automatici di programmazione logica.

3.4. Calcolo dei sequenti

Il calcolo dei sequenti di Gentzen risulta una specie di variante notazionale del calcolo dei tableau. Più precisamente, se si scrivono le regole dei tableau in modo opportuno e si invertono le premesse con le conclusioni si ottiene una versione diretta dei tableau che coincide con il calcolo di Gentzen. Questo fatto indica la centralità del metodo dei tableau, che da una parte è naturalmente collegato alla semantica predicativa e dall'altra è anche connesso ai metodi deduttivi diretti di cui il calcolo dei sequenti costituisce la forma più strutturata e matura.

Indichiamo in modo conciso l'idea generale sottostante al passaggio dal calcolo con tableau a quello con sequenti. Bisogna innanzitutto riformulare i tableau in una forma, del tutto equivalente, in cui essi non sono più etichettati con formule, ma con insiemi di formule *marcate* con i simboli T, F (ponendo $(T : \neg \varphi) = (F : \varphi)$ e $(F : \neg \varphi) = (T : \varphi)$). Inoltre adottiamo una notazione compatta, introdotta da Smullyan, secondo cui le formule *segnate* si suddividono in quattro tipi:

1. le formule α sono le congiunzioni marcate con T o disgiunzioni marcate con F ;
2. le formule β sono disgiunzioni marcate con T o congiunzioni marcate con F ;
3. le formule γ sono quantificazioni universali marcate con T o esistenziali marcate con F ;
4. le formule δ sono esistenziali marcate con T o universali marcate con F .

Con tale notazione le regole dei tableau diventano:

1. $\alpha = (T : \varphi \wedge \psi) \Rightarrow \alpha_1 = (T : \varphi), \alpha_2 = (T : \psi)$
2. $\alpha = (F : \varphi \vee \psi) \Rightarrow \alpha_1 = (F : \varphi), \alpha_2 = (F : \psi)$
3. $\beta = (T : \varphi \vee \psi) \Rightarrow \beta_1 = (T : \varphi), \beta_2 = (T : \psi)$
4. $\beta = (F : \varphi \wedge \psi) \Rightarrow \beta_1 = (F : \varphi), \beta_2 = (F : \psi)$
5. $\gamma = (T : \forall x \varphi(x)) \Rightarrow \gamma(t) = (T : \varphi(t))$
6. $\gamma = (F : \exists x \varphi(x)) \Rightarrow \gamma(t) = (F : \varphi(t))$
7. $\delta = (T : \exists x \varphi(x)) \Rightarrow \delta(a) = (T : \varphi(a))$
8. $\delta = (F : \forall x \varphi(x)) \Rightarrow \delta(a) = (F : \varphi(a))$.

In tal modo le regole dei tableau si possono esprimere nel modo seguente, ove S indica un insieme di formule marcate e $S, \dots$ abbrevia $S \cup \{\dots\}$ (tralasciamo le regole per il trattamento dell'uguaglianza):

$$\frac{S, \alpha}{S, \alpha_1, \alpha_2} \quad \frac{S, \beta}{S, \beta_1 | S, \beta_2} \quad \frac{S, \gamma}{S, \gamma, \gamma(t)} \quad \frac{S, \delta}{S, \delta(a)}.$$

Un tableau si dice *chiuso* se tutti gli insiemi di formule marcate che etichettano le foglie sono inconsistenti (includono una formula marcata con T e la stessa formula marcata con F). Ovviamente in questa formulazione si possono omettere le regole di introduzione, ricopiatura, chiusura e doppia negazione. Il termine t che compare sopra è un qualsiasi termine chiuso, e la costante a non occorre in nessuna formula di S ed è univocamente individuata da δ .

L'equivalenza tra questa formulazione dei tableau e quella data precedentemente è un semplice esercizio di traduzione.

A questo punto, dati due insiemi di formule predicative Φ e Ψ , definiamo un *sequente* come la metaformula

$$\Phi \vdash \Psi$$

la cui lettura intuitiva è: da tutte le formule di Φ segue almeno una formula di Ψ . Una *dimostrazione tableau* per un tale sequente è un tableau chiuso che ha come radice $(T : \Phi) \cup (F : \Psi)$, ove $(T : \Phi)$ indica le formule di Φ marcate con T e $(F : \Psi)$ indica le formule di Ψ marcate con F . Ovviamente un tale tableau è chiuso se e solo se dalla teoria Φ segue logicamente almeno una proposizione della teoria Ψ . Viceversa un insieme S di formule marcate individua univocamente un sequente che indichiamo con $[S]$. Ora capovolgiamo le precedenti regole dei tableau:

$$\frac{S, \alpha_1, \alpha_2}{S, \alpha} \quad \frac{S, \beta_1 | S\beta_2}{S, \beta} \quad \frac{S, \gamma, \gamma(t)}{S, \gamma} \quad \frac{S, \delta(a)}{S, \delta}.$$

Applicando tali regole, a partire da insiemi inconsistenti di formule marcate del tipo $\{S, (T : \varphi), (F : \varphi)\}$ otteniamo un insieme S' di formule marcate sse esiste una dimostrazione-tableau del sequente $[S']$. Infatti, tali regole permettono semplicemente di capovolgere il processo di costruzione dei tableau. Se usiamo la notazione $[]$ per i sequenti, otteniamo la seguente notazione compatta per il calcolo dei sequenti, ove nella terza regola si omette γ perché, come si verifica facilmente, l'insieme marcato $S, \gamma, \gamma(t)$ è tableau-inconsistente se lo è $S, \gamma(t)$, per un opportuno t :

$$\frac{[S, \alpha_1, \alpha_2]}{[S, \alpha]} \quad \frac{[S, \beta_1] [S, \beta_2]}{[S, \beta]} \quad \frac{[S, \gamma(t)]}{[S, \gamma]} \quad \frac{[S, \delta(a)]}{[S, \delta]}.$$

Se ora riscriviamo queste regole nella notazione originale dei sequenti, esplicitando i vari tipi di formule $\alpha, \beta, \gamma, \delta$, otteniamo finalmente il calcolo di Gentzen i cui sequenti iniziali sono del tipo $\Gamma, \varphi \vdash \Delta, \varphi$:

$$\frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}$$

$$\frac{\Gamma \vdash \Delta, \varphi; \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$$

$$\frac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$$

$$\frac{\Gamma, \varphi \vdash \Delta; \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$$

$$\frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \rightarrow \psi}$$

$$\frac{\Gamma \vdash \Delta, \varphi; \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \rightarrow \psi \vdash \Delta}$$

$$\frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg \varphi}$$

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg \varphi \vdash \Delta}$$

$$\frac{\Gamma, \varphi(t) \vdash \Delta}{\Gamma, \forall x \varphi(x) \vdash \Delta}$$

$$\frac{\Gamma \vdash \Delta, \varphi(a)}{\Gamma \vdash \Delta, \forall x \varphi(x)}$$

$$\frac{\Gamma \vdash \Delta, \varphi(t)}{\Gamma \vdash \Delta, \exists x \varphi(x)}$$

$$\frac{\Gamma, \varphi(a) \vdash \Delta}{\Gamma, \exists x \varphi(x) \vdash \Delta}$$

Come dimostra Smullyan,² la notazione tableau dei sequenti permette di semplificare la dimostrazione dei classici teoremi di normalizzazione dimostrati da Gentzen e di estendere risultati fondamentali di teoria della dimostrazione.

² R. M. Smullyan, *First-Order Logic*, Springer-Verlag, Berlin 1968.

3.5. Calcoli logici equazionali

I calcoli equazionali sono i calcoli *naturali* della matematica; è quindi del tutto giustificato cercare formulazioni equazionali della logica predicativa. I calcoli logici equazionali sono essenzialmente basati sull'equivalenza logica tra formule. Indichiamola con l'uguaglianza e introduciamo i simboli 1 e 0 per indicare una tautologia e la sua negazione. A questo punto la validità logica di una proposizione φ equivale a una derivazione di $\varphi = 1$. Si tratta quindi di estendere il calcolo di Boole aggiungendo ulteriori equivalenze tra gli assiomi. La riduzione di una formula predicativa in forma prenessa è per esempio facilmente esprimibile in termini equazionali. Sviluppando una tale prospettiva si giunge a strutture algebriche che generalizzano la struttura di algebra di Boole (algebre poliadiche e cilindriche) collegandosi a temi di ricerca che sono tipici della cosiddetta *logica algebrica*. Tuttavia, forse proprio per la ricchezza delle strutture algebriche sottostanti, per tale via non si trovano calcoli equazionali completi. Un'altra *via equazionale* si collega alla teoria delle relazioni binarie, una delle prime teorie logiche sviluppate a partire da Peirce e Schröder, e coltivata poi da Tarski e dalla sua scuola americana.

Nella forma finale il calcolo di Schröder era basato su sei operazioni relazionali e quattro relazioni iniziali (su un prefissato universo):

- somma, + (unione insiemistica)
- prodotto, $\cdot$ (intersezione insiemistica)
- complemento, $-$ (differenza insiemistica)
- prodotto relativo, $|$ (composizione)
- somma relativa, $\square$ ($x(R \square S)y \Leftrightarrow \exists z(xRz \vee zSy)$)
- inversione, $^{\circ}$
- uguaglianza,
- diversità,
- relazione universale, (sempre valida)
- relazione nulla, (mai valida).

Si vede che, utilizzando tali relazioni su un universo D , si può esprimere equazionalmente una grande quantità di formule predicative su tale dominio. Per esempio la proposizione: $\forall xyz(Rxy \wedge Ryz \rightarrow Rxz)$ si esprime con l'equazione relazionale:

$$(R|R) + R = R.$$

Tuttavia anche per tale via non si riesce ad ottenere un calcolo equazionale completo, ovvero un insieme di assiomi da cui si deducano equazionalmente tutte le equazioni relazionali logicamente valide (il risultato limitativo

generale fu scoperto da Tarski nel 1941). Nonostante tali limitazioni Tarski e Givant hanno ottenuto caratterizzazioni e risultati di universalità rappresentativa per un linguaggio relazionale binario, indicato con $\mathcal{L}^\times$. Tali ricerche si collegano a un altro filone molto importante indicato come *logica combinatoria*, iniziato da Schönfinkel, Curry e Feys, a partire dagli anni Venti, che indagava sulla possibilità di eliminare le variabili vincolate nei formalismi matematici. Il lambda-calcolo e i linguaggi programmativi funzionali hanno dimostrato l'importanza di tali ricerche nello studio di formalismi di calcolo potenti e del tutto generali.

Una formulazione equazionale completa della logica predicativa si ottiene estendendo il calcolo relazionale al caso generale di relazioni di qualsiasi arietà e introducendo ulteriori operazioni relazionali: i) il prodotto cartesiano $R \times S$ in cui le sequenze che soddisfano il prodotto sono la concatenazione di due sequenze, la prima delle quali soddisfa R e la seconda soddisfa S ; ii) le proiezioni, ove $(\Pi_i R)x \Leftrightarrow R(\dots, x, \dots)$ con x in posizione i (le relazioni universali e vuote vanno naturalmente considerate per tutte le arietà).

Tale algebra (sistema di operazioni) relazionale è alla base della teoria relazionale delle basi di dati in cui un *record* è essenzialmente una k -pla di valori e una tabella come insieme di record è proprio una relazione. Una *query* consiste nel chiedere se un certo record appartiene a una tabella derivata da quelle primitive applicando una certa sequenza di operazioni riconducibili a quelle relazionali prima descritte. La teoria relazionale dei dati, sviluppata a partire dai lavori di Codd, risulta quindi un'applicazione del punto di vista logico relazionale.

Un'altra soluzione consiste in una trascrizione equazionale dei calcoli assiomatici. Si introduce un *operatore deduttivo* δ tale che intuitivamente $\delta(\varphi)$ indichi il valore di verità della proposizione φ (o, più in generale, un valore in un'algebra di Boole, o in strutture ancora più generali). A questo punto, indicando con $+$, $\cdot$, $'$, 0 , 1 la segnatura booleana, si pone in un'algebra di Boole $x \leq y$ se $x + y = y$. Quindi il calcolo assiomatico di Hilbert ha un'immediata riformulazione equazionale laddove si ponga $\delta(\varphi) = 1$ per ogni assioma φ di tale calcolo e si esprima la regola di modus ponens nella forma

$$\delta(\varphi) \cdot \delta(\varphi \rightarrow \psi) \leq \delta(\psi).$$

Per tale via si scoprono profondi legami tra teoremi della logica predicativa e teoremi di algebra universale (per esempio, tra il teorema di completezza della logica predicativa e il teorema di completezza di Birkhoff per la logica equazionale).

3.6. Tipologia dei calcoli logici

Tutti i metodi deduttivi considerati in questo paragrafo, insieme a quello basato sui tableau analitici, per quanto completamente formali, sono ben lungi dal potere essere direttamente automatizzati. Infatti, essi forniscono regole deduttive, ma non indicano con quali criteri tali regole vanno applicate per ottenere una specifica deduzione. In altre parole, la *strategia* con cui applicare le regole per ottenere un risultato desiderato non è esplicitata. Dagli esempi forniti si possono trarre suggerimenti per operare in casi analoghi, ma tali suggerimenti sottintendono l'intelligenza umana. Un sistema deduttivo automatico che abbia delle prestazioni accettabili, seppure basato su tali metodi, deve sviluppare teorie e tecniche di programmazione che rendano efficiente il suo comportamento. In definitiva, la teoria della dimostrazione costituisce il primo e necessario passo verso il progetto leibniziano di un *calculus ratiocinator*, ma altri passi fondamentali occorrono per giungere a una realizzazione effettiva di un tale progetto in reali casi specifici.

In definitiva, i calcoli logici possono essere raggruppati nei seguenti tipi:

- calcoli assiomatici (Hilbert-Frege);
- calcoli analitici (metodo dei tableau);
- calcoli espansivi (Herbrand-Skolem);
- calcoli espansivi con risoluzione (A. J. Robinson);
- calcoli naturali (deduzione naturale);
- calcoli naturali con sequenti (Gentzen);
- calcoli equazionali (estensioni predicative del calcolo di Boole).

I calcoli del penultimo tipo aggiungono un'ulteriore livello di strutturazione. Infatti le regole stabiliscono direttamente, tramite sequenti, una relazione di deducibilità. La relazione di deducibilità del calcolo di deduzione naturale poteva essere definita direttamente riformulando le regole con particolari sequenti del tipo $\Phi \vdash \varphi$ (ove Φ è una teoria e φ una proposizione) che sono da considerare appunto come una sorta di *metaformule*. Per esempio, utilizzando il sequente $\Phi \vdash \varphi$, la regola della deduzione naturale di introduzione del connettivo di congiunzione si formula ponendo:

$$\frac{\Phi \vdash \varphi, \Phi \vdash \psi}{\Phi \vdash \varphi \wedge \psi}$$

Analogamente l'introduzione dell'implicazione si esprime con

$$\frac{\Phi, \varphi \vdash \psi}{\Phi \vdash \varphi \rightarrow \psi}$$

I calcoli assiomatici e il calcolo di deduzione naturale (come quello dei sequenti) sono diretti perché *generano* le formule logicamente valide. I calcoli analitici sono inversi, ovvero confutativi: cercano di provare l'insoddisfacibilità della negata di una proposizione data, generando una contraddizione tra proposizioni meno complesse di quella di partenza. I calcoli espansivi sono anch'essi confutativi, generano una teoria proposizionale equisoddisfacibile con la negata della proposizione data, e cercano di provarne l'insoddisfacibilità determinando una contraddizione tra proposizioni generate in tale teoria. La risoluzione introduce un meccanismo di *contrazione* che consiste nel rendere efficiente il metodo espansivo generando proposizioni, ma cercando contemporaneamente di ridurre la complessità delle proposizioni tra cui si cerca di trovare l'assurdo.

I calcoli logici procedono comunque generando formule, ma la generazione ha nei vari casi scopi, modalità e direzioni diverse.

I calcoli assiomatici, naturali e su sequenti generano proposizioni o derivazioni valide partendo dagli assiomi o dalle ipotesi.

I calcoli analitici generano sottoformule della proposizione (o delle proposizioni) di partenza, frammentandole in componenti sempre più elementari (per giungere a contraddizione).

I calcoli espansivi generano proposizioni in cui le proposizioni di partenza, una volta poste in forma prenessa, si espandono in proposizioni dove le variabili sono rimpiazzate da termini di complessità crescente. Aggiungendo un'ulteriore fase, di contrazione, si generano sottoformule delle formule precedentemente generate.

I calcoli assiomatici e quelli naturali sono entrambi diretti, ma nei secondi si hanno regole per ciascun operatore logico e ipotesi piuttosto che assiomi. I calcoli naturali e quelli su sequenti hanno una struttura ipotesi/regole, con regole per ciascun operatore logico, ma nei calcoli naturali si hanno regole di introduzione e di eliminazione, mentre nei calcoli su sequenti si hanno solo regole di introduzione; questo conferisce loro un carattere sintetico, analogo e opposto al carattere analitico dei tableau, ovvero, tramite sequenti si generano le derivazioni valide procedendo da formule meno complesse a formule sempre più complesse.

I calcoli logici equazionali sono in un certo senso un tipo a parte e come si è visto si collegano a nozioni del tutto generali di calcolo, all'eliminazione delle variabili vincolate o all'algebra universale.

Per una relazione di deducibilità $\vdash$ si possono definire le seguenti condizioni del tutto generali.

Definizione 3.1

1. *Correttezza*: $\vdash \leq \models$
2. *Completezza*: $\models \leq \vdash$

- 3. *Finitezza*: $\Phi \vdash \varphi \Rightarrow \exists \Delta \subseteq \Phi, |\Delta| \in \omega : \Delta \vdash \varphi$
- 4. *Monotonia*: $\Psi \vdash \varphi, \Psi \subset \Phi \Rightarrow \Phi \vdash \varphi$
- 5. *Taglio*: $\Phi \vdash \varphi, \Phi \cup \{\varphi\} \vdash \psi \Rightarrow \Phi \vdash \psi$
- 6. *Modus ponens*: $\Phi \cup \{\varphi, \varphi \rightarrow \psi\} \vdash \psi$
- 7. *Deduzione*: $\Phi \cup \{\varphi\} \vdash \psi \Rightarrow \Phi \vdash \varphi \rightarrow \psi$.

Proposizione 3.2 *Siano $\vdash_1$ e $\vdash_2$ due relazioni di deducibilità. Se $\vdash_1 \leq \vdash_2$ e $\vdash_1$ è completa, allora anche $\vdash_2$ è completa.*

Dimostrazione $\Phi \models \varphi \Rightarrow \Phi \vdash_1 \varphi \Rightarrow \Phi \vdash_2 \varphi$.

Corollario 3.1 *Se $\vdash_2$ è corretta, allora è corretta e completa, ovvero coincide con $\models$.*

Concludiamo il paragrafo con una tabella che evidenzia i vari livelli in cui l'implicazione occorre nella logica predicativa. Il *se, allora* si riferisce alla relazione (informale) di base con cui si concatenano le proposizioni di una dimostrazione matematica.

Tabella 3.1 I livelli dell'implicazione

$\rightarrow$	connettivo
---	regola
$\vdash$	deduzione
-----	metaregola
$\models$	conseguenza
$\Rightarrow$	se, allora
$\Rightarrow\Rightarrow$	dimostrazione

Nelle dimostrazioni matematiche intervengono comunque una serie di strumenti di supporto che sono fondamentali per strutturare e potenziare i meccanismi deduttivi e per costruire teorie che siano organicamente sviluppate intorno a certi ambiti concettuali: assiomi, definizioni, abbreviazioni, proposizioni, lemmi, teoremi, corollari, interpretazioni e diagrammi.

Le dimostrazioni formali sono un tipo particolare di dimostrazioni matematiche, quelle strutturabili entro opportuni sistemi simbolici. Come vedremo, nell'ultima parte di questo testo, nessun sistema formale può completamente racchiudere tutta la potenza delle dimostrazioni matematiche, che quindi rimangono essenzialmente prodotti dell'ingegno e della creatività umana. Tuttavia è interessante studiarne la struttura simbolica, alla ricerca di sistemi formali sempre più potenti e adatti alle esigenze dei vari

contesti applicativi. In un certo senso, gran parte della ricerca logica è rivolta alla determinazione e allo studio di forme implicative sempre più versatili e alla loro formalizzazione. Il testo di logica elementare di Tarski³ presenta un'analisi semplice e tuttavia molto interessante di varie forme di implicazione che emergono in svariati contesti.

I calcoli logici sono comunque, oltre che strumenti deduttivi, paradigmi di calcolo in senso lato. Ad essi si ispirano direttamente buona parte dei metodi formali nella definizione dei modelli di calcolo. Per esempio, la cosiddetta *semantica operativa* strutturata nella semantica dei linguaggi programmativi è un'adattamento del metodo dei sequenti alla descrizione formale dei costrutti dei linguaggi di programmazione. Analogamente, la ben nota corrispondenza *proposizioni-tipi* è una formulazione in termini di calcoli logici di algoritmi per la verifica di correttezza di programmi. La stessa definizione dei sistemi di Post, un formalismo di grande generalità nella definizione di sintassi ed elaborazioni simboliche, non è altro che una versione astratta e finitista dei sistemi assiomatici di Hilbert. Le teorie monoidali che presenteremo più avanti costituiscono una generalizzazione logica dei sistemi di Post. Gli esempi che forniremo di teorie monoidali dimostrano la versatilità del paradigma logico nella rappresentazione dei sistemi simbolici e la naturalezza con cui qualsiasi calcolo può essere rappresentato, entro un'opportuna teoria, tramite un calcolo logico. Infine i calcoli logici equazionali si collegano ai sistemi di manipolazione di termini algebrici, alla logica combinatoria e ai formalismi funzionali, strumenti essenziali nello studio e nella definizione di formalismi per la specifica di dati e la realizzazione di calcoli su di essi.

³ Tarski, *Introduzione alla logica* cit.

Capitolo 4

Rappresentabilità logica

Nelle pagine precedenti abbiamo considerato vari esempi di formalizzazione logica in cui proposizioni, proprietà e relazioni venivano espresse tramite formule della logica predicativa. La determinazione di formule che esprimano simbolicamente certi fatti è preliminare a qualsiasi procedimento deduttivo; inoltre, spesso, la rappresentazione simbolica costituisce una comprensione più profonda di quanto si rappresenta. Scrivere in formule significa usare funzioni e relazioni di base combinandole tramite connettivi e quantificatori. Tale processo è una riduzione di descrizioni complesse in termini di forme espressive primitive prescelte. In un certo senso, è un'attività che ha molti punti in comune con quella di esprimere un algoritmo in un dato linguaggio di programmazione. Infatti, in questo caso si rappresentano i dati con le strutture dati del linguaggio prescelto e la strategia di calcolo con i costrutti di controllo del linguaggio.

In questo capitolo analizziamo vari aspetti della rappresentabilità logica. Il punto di partenza di questa analisi sono le seguenti definizioni di insieme rappresentabile in un dato modello, o in una data teoria.

Definizione 4.1 *Sia dato un Σ -modello $\mathcal{M}$; una Σ -formula $\varphi(x)$ (con variabile libera x) rappresenta un sottoinsieme A del dominio di $\mathcal{M}$ se vale la seguente equivalenza:*

$$a \in A \Leftrightarrow \mathcal{M} \models \varphi(a).$$

Definizione 4.2 *Data una segnatura Σ e un insieme T di termini chiusi su Σ , T è rappresentato da una Σ -formula $\varphi(x)$ nella Σ -teoria Φ se vale la seguente equivalenza:*

$$t \in T \Leftrightarrow \Phi \models \varphi(t).$$

Le definizioni precedenti si estendono al caso di relazioni k -rie su D considerando formule con k variabili libere.

4.1. Modelli e teorie

Presentiamo nel seguito alcuni modelli e teorie di notevole interesse ai fini della rappresentabilità logica. Per non appesantire le notazioni non distingueremo i simboli di una segnatura con le loro interpretazioni nei modelli. In base al contesto si capirà se un simbolo è da considerarsi nella sua accezione *autoreferenziale* (in tal caso si dice anche “menzionato”) oppure *referenziale* (in tal caso si dice anche “usato”).

Esempio 4.1 (aritmetica standard) Il modello aritmetico standard AR è il seguente modello sull'insieme ω dei naturali con la somma, il prodotto, lo zero e uno:

$$\text{AR} = (\omega, +, \cdot, 0, 1).$$

Esempio 4.2 (sequenze finite di naturali) Il modello SEQ è il seguente modello sull'insieme ω^* delle sequenze finite di naturali con la concatenazione (indicata come sempre giustapponendo gli argomenti), la lunghezza di una parola, lo zero e la parola vuota (i numeri sono parole di lunghezza unitaria):

$$\text{SEQ} = (\omega^*, --, ||, 0, \lambda).$$

Esempio 4.3 (aritmetica di Peano) La seguente è la teoria PA dell'aritmetica di Peano nella segnatura $\{+, \cdot, 0, 1\}$. Si noti che l'ultimo assioma è uno schema di assiomi che esprime il principio di induzione, ove $\varphi(x)$ varia nell'insieme delle formule predicative con una variabile libera x :

$$\forall x \neg (0 = x + 1)$$

$$\forall xy (x + 1 = y + 1 \rightarrow x = y)$$

$$\forall x (x + 0 = x)$$

$$\forall xy (x + (y + 1) = (x + y) + 1)$$

$$\forall x (x \cdot 0 = 0)$$

$$\forall xy (x \cdot (y + 1) = (x \cdot y) + x)$$

$$(\varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(x + 1))) \rightarrow \forall x \varphi(x).$$

Notiamo che se nell'esempio precedente formulassimo l'ultima proposizione (principio di induzione) utilizzando una variabile P che varia su tutte le proprietà dei numeri naturali, allora l'assioma corrispondente non sarebbe più uno schema di assiomi, ma un singolo assioma:

$$\forall P[(P(0) \wedge \forall x(P(x) \rightarrow P(x+1))) \rightarrow \forall x P(x)].$$

Tale cambiamento non è un semplice cambiamento linguistico, ma equivale al passaggio dalla logica predicativa del *primo ordine* a una logica predicativa di *secondo ordine* (con variabili quantificate non solo sul dominio, ma sulle parti di esso). Si dimostra che in tal modo la caratterizzazione dell'aritmetica è univoca, ovvero, ogni modello che soddisfa gli assiomi di Peano al secondo ordine è *isomorfo* (vedi oltre) all'algebra standard dei naturali, quindi essenzialmente identico a tale struttura a meno di cambiamenti notazionali. A questo punto cadono tutti gli effetti patologici introdotti dai teoremi di Skolem (modelli non standard con cardinalità arbitrarie). Ovviamente, come sempre, questi aspetti positivi sono accompagnati da controparti negative: si dimostra che una logica del secondo ordine non può avere un calcolo deduttivamente completo. Tale fenomeno mette in luce una caratteristica del tutto generale dei formalismi logici, che si presenta in varie forme e in svariati contesti: *vi è un bilancio tra potenza deduttiva e potenza rappresentativa dei linguaggi logici*. Se un linguaggio guadagna nel primo aspetto, allora si indebolisce nell'altro e viceversa. Tutto non si può avere, neppure in logica! Bisogna sapersi accontentare e scegliere in base alle circostanze!

Esempio 4.4 (aritmetica di R. Robinson) L'aritmetica di Robinson è la teoria RR con la stessa segnatura dell'aritmetica di Peano e i seguenti schemi di assiomi ($n = 0 + 1 + \dots + 1$, n volte; analogamente per m e k)

$$n + k = m \quad \text{sse } (n + k = m) \in \text{Diag}(AR)$$

$$n \cdot k = m \quad \text{sse } (n \cdot k = m) \in \text{Diag}(AR)$$

$$\neg n = m \quad \text{per ogni } n \neq m \in \omega$$

$$\forall xy(x \leq y \leftrightarrow \exists z(x + z = y))$$

$$\forall x(x \leq n \leftrightarrow (x = 0 \vee x = 1 \vee \dots \vee x = n)) \quad \text{per ogni } n \in \omega.$$

Esercizio 4.1 Si estenda PA con gli elementi di ω e si aggiungano simboli opportuni e assiomi per rappresentare le operazioni di prodotto, potenza, fattoriale e la relazione di divisibilità.

Diamo qui di seguito alcuni esempi di notevoli teorie algebriche, i cui modelli costituiscono l'argomento centrale dell'algebra astratta. I sistemi nu-

merici con le usuali operazioni, i polinomi, le funzioni su un insieme e le matrici numeriche sono modelli di alcune delle teorie che seguono, e cioè le teorie MN, GR, GA, SAN, AN, CR. Nel seguito le variabili si intendono implicitamente quantificate universalmente.

Esempio 4.5 Teoria MN (dei monoidi). Segnatura: e costante, concatenazione come simbolo di funzione binaria; assiomi:

$$(xy)z = x(yz)$$

$$xe = x$$

$$ex = x.$$

Esempio 4.6 Teoria GR (dei gruppi). Segnatura come per MN, più un simbolo $'$ di funzione unaria; assiomi come per MN, più i seguenti:

$$xx' = e$$

$$x'x = e.$$

Esempio 4.7 Teoria GA (dei gruppi abeliani). Assiomi come per GR, con 0 al posto di e , $+$ al posto della concatenazione, più il seguente:

$$x + y = y + x.$$

Esempio 4.8 Teoria SAN (dei semianelli). Due simboli di funzione binaria e due costanti 0 e 1; assiomi come per MN per $+$, 0, più i seguenti:

$$(x + y) = (y + x)$$

$$(xy)z = x(yz)$$

$$x1 = x$$

$$1x = x$$

$$x(y + z) = (xy) + (xz)$$

$$(x + y)z = (xz) + (yz)$$

$$0x = 0$$

$$x0 = 0.$$

Esempio 4.9 Teoria AN (degli anelli). Assiomi come per GA (con due simboli di funzione binaria e due costanti 0, 1), più i seguenti:

$$(xy)z = x(yz)$$

$$x1 = x$$

$$1x = x$$

$$x(y + z) = (xy) + (xz)$$

$$(x + y)z = (xz) + (yz).$$

Esempio 4.10 Teoria CR (dei corpi). Segnatura e assiomi come per AN, con in più gli assiomi:

$$xy = yx$$

$$\neg 0 = 1$$

$$\neg x = 0 \rightarrow \exists y(xy = 1).$$

Esempio 4.11 Teoria CR_p (dei corpi di caratteristica p , con p primo). Segnatura e assioma come per CR, con in più l'assioma $p = 0$.

Esempio 4.12 La seguente teoria assiomatizza i grafi semplici orientati su cui è definita una relazione binaria di connessione. La segnatura ha un predicato binario E che esprime la connessione tra due nodi con un arco diretto e la relazione binaria C di connessione tra due nodi attraversati da un cammino:

$$\forall xy(Exy \rightarrow Cxy)$$

$$\forall xyz(Cxy \wedge Eyz \rightarrow Cxz)$$

$$\forall xyz(Ezx \wedge Cxy \rightarrow Czy).$$

Esercizio 4.2 Si diano teorie predicative per:

- multigrafi;
- grafi e multigrafi non orientati;
- alberi e alberi radicati;
- ordinamenti lineari e densi senza massimo e minimo;
- reticoli;
- corpi algebricamente chiusi;
- spazi vettoriali.

Esempio 4.13 La seguente teoria assiomatizza le sequenze su un prefissato insieme di elementi (predicato El) con le operazioni e relazioni di concatenazione (giustapposizione), prefisso ($Pref$), suffisso ($Suff$), sottosequenza (Sub):

$$\forall xyz((xy)z = x(yz))$$

$$\exists y \forall x(xy = x \wedge yx = x)$$

$$\forall x(El(x) \rightarrow Pref(x, x))$$

$$\forall xyz(\text{Pref}(x, y) \rightarrow \text{Pref}(zx, zy))$$

$$\forall x(\text{El}(x) \rightarrow \text{Suff}(x, x))$$

$$\forall xyz(\text{Suff}(x, y) \rightarrow \text{Suff}(xz, yz))$$

$$\forall xyz \text{ Sub}(y, xyz).$$

Esercizio 4.3 *Si diano teorie predicative per:*

1. *pile su un prefissato insieme E , con le tipiche relazioni delle pile (essere elemento in testa a una pila, differire solo per la rimozione o l'aggiunta dell'elemento di testa);*
2. *code su un prefissato insieme E , con le tipiche relazioni delle code (essere l'elemento di coda, differire solo per l'aggiunta o la rimozione dell'elemento di coda);*
3. *liste concatenate su un prefissato insieme E (nil è una lista e, per ogni lista l , $\text{val}(l) \in E$ e $\text{pointer}(l)$ è una lista) con le tipiche relazioni delle liste (differire per l'aggiunta e rimozione di un elemento in una data posizione).*

Estendiamo PA con il simbolo $\leq$ per indicare l'usuale relazione di ordinamento sui numeri:

$$x \leq y \leftrightarrow \exists z(x + z = y).$$

Nella segnatura di PA così estesa definiamo la classe delle formule aritmetiche Σ_1 come quelle formule che poste in forma prenessa hanno esternamente quantificazioni esistenziali e se queste sono seguite da quantificazioni universali le variabili quantificate universalmente sono limitate. Per esempio, se x è una variabile quantificata universalmente, la formula ha una struttura del tipo $\exists y \dots \forall x \dots (\dots x \leq t \rightarrow \dots)$ per qualche termine t (in generale le formule logiche poste in forma prenessa possono essere classificate in relazione al loro prefisso di quantificatori, o anche al tipo di alternanza dei quantificatori: $\exists, \forall, \exists\forall, \forall\exists, \exists\forall\exists, \dots$ stabilendo in tal modo delle gerarchie di complessità logica).

Un risultato fondamentale riguardante la classe di formule Σ_1 è la seguente proposizione dovuta a Gödel.

Proposizione 4.1 (teorema di Σ_1 -completezza) *Le teorie PA e RR sono Σ_1 -complete rispetto al modello aritmetico standard, ovvero, per ogni $\varphi \in \Sigma_1$:*

$$\text{PA} \models \varphi \Leftrightarrow \text{AR} \models \varphi$$

$$\text{RR} \models \varphi \Leftrightarrow \text{AR} \models \varphi.$$

Si dimostra che la classe dei sottoinsiemi di naturali rappresentabili entro AR (o PA o RR) con formule di Σ_1 (con una variabile libera) coincide con la classe RE degli insiemi ricorsivamente enumerabili, ovvero generati (o riconosciuti), previa codifica dei numeri, da macchine di Turing (vedi oltre).

Un risultato fondamentale dimostrato da Jurij Matijasevič nel 1970 è la cosiddetta irrisolubilità del *decimo problema di Hilbert*. Tale problema può essere così formulato. Consideriamo un polinomio $P(a_1, \dots, a_m, x_1, \dots, x_n)$ a coefficienti interi positivi con n variabili e m parametri letterali. I valori di tali parametri per cui l'equazione $P(a_1, \dots, a_m, x_1, \dots, x_n) = 0$ ha soluzioni intere costituiscono un insieme di m -ple che si dice *diofanteo* (dal matematico greco Diofanto che studiò per primo). La questione posta da Hilbert concerne la ricerca di un metodo generale per decidere se, dati i valori degli m parametri, l'equazione corrispondente è risolubile, ovvero se la m -pla di tali valori appartiene al relativo insieme diofanteo. Matijasevič rispose negativamente, dimostrando che la classe degli insiemi diofantei coincide con la classe degli insiemi aritmeticamente rappresentabili in Σ_1 e quindi con RE. Poiché esistono (come vedremo) insiemi in RE che non sono "decidibili" si giunge facilmente alla conclusione di irrisolubilità generale del decimo problema di Hilbert.

Esercizio 4.4 *Data un'equazione diofantea con m parametri, si estenda opportunamente PA per rappresentare l'insieme delle m -ple di naturali per cui l'equazione ha soluzioni nei numeri naturali.*

Esempio 4.14 La teoria SS (della *sintassi standard*), ispirata all'aritmetica di Robinson RR, è il diagramma del modello SEQ.

Esempio 4.15 La teoria aritmetica Q, dovuta ancora a R. Robinson, consiste dei seguenti assiomi (la segnatura è evidente):

$$\forall x \neg (0 = x + 1)$$

$$\forall xy (x + 1 = y + 1 \rightarrow x = y)$$

$$\forall x (x + 0 = x)$$

$$\forall xy (x + (y + 1) = (x + y) + 1)$$

$$\forall x (x \cdot 0 = 0)$$

$$\forall xy (x \cdot (y + 1) = (x \cdot y) + x)$$

$$\forall xy (x \leq y \leftrightarrow \exists z (x + z = y))$$

$$\forall x (\neg x = 0 \rightarrow \exists y (x = y + 1)).$$

Esempio 4.16 La teoria assiomatica degli insiemi ZF (dovuta a Zermelo e Fraenkel, con apporti fondamentali di Skolem), consente di esprimere formalmente quasi tutte le teorie matematiche. La sua segnatura è quella dei simboli insiemistici (appartenenza, insieme vuoto, inclusione, ...). Ne daremo qui di seguito gli assiomi, omettendo le definizioni di simboli ausiliari (inclusione, intersezione, parentesi di singoletto e di applicazione funzionale, freccia di funzionalità, simbolo di cardinalità e di ordinamento stretto tra le cardinalità). Tutti gli assiomi si potrebbero esprimere, anche se in modo meno leggibile, utilizzando solo il simbolo di appartenenza. In senso più stretto, si indica con ZF la teoria costituita dai primi nove assiomi e più propriamente con ZFC quella costituita dai primi dieci. L'ultimo assioma corrisponde alla cosiddetta ipotesi generalizzata del continuo e in genere si considera a parte. Le formule φ , ψ sono variabili sintattiche sulle formule predicative rispettivamente con una e con due variabili (nella segnatura considerata). Tutte le lettere latine minuscole sono variabili. Tutti gli assiomi che seguono, tranne quelli di fondazione e rimpiazzamento, sono stati già ampiamente considerati nel capitolo iniziale. L'assioma di fondazione (8) assicura che non vi siano catene di appartenenze che possano regredire all'infinito (eventualmente ciclicamente): $x_1 \ni x_2 \ni x_3 \ni \dots$ (una catena del genere avrebbe intersezione non vuota con ciascuno dei suoi elementi). L'assioma di rimpiazzamento (9), introdotto da Fraenkel ci dice che si può costruire un insieme utilizzando un predicato $\varphi(t, z)$ funzionale rispetto a t (soddisfatto da valori distinti di z in corrispondenza a valori distinti di t): si fa variare t su un insieme già dato e si raccolgono tutti i corrispondenti valori di z in un nuovo insieme. In altri termini, indicando con F l'operazione individuata da ψ , l'assioma postula che la classe $\{F(y) | y \in x\}$ è un insieme (notare la differenza con l'insieme $\{y \in x | \varphi(y)\}$). Si tratta di un enunciato molto forte dal punto di vista esistenziale, utilizzato implicitamente quando si costruisce l'unione di una famiglia di insiemi. L'assioma di separazione (3) diventa un caso particolare del rimpiazzamento se si pone $\psi(t, z) \equiv t = z \wedge \varphi(z)$.

1. $\forall xy(x = y \leftrightarrow \forall z(z \in x \leftrightarrow z \in y))$ (estensionalità)
2. $\forall x(\neg x \in \emptyset)$ (vuoto)
3. $\forall x\exists y\forall z(z \in y \leftrightarrow z \in x \wedge \varphi(z))$ (separazione)
4. $\forall xyz(z \in \{x, y\} \leftrightarrow z = x \vee z = y)$ (coppia)
5. $\forall y(y \in \bigcup x \leftrightarrow \exists z(y \in z \wedge z \in x))$ (unione)
6. $\forall xy(x \in \mathcal{P}(y) \leftrightarrow x \subseteq y)$ (potenza)
7. $\exists z(\emptyset \in z \wedge \forall x(x \in z \rightarrow x \cup \{x\} \in z))$ (infinito)
8. $\forall x(\neg(x = \emptyset) \rightarrow \exists y(y \in x \wedge x \cap y = \emptyset))$ (fondazione)
9. $\forall x\exists! y\psi(x, y) \rightarrow \forall x\exists y\forall z(z \in y \leftrightarrow \exists t(t \in x \wedge \psi(t, z)))$ (rimpiazzamento)

10. $\forall x(\neg(\emptyset \in x) \rightarrow \exists f(f: x \rightarrow \bigcup x \wedge \forall y(y \in x \rightarrow f(y) \in y)))$ (scelta)
11. $\forall x \neg \exists y(|x| < |y| \wedge |y| < |\mathcal{P}(x)|)$ (continuo)

Diamo ora degli esempi di rappresentabilità entro modelli.

Esempio 4.17 Rappresentiamo in AR le seguenti relazioni e proprietà aritmetiche:

1. x è minore o uguale a y :

$$\exists z(x + z = y)$$

2. x è primo:

$$\forall yz(\neg x = 0 \wedge \neg x = 1 \wedge (x = y \cdot z \rightarrow x = y \vee x = z))$$

3. y è un numero primo maggiore di x (Prim(x) è la formula precedente):

$$\text{Prim}(y) \wedge y > x$$

4. x è un numero pari diverso da 2:

$$\exists y(x = y + y \wedge \neg x = 1 + 1)$$

Se $\varphi(x)$ è la formula del punto precedente, allora la famosa congettura di Goldbach: *Ogni pari diverso da 2 è somma di due primi* può essere espressa nel modo seguente:

$$\forall x(\varphi(x) \rightarrow \exists uv(\text{Prim}(u) \wedge \text{Prim}(v) \wedge x = u + v))$$

Esempio 4.18 Esprimiamo nel linguaggio della logica predicativa che, dati tre numeri consecutivi non nulli: i) almeno uno di essi è divisibile per 3; ii) la loro somma è divisibile per 3.

Consideriamo le seguenti formule:

$\varphi(x, y, z)$:

$$\exists w(x + y + z = (1 + 1 + 1)w)$$

$\psi(x, y, z)$:

$$\exists w(x = (1 + 1 + 1)w \vee y = (1 + 1 + 1)w \vee z = (1 + 1 + 1)w)$$

A questo punto le proposizioni diventano:

- I. $\forall xyz(y = x + 1 \wedge z = y + 1 \rightarrow \varphi(x, y, z))$
- II. $\forall xyz(y = x + 1 \wedge z = y + 1 \rightarrow \psi(x, y, z))$.

Si può generalizzare questo metodo per esprimere che, dati n numeri consecutivi non nulli, almeno uno di essi è divisibile per n ?

Gli esempi che seguono permettono di formalizzare concetti intrinsecamente legati alla nozione di sequenza, quindi il loro modello di riferimento naturale è SEQ.

Esempio 4.19 Rappresentiamo nel modello SEQ le seguenti relazioni.

1. $n = 1$

$$n = |0|$$

2. $\alpha(i) = n$

$$\exists zw(\alpha = znw \wedge |n| = 1 \wedge |zn| = i)$$

3. $\alpha \leq \beta$ (α è prefisso di β)

$$\exists z(\alpha z = \beta)$$

4. $x \leq y$

$$\exists \alpha \beta (x = |\alpha| \wedge y = |\beta| \wedge \alpha \leq \beta)$$

5. $x \in \alpha$

$$\exists i(1 \leq i \wedge i \leq |\alpha| \wedge x = \alpha(i))$$

L'esempio che segue esprime relazioni più complesse tra sequenze numeriche.

Esempio 4.20 Rappresentiamo nel modello SEQ le seguenti relazioni.

1. In α il numero n occorre m volte (in simboli $|\alpha|_n = m$)

$$\begin{aligned} &\exists v(|v| = m \wedge (1 \leq i \wedge i \leq m \rightarrow \alpha(v(i)) = n)) \\ &\wedge \forall i(\alpha(i) = n \rightarrow \exists j(v(j) = i)) \end{aligned}$$

2. α è permutazione di β

$$|\alpha| = |\beta| \wedge \forall x (x \in \alpha \rightarrow |\alpha|_x = |\beta|_x)$$

3. α è una sequenza ordinata di numeri

$$\forall ij (i \leq j \wedge 1 \leq i \wedge j \leq |\alpha| \rightarrow \alpha(i) \leq \alpha(j))$$

Il modello SEQ nonostante abbia una semplice struttura di monoide ha una formidabile potenza rappresentativa, ovvero tutta l'aritmetica può essere naturalmente descritta entro di esso. Il seguente esempio mostra le idee che stanno alla base di una tale possibilità.

Esempio 4.21 Si rappresentino nel modello SEQ le operazioni aritmetiche di somma e prodotto.

– n è la somma di m e k

$$\exists xy (|x| = m \wedge |y| = k \wedge |xy| = n)$$

– n è il prodotto di m e k

$$\exists x (|x| = m \wedge x(1) = k \wedge x(m) = n \wedge \forall i (1 \leq i \wedge i < m \rightarrow x(i+1) = x(i) + k))$$

Esercizio 4.5 Rappresentare in SEQ che n è il fattoriale di m .

La funzione β , introdotta da Gödel, è definita come:

$$\beta(c, d, i) = \text{Rem}(c, id + d + 1)$$

ove $\text{Rem}(n, m)$ indica il resto della divisione di n per m . Vale la seguente importante proprietà che è conseguenza di un notevole teorema aritmetico noto come *teorema cinese del resto*.

Proposizione 4.2 Data una sequenza α di n numeri naturali, esistono sempre due naturali c, d tali che $\beta(c, d, 0) = n$ e per $1 \leq i \leq n$ vale: $\beta(c, d, i) = \alpha(i)$.

Esercizio 4.6 Utilizzando la funzione β di Gödel si rappresenti in AR la relazione $n = a^m$. Si rappresentino quindi in AR anche le seguenti relazioni:

- n è l' i -esimo numero primo nella successione naturale dei primi
- k è l'esponente di m nella fattorizzazione in primi di n .

4.2. Linguaggi formali

Un *monoide* è determinato da un insieme M su cui è definita un'operazione binaria associativa $\cdot$ e che contiene un elemento neutro e , indifferente rispetto a tale operazione ($e \cdot x = x \cdot e = x$, $\forall x \in M$). Dato un *alfabeto* finito A le stringhe su tale alfabeto costituiscono l'insieme A^* , detto anche *universo linguistico* su A . Tale insieme è naturalmente dotato di una struttura di monoide, detto *monoide libero* su A , in cui l'operazione binaria è la concatenazione tra stringhe e l'elemento neutro è la stringa nulla λ . Un *linguaggio* sull'alfabeto A è un sottoinsieme di A^* .

Tra i linguaggi, in quanto insiemi, si possono applicare le usuali operazioni insiemistiche di *unione* (spesso denotata con $+$), *intersezione* e *complemento*. Un *morfismo* tra due linguaggi è una funzione f tale che $f(xy) = f(x)f(y)$. Dato un linguaggio L , $f(L)$ è il linguaggio le cui stringhe sono immagini di stringhe di L secondo f . Una *codifica* di un linguaggio in un altro è una funzione iniettiva dal primo al secondo. Ricordiamo che ogni linguaggio può essere codificato in un linguaggio sull'alfabeto binario 0, 1 e in un linguaggio sull'alfabeto unario 1 (ovvero in un insieme di naturali).

La nozione di linguaggio sta alla matematica discreta come quella di insieme sta a tutta la matematica. Utilizzando un aforisma potremmo dire che se in matematica tutto è insieme, nella matematica discreta tutto è linguaggio.

In senso lato, una struttura discreta è qualcosa in ultima analisi rappresentabile con un linguaggio (o con più linguaggi) e una struttura discreta finita qualcosa che si può rappresentare con una stringa (o con un linguaggio finito).

Questo giustifica l'interesse teorico per i linguaggi e le classi di linguaggi, i metodi per definirli e le loro caratteristiche algebriche e computazionali. La *teoria dei linguaggi formali*, sviluppatasi a partire dai primi anni del Novecento, ha dimostrato una centralità sorprendente nelle teorie matematiche della computazione e quindi in tutta l'informatica teorica. Inoltre, la scoperta della natura discreta dell'informazione in tanti meccanismi biologici fondamentali (DNA, sintesi proteica, metabolismi biochimici) ha reso la teoria dei linguaggi formali un campo in grande sviluppo in cui potere ricercare modelli adeguati per la modellizzazione di un gran numero di fenomeni.

I seguenti sono alcuni esempi di strutture facilmente rappresentabili con linguaggi.

1. L'insieme di tutte le formule predicative su una segnatura finita o numerabile.
2. Una teoria predicativa su una segnatura finita o numerabile.
3. Un modello predicativo su un dominio finito o numerabile (identificato con il suo diagramma).

4. L'insieme *TAUT* delle formule proposizionali che rappresentano tautologie (sottintendendo un alfabeto numerabile di simboli proposizionali).
5. L'insieme *SAT* delle formule proposizionali soddisfacibili (sottintendendo un alfabeto numerabile di simboli proposizionali).
6. L'insieme delle soluzioni (rappresentate come opportune stringhe) di un problema *P*.

La nozione stessa di *problema*, formulato entro qualche rappresentazione dei suoi dati, equivale a quella di linguaggio. Data una formula proposizionale, quando possiamo dire che essa è soddisfacibile (ovvero rispondere affermativamente al problema di verificarne la soddisfacibilità)? Quando, previa sua rappresentazione, possiamo dire che essa appartiene al linguaggio *SAT*. In effetti, la teoria matematica dei problemi e dei loro gradi di risolubilità può considerarsi una specializzazione della teoria della *complessità computazionale*. Il problema (o meglio metaproblema) più famoso in tale teoria consiste nello stabilire se le due classi di linguaggi *P* (in cui l'appartenenza di una stringa è *decidibile deterministicamente* in tempo *polinomiale*, rispetto alla lunghezza della stringa) e *NP* (in cui l'appartenenza di una stringa è decidibile *non deterministicamente* in tempo polinomiale, rispetto alla lunghezza della stringa) sono uguali o diverse. Si dimostra che il linguaggio *SAT* ha complessità massima nella classe *NP*, nel senso che tutti gli altri problemi di *NP* possono essere ricondotti a *SAT* in tempo polinomiale. In tale questione si intersecano in modo inestricabile logica, teoria dei linguaggi e teoria della complessità.

Esempi di linguaggi in contesti ancora più generali sono i seguenti.

1. Tutte le espressioni corrette secondo una sintassi (per esempio i programmi sintatticamente corretti di un certo linguaggio di programmazione).
2. Una funzione sui naturali o sulle stringhe di un alfabeto, vista come insieme di coppie (argomento, risultato).
3. La rappresentazione di un numero in una qualche base (linguaggio infinito se il numero è irrazionale).
4. L'insieme di stringhe che codificano (secondo qualche criterio) una classe di strutture finite (grafi, alberi, tabelle, formule).
5. Le sequenze genetiche del genoma di un organismo biologico.
6. L'insieme di stati che può assumere un sistema dinamico simbolico.

Soffermiamoci su questo ultimo punto che presenta sviluppi ed interpretazioni di grande interesse.

Un *sistema dinamico simbolico* è un sistema che cambia nel tempo e i cui stati sono descrivibili con stringhe.

Il problema di stabilire se il sistema arriva a un certo stato corrisponde a quello di poter decidere se una data stringa appartiene a un certo linguaggio. Analogamente gli stati raggiungibili a partire da certi stati iniziali costituiscono un linguaggio. Gli stati in cui il sistema rimane stabile nel tempo (stati finali) sono un altro linguaggio, e gli stati che dopo un tempo finito portano a certi stati finali sono un altro linguaggio ancora.

I sistemi dinamici naturali continui sono oggetto di studio nella fisica (sistema solare, sistemi idrodinamici, sistemi meteorologici); anche per essi le simulazioni discrete forniscono modelli approssimati, ma estremamente utili, allorché gli strumenti classici (le equazioni differenziali) diventano di complessità proibitiva.

Esempi di sistemi dinamici discreti sono: un sistema di calcolo, o una parte di esso; una rete digitale di comunicazione, in cui ad ogni istante certi pacchetti informativi si trovano sui nodi di un grafo di comunicazione; un archivio o una base di dati con evoluzione temporale; una deduzione (secondo qualche calcolo logico); l'insieme delle possibili configurazioni di una scacchiera durante un gioco (a scacchi, a dama, ...); una miscela biochimica che si trasforma secondo reazioni tra le sue molecole e secondo parametri dipendenti da condizioni esterne (acidi nucleici, proteine, e biomolecole in genere, sono rappresentabili per molti versi come stringhe di opportuni alfabeti).

In tutti i tipi di sistemi dinamici (naturali o artificiali, continui o discreti, chiusi o interattivi, deterministici o no) rimane centrale il problema di una loro descrizione matematica il più possibile rigorosa e generale.

Un primo passo consiste nel passare da descrizioni informali a descrizioni matematicamente rigorose che garantiscono una maggiore affidabilità. In passi successivi si tende a descrizioni più complete, o più semplici, o più generali.

Le famose leggi di Keplero sono una descrizione chiara dei moti planetari (orbite ellittiche, costanza della velocità areolare, tempi di percorrenza). La descrizione newtoniana in termini della forza gravitazionale e del secondo principio della dinamica è un'altra descrizione dello stesso sistema, che ha il vantaggio di ricondurlo a principi generali validi per un'ampia classe di sistemi meccanici.

La descrizione di un sistema dinamico consiste sempre nel passaggio da un sistema rappresentativo a un altro in modo che vi sia un guadagno in termini di accuratezza, semplicità, generalità.

Il passaggio da una rappresentazione a un'altra è la base della problematica della teoria dei linguaggi formali.

Infatti, il problema centrale della teoria matematica dei linguaggi consiste nella ricerca di metodi formali (finitistici) di rappresentazione dei linguaggi e nello studio dei rapporti tra i vari sistemi rappresentativi.

Un primo modo di definire un linguaggio è tramite le usuali notazioni matematiche per definire insiemi. La formalizzazione di una tale descrizione porta alla definizione del linguaggio come linguaggio formale.

Possiamo distinguere quattro metodi principali nella definizione dei linguaggi formali:

(LM) *Definizione entro un modello di stringhe* (le stringhe che verificano certe proprietà).

(AL) *Definizione entro un'algebra di linguaggi* (il linguaggio costruito applicando certe operazioni a partire da certi linguaggi iniziali).

(AG) *Definizione algoritmica generativa* (grammatica).

(AR) *Definizione algoritmica riconoscitiva* (automa).

Negli esempi seguenti, data una stringa α , indichiamo con α^n la concatenazione di n copie di α ($\alpha^0 = \lambda$, stringa vuota).

1. Consideriamo il linguaggio

$$L_1 = \{a^n b^n \mid n \in \omega\}$$

e il seguente modello

$$(\{a, b\}^*, \cdot, ||, a, b, \lambda).$$

Una formalizzazione (LM) di L_1 consiste nella sua rappresentazione logica entro tale modello tramite la seguente formula (soddisfatta da ogni stringa $\alpha \in L$):

$$\begin{aligned} \exists xy (\alpha = xy \wedge |x| = |y| \wedge \forall uvw (x = u \cdot v \cdot w \wedge |v| = |a| \rightarrow v = a) \wedge \\ \wedge \forall uvw (y = u \cdot v \cdot w \wedge |v| = |a| \rightarrow v = b)). \end{aligned}$$

2. Consideriamo il linguaggio:

$$L_2 = \{a^n b^m \mid n, m \in \omega\}$$

e la seguente algebra di linguaggi:

$$(\mathcal{P}(\{a, b\}^*), \cdot, *, \{a\}, \{b\}, \{\lambda\})$$

ove $\cdot$ indica la *concatenazione di linguaggi*, ovvero $L \cdot L'$ è il linguaggio le cui stringhe sono concatenazione di una stringa di L con una stringa di L' , mentre $*$ indica l'iterazione o *stella di Kleene*, ovvero L^* è il linguaggio le cui stringhe sono la concatenazione di un numero qualsivoglia di stringhe di L . La formalizzazione (AL) di L_2 consiste nella sua rappresentazione in termini delle operazioni di concatenazione e iterazione a partire dai linguaggi finiti $\{a\}, \{b\}$:

$$L_2 = \{a\}^* \cdot \{b\}^*.$$

3. Consideriamo di nuovo il linguaggio L_1 . Una grammatica per generare le sue stringhe sarà data nel prossimo paragrafo; tuttavia l'idea soggiacente ad essa è la seguente definizione induttiva:

- genera λ ;
- se hai generato α , allora genera $a\alpha b$;
- non generare altro.

Consideriamo di nuovo il linguaggio L_2 . Un automa per riconoscere le sue stringhe sarà dato nel prossimo paragrafo, tuttavia l'idea soggiacente ad esso è la seguente definizione induttiva:

- riconosci λ ;
- riconosci un qualsiasi numero di a concatenate;
- riconosci un qualsiasi numero di a concatenate seguite da un qualsiasi numero di b concatenate. Non riconoscere altro.

Problemi centrali della teoria dei linguaggi formali sono i seguenti:

1. Data una rappresentazione formale di un linguaggio, costruita con un certo metodo, passare a una rappresentazione equivalente ottenuta con un altro metodo.
2. Caratterizzare matematicamente la classe dei linguaggi rappresentati con certi tipi di metodi e studiare proprietà di tali classi (e.g. proprietà di chiusura e di decidibilità).

Nei metodi descritti possiamo individuare un'altra importante analogia con lo studio dei sistemi dinamici studiati dalla fisica. Un aspetto notevole nel passaggio dalla descrizione kepleriana dei moti planetari a quella newtoniana consiste nel considerare caratteristiche locali del moto piuttosto che globali. Il fatto che le orbite dei moti siano ellittiche (con il Sole in uno dei fuochi) è un dato della descrizione kepleriana, mentre in quella newtoniana è piuttosto una conseguenza della legge di attrazione gravitazionale e della seconda legge della dinamica ($F = ma$). Tali leggi determinano equazioni differenziali che stabiliscono in ultima analisi il tipo di rapporto che deve intercorrere tra il differenziale secondo dello spostamento infinitesimo istantaneo e l'infinitesimo temporale in cui questo avviene.

In modo analogo, come vedremo nel paragrafo successivo, una grammatica o un automa fanno passare da una descrizione globale di un linguaggio (forma delle sue stringhe) a una caratterizzazione tramite trasformazioni locali per generare o riconoscere stringhe del linguaggio.

4.3. Grammatiche e automi

Una *grammatica a struttura di frase* $G = (A, T, S, P)$ è una struttura individuata da un alfabeto finito A , un sottoalfabeto T di A i cui simboli si dicono *terminali* (quelli di A che non sono in T si dicono *non terminali*), da un simbolo iniziale S e da un insieme finito P di coppie di stringhe (α, β) di A^* dette *regole* o *produzioni* di G e indicate solitamente con $\alpha \rightarrow \beta$. Una grammatica individua un metodo generativo per definire un linguaggio $L(G) \subseteq T^*$. Le stringhe di $L(G)$ sono tutte le stringhe costituite da simboli terminali che si ottengono partendo dal simbolo iniziale S , e sostituendo, fino a quando è possibile, un'occorrenza della sottostringa α con la stringa β se $(\alpha \rightarrow \beta)$ è una regola di G .

Di solito i simboli non terminali si indicano con lettere latine maiuscole, e quelli terminali con le minuscole, mentre il simbolo iniziale è indicato con S . In tal modo una grammatica è completamente individuata dalle sue regole.

Esempio 4.22 La seguente grammatica genera $\{a^n b^n \mid n \in \omega\}$ (la dimostrazione è immediata):

$$S \rightarrow \lambda$$

$$S \rightarrow aSb.$$

L'esempio che segue è di importanza fondamentale nella teoria dei linguaggi formali. Esso descrive una forma di accrescimento che potremmo dire *trisomatico*, presente in senso idealizzato in molti organismi biologici costituiti da una parte *cefalica*, una parte *media* e una parte *terminale*, o anche più in generale, nella distinzione fondamentale tra *ectoderma*, *mesoderma* ed *endoderma* che si ritrova nei vari modelli embrionali (in effetti, ciò che è peculiare è un certo rapporto tra le dimensioni delle tre parti). Da un punto di vista strettamente formale si dimostra che la generazione delle stringhe di questo linguaggio implica una qualche forma di sincronizzazione o comunicazione tra le regole che si applicano in punti distanti di una stringa.

Esempio 4.23 La seguente grammatica genera $\{a^n b^n c^n \mid n \in \omega\}$:

$$S \rightarrow \lambda$$

$$S \rightarrow abc$$

$$S \rightarrow aSBc$$

$$cB \rightarrow Bc$$

$$bB \rightarrow bb.$$

Applicando la terza regola più volte, da S si genera la stringa $aa \dots aaS BcBc \dots BcBc$ (tante a quante Bc), e da questa, con la seconda regola,

$aa \dots aaabcBcBc \dots BcBc$. A questo punto la quarta regola permette di spostare i simboli B al centro, generando $aa \dots aaabBB \dots BBccc \dots cc$. Infine, applicando l'ultima regola, a partire dal centro della stringa, si ottiene $aa \dots aaabbb \dots bbccc \dots cc$.

La *classificazione di Chomsky* delle grammatiche è basata sulla forma delle regole. Sia G una grammatica.

1. G è di *tipo 0* se le sue produzioni sono tutte del tipo $\alpha \rightarrow \beta$, ove in α occorre qualche simbolo non terminale.
2. G è di *tipo 1* se è di tipo 0 e inoltre, in ogni sua produzione, $\alpha \rightarrow \beta$, vale che $|\alpha| \leq |\beta|$.
3. G è di *tipo 2* se è di tipo 1 e se inoltre, in ogni sua produzione, $\alpha \rightarrow \beta$, vale che $|\alpha| = 1$.
4. G è di *tipo 3* se è di tipo 2 e se inoltre, in ogni sua produzione, $\alpha \rightarrow \beta$, vale che β , è costituita da un simbolo terminale o da due simboli, di cui il primo non terminale e il secondo terminale.

In senso lato si ammette che anche per i tipi 1, 2, 3 possa esserci una regola del tipo $X \rightarrow \lambda$ purché X sia un simbolo non terminale che non occorre mai nella parte destra di qualche altra regola (per esempio la grammatica precedentemente data per $\{a^n b^n | n \in \omega\}$, verifica una tale condizione se riformulata nel modo seguente ($S \rightarrow \lambda$, $S' \rightarrow ab$, $S \rightarrow S'$, $S' \rightarrow aS'b$).

La classificazione di Chomsky è di fondamentale importanza nella teoria dei linguaggi formali. Infatti, a partire da essa si possono individuare le *classi di linguaggi*:

RE, CS, CF, REG.

La classe *RE* è costituita dai linguaggi *ricorsivamente enumerabili* generati da grammatiche di tipo 0; *CS* (*context sensitive*) dai linguaggi generati da grammatiche di tipo 1; *CF* (*context free*) dai linguaggi generati da grammatiche di tipo 2; *REG* dai linguaggi generati da grammatiche di tipo 3 (*regolari*, che si possono anche costruire a partire dai linguaggi di un solo simbolo, usando l'unione, la concatenazione e l'operatore $*$).

Tali classi sono strettamente incluse nell'ordine $RE \subset CS \subset CF \subset REG$. Infatti si dimostra che $\{a^n b^n | n \in \omega\} \in CF - REG$, $\{a^n b^n c^n | n \in \omega\} \in CS - CF$, e *CS* è strettamente inclusa nella classe dei linguaggi decidibili (vedi oltre) che sono una classe strettamente inclusa in *RE* (vedi oltre). Inoltre si possono trovare classi intermedie tra *CF* e *REG*, tra *CF* e *CS*, tra *CS* e *RE* e oltre *RE* entro tutta la classe dei linguaggi; all'interno di tale gerarchia vi sono

sottogerarchie (alcune infinite) estremamente complesse e articolate (gerarchia dei lineari, dei decidibili, dei semidecidibili e degli indecidibili). Ci si rende conto quindi come entro il numerabile vi sia una ricchezza di gradi di complessità generativa analoga a quella scoperta da Cantor per gli insiemi infiniti. La complessità generativa corrisponde a caratteristiche computazionali molto importanti; per esempio, vari linguaggi di grande interesse computazionale si trovano in classi intermedie tra CS e CF . In tale intervallo si situano le classi P e NP dei linguaggi generabili in *tempo polinomiale* rispettivamente con macchine di Turing deterministiche o non deterministiche (vedi oltre). Il tempo di generazione è dato da un polinomio $p(n)$, ove n è la lunghezza della stringa da generare. Il linguaggio SAT di tutte le formule proposizionali soddisfacibili appartiene a una classe di tale intervallo, detta $ETOL$.

Un *automa a stati finiti* $M = (A, Q, q_0, F, t)$ è una struttura determinata da: un alfabeto finito A ; un insieme finito di *stati* Q ; uno *stato iniziale* q_0 ; un sottoinsieme di *stati finali* F ; un insieme finito di *regole di transizione* t , ovvero triple (stato, simbolo, stato). L'automa prende in ingresso una stringa di simboli leggendone il primo simbolo e ponendosi nello stato iniziale; in base a una regola di transizione (q, a, q') , se legge il simbolo a nello stato q , passa a leggere il simbolo seguente della stringa di ingresso ponendosi nello stato q' . Il *linguaggio* $L(M)$ *riconosciuto da* M è costituito dalle stringhe che, date in ingresso a M lo pongono, a lettura conclusa, in uno stato finale. Un automa è non deterministico se durante il funzionamento può applicare più di una regola (e in tal caso ne sceglie una tra le applicabili). Si dimostra che per ogni automa a stati finiti non deterministico ve ne è uno deterministico equivalente. Si dimostra anche che i linguaggi riconosciuti da automi a stati finiti sono tutti e solo quelli della classe REG . Conveniamo di indicare con q_0 lo stato iniziale, con lettere minuscole i simboli e con $q_i, \in \omega$ gli stati, asteriscandoli quando sono finali. In tal modo un automa è completamente individuato dalle sue regole di transizione che diamo nella forma (stato simbolo $\rightarrow$ stato).

Esempio 4.24 Il seguente automa riconosce $\{a^n b^m \mid n, m \in \omega\}$:

$$q_0^* a \rightarrow q_0^*$$

$$q_0^* b \rightarrow q_1^*$$

$$q_1^* b \rightarrow q_1^*$$

$$q_1^* a \rightarrow q_2.$$

4.4. Teorie monoidali

Le teorie monoidali costituiscono un ambiente naturale per la *rappresentazione logica di linguaggi*.

Definizione 4.3 *Una teoria monoidale su un alfabeto A è una teoria i cui termini chiusi includono il monoide libero A^* su A e i cui assiomi includono gli assiomi di monoide.*

La rappresentabilità entro teorie monoidali è un caso particolare di rappresentabilità di insiemi entro teorie predicative.

Definizione 4.4 *Un linguaggio L su un alfabeto A si dice monoidalmente rappresentabile se esso è rappresentabile entro la teoria monoidale Φ su A (tramite una formula $\varphi(x)$), ovvero se:*

$$\alpha \in L \Leftrightarrow \Phi \models \varphi(\alpha).$$

Usualmente nelle rappresentazioni monoidali si sottointendono gli assiomi di monoide (e le variabili libere si intendono implicitamente quantificate universalmente).

Esempio 4.25 Rappresentazione monoidale di $\{a^n b^n \mid n \in \omega\}$ tramite il predicato P :

$$P(\lambda)$$

$$P(x) \rightarrow P(axb).$$

Esempio 4.26 Rappresentazione monoidale di $\{a^n b^n c^n \mid n \in \omega\}$ tramite il predicato P :

$$P(\lambda)$$

$$P(abc)$$

$$P(xby) \rightarrow P(axbbbyc).$$

La seguente deduzione genera in tale teoria $P(aabbcc)$:

1. $P(abc)$ (secondo assioma)
2. $P(abc) \rightarrow P(aabbcc)$ (istanza del terzo assioma per $x = a, y = c$)
3. $P(aabbcc)$ (modus ponens da 1, 2).

In generale, supponiamo di avere generato $P(a^n b^n c^n)$; allora, istanziando il secondo assioma con $x = a^n, y = b^{n-1} c^n$, si ha $P(a^n b^n c^n) \rightarrow P(a^{n+1} b^{n+1} c^{n+1})$.

c^{n+1}) e, per modus ponens, si deriva $P(a^{n+1}b^{n+1}c^{n+1})$. Quindi, per induzione, segue che il predicato P rappresenta, entro tale teoria monoidale, il linguaggio $\{a^n b^n c^n \mid n \in \omega\}$.

Esempio 4.27 Un metodo alternativo al precedente per rappresentare monoidalmente $\{a^n b^n c^n \mid n \in \omega\}$ utilizza un ulteriore predicato ternario R :

$$R(\lambda, \lambda, \lambda)$$

$$R(x, y, z) \rightarrow R(ax, by, cz)$$

$$R(x, y, z) \rightarrow P(xyz).$$

Esempio 4.28 Rappresentazione monoidale di $\{a^n b^m \mid n \in \omega\}$ tramite il predicato P :

$$P(\lambda)$$

$$P(x) \rightarrow P(ax)$$

$$P(x) \rightarrow P(xb).$$

Esempio 4.29 Rappresentazione monoidale di $\{a^{n+m} b^n c^m \mid n \in \omega\}$ tramite il predicato P :

$$R(\lambda, \lambda)$$

$$L(\lambda, \lambda)$$

$$R(x, y) \rightarrow R(ax, by)$$

$$L(x, y) \rightarrow L(ax, cy)$$

$$R(x, y) \wedge L(z, w) \rightarrow P(xzyw).$$

Esercizio 4.7 Si dia una rappresentazione monoidale del linguaggio dei duplicati su un alfabeto binario: $\{\alpha\alpha \mid \alpha \in \{a, b\}^*\}$.

Il linguaggio dell'esercizio precedente è di grande importanza sia in teoria dei linguaggi formali che in natura. Una sua grammatica di Chomsky è notevolmente complessa (si tratta, come per il linguaggio trisomatico, di un linguaggio dipendente dal contesto). In natura esso è collegato alla riproduzione, e in un certo senso una delle caratteristiche del DNA è quella di strutturare l'informazione in modo da rendere efficiente la generazione di duplicati.

Esempio 4.30 Rappresentazione monoidale dei numeri primi tramite il predicato Prime:

$$\alpha \in \{a^p \mid p \text{ è un numero primo}\} \Leftrightarrow \Phi \models \text{Prime}(\alpha).$$

Assiomi propri (segnatura $\{--, \lambda, a, \text{Factor}, \text{Less}, \text{Prime}\}$):

$$\forall x \text{Factor}(x, x)$$

$$\forall xy (\text{Factor}(x, y) \rightarrow \text{Factor}(x, xy))$$

$$\forall x \text{Less}(x, ax)$$

$$\forall xy (\text{Less}(x, y) \wedge \text{Less}(y, z) \rightarrow \text{Less}(x, z))$$

$$\forall x (\forall y (\text{Less}(y, x) \wedge \neg a = y \rightarrow \neg \text{Factor}(y, x)) \rightarrow \text{Prime}(x)).$$

Proposizione 4.3 *Data una grammatica $G = (A, T, S, P)$ si può costruire una teoria monoidale che rappresenta il linguaggio $L(G)$ tramite un opportuno predicato.*

Dimostrazione Consideriamo i seguenti assiomi *CG* (*Chomsky grammars*).

$$D(S)$$

$$D(xyz) \wedge R(y, w) \rightarrow D(xwz) \quad \text{per ogni regola } x \rightarrow y \in P$$

$$F(a) \quad \text{per ogni simbolo terminale } a \in T$$

$$F(x) \wedge F(y) \rightarrow F(xy)$$

$$D(x) \wedge F(x) \rightarrow H(x).$$

Aggiungiamo a tale teoria gli assiomi $\text{Th}(G)$ che descrivono una grammatica $G = (A, T, S, P)$:

$$D(S)$$

$$R(\alpha, \beta), \forall \alpha \rightarrow \beta \in P$$

$$F(a), \forall a \in T.$$

Di qui segue facilmente:

$$CG \cup \text{Th}(G) \models H(\alpha) \Leftrightarrow \alpha \in L(G). \quad \blacksquare$$

Il funzionamento di un automa a stati finiti è descritto dalla seguente teoria monoidale *ASF* su $A \cup Q$:

$$I(x) \wedge I(y) \rightarrow I(xy)$$

$$Q_0(q) \wedge I(x) \rightarrow T(qx)$$

$$T(xqyz) \wedge R(qy, q') \rightarrow T(xyq'z)$$

$$T(xq) \wedge F(q) \rightarrow A(x).$$

Se a tale teoria si aggiungono degli assiomi $\text{Th}(M)$ per predicati che specificano i simboli, gli stati, lo stato iniziale, quelli finali e le transizioni rispettivamente, allora vale la seguente rappresentazione logica.

Proposizione 4.4

$$ASF \cup \text{Th}(M) \models A(\alpha) \Leftrightarrow \alpha \in L(M).$$

Esempio 4.31 Una teoria monoidale per le alghe rosse. Le alghe rosse sono un esempio famoso che ha ispirato la definizione degli L -sistemi da parte di Lindenmayer alla fine degli anni Sessanta. Si tratta di organismi primitivi il cui accrescimento avviene secondo il seguente schema geometrico discreto (fig. 4.1) in cui sono raffigurati i primi sette stadi di tale evoluzione (ogni segmento rappresenta una cellula).

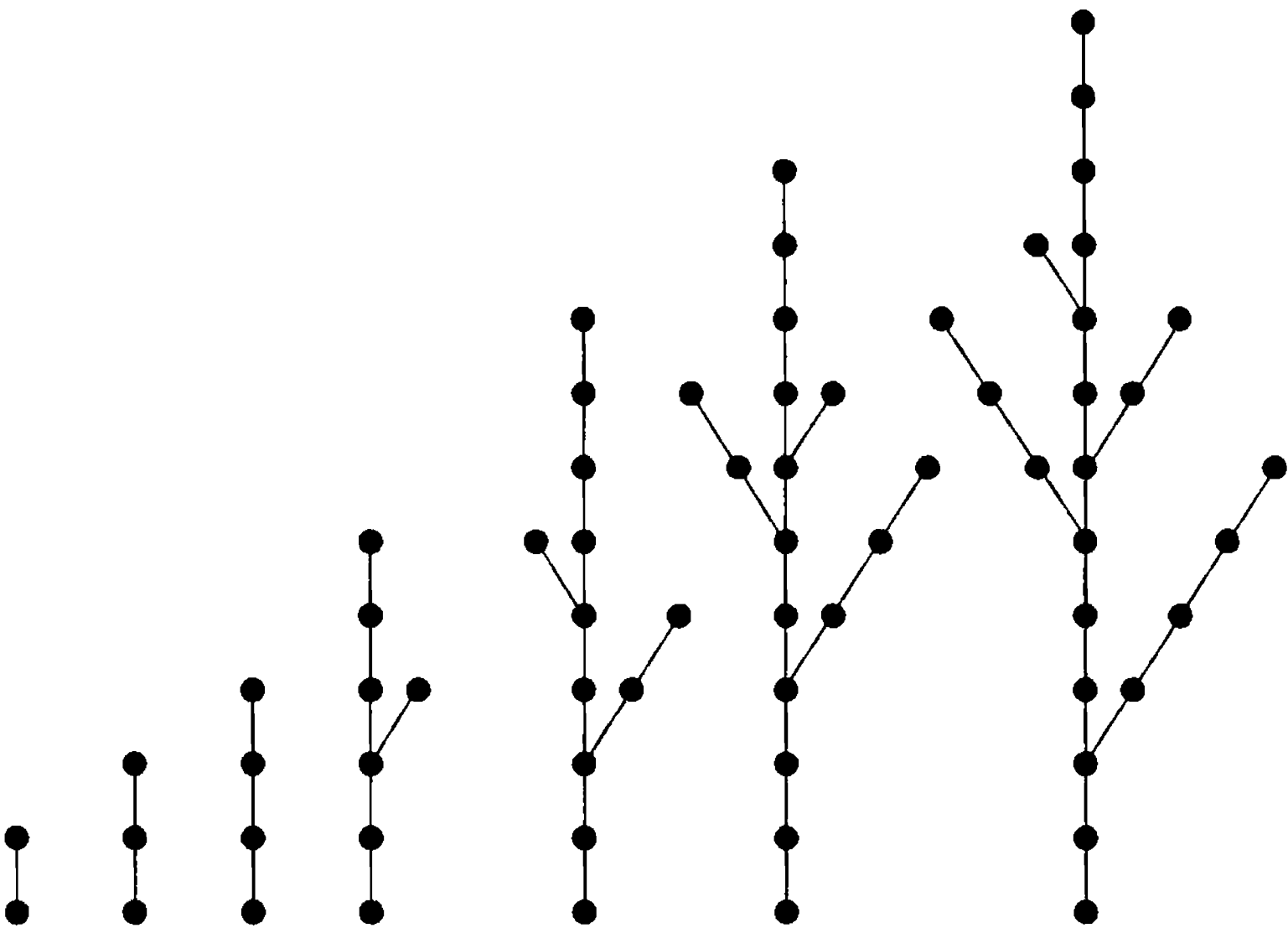


Figura 4.1
Stadi di sviluppo dell'alga rossa.

Adottando l'usuale rappresentazione Logo (a tartaruga) possiamo rappresentare i primi sei stadi dello sviluppo con le seguenti stringhe sull'alfabeto $\{F, [,]\}$, dove $R(n)$ è la stringa che rappresenta l'organismo allo stadio n (F è un segmento verticale e ciò che si trova tra parentesi rappresenta una struttura che alternativamente ha un angolo positivo o negativo rispetto

all'asse principale di accrescimento):

$$R(1) = F$$

$$R(2) = FF$$

$$R(3) = FFFF$$

$$R(4) = FF[F]FF$$

$$R(5) = FF[FF]FF[F]FF$$

$$R(6) = FF[FFF]FF[FF]FF[F]FFFF.$$

(Dopo i primi sei stadi lo sviluppo avviene secondo la seguente regola individuata da Lindenmayer):

Dallo stadio 6 in poi l'organismo può essere diviso in due parti. Le prime sei celle (dal basso) del ramo principale costituiscono una parte basale, il resto una parte apicale. La seconda, la quarta e la sesta cella della parte basale sostengono dei rami semplici collaterali ad angolo alternativamente positivo o negativo rispetto alla direzione basale (partendo dal basso), che al sesto stadio hanno lunghezza rispettivamente di 3, 2, 1. Dopo lo stadio 6 la parte basale cresce semplicemente allungando di una cellula ciascuno dei suoi rami collaterali. La parte apicale allo stadio 6 consiste di 4 cellule senza alcun ramo collaterale. Negli stadi successivi la parte apicale è una ripetizione della parte apicale dello stadio precedente più altre due celle che si aggiungono alla sua estremità inferiore, la seconda delle quali sostiene una struttura uguale all'intero organismo di 6 stadi anteriore, con un angolo opposto all'angolo del ramo immediatamente sottostante.¹

La figura 4.2 illustra la dinamica dell'accrescimento descritto. Al passo n ($n > 6$) la parte basale aggiunge una cellula a ciascun ramo (freccie laterali); si aggiungono due celle all'asse della basale (doppie linee) e un ramo che coincide con l'intero organismo di sei stadi precedenti (triangolo a doppie linee):

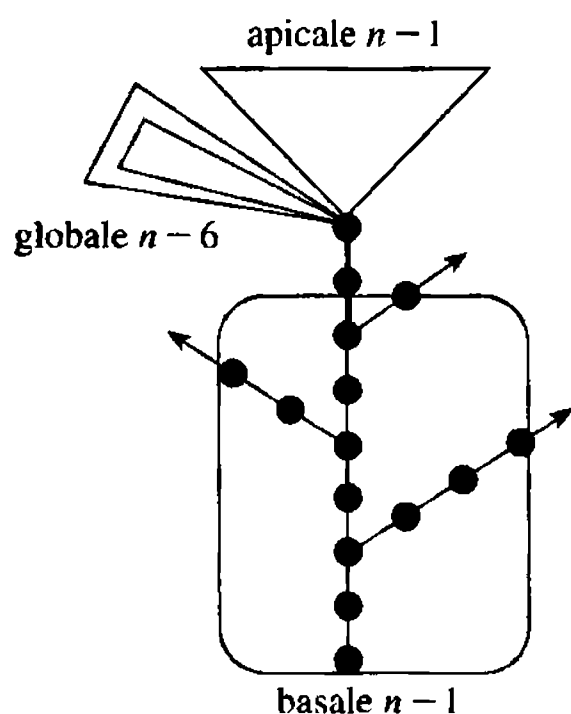


Figura 4.2
Schema di sviluppo di un'alga rossa.

¹ Citata da G. T. Herman e G. Rozenberg in *Developmental Systems and Languages*, North-Holland, Amsterdam 1975, cap. 1.

Se aggiungiamo ai precedenti assiomi (tranne l'ultimo che diventa ridondante) quelli che seguono, otteniamo una teoria monoidale RA di alfabeto $\{F, [,]\}$ e segnatura $\{A_, B_, R_, L_, +, 0, 1\}$ (più i simboli dell'alfabeto e quelli di monoidale) che formalizza completamente il processo di accrescimento appena descritto. Infatti, per $n > 5$ valgono le seguenti condizioni, dove $R(n)$, $B(n)$, $A(n)$ sono le stringhe che rappresentano rispettivamente l'intero organismo, la sua parte basale e la sua parte apicale allo stadio n (n variabile implicitamente universalmente quantificata, 1 sta per $0 + 1$, 2 sta per $0 + 1 + 1$, ..., 6 sta per $0 + 1 + 1 + 1 + 1 + 1 + 1$):

$$A(5) = FF$$

$$R(0) = \lambda$$

$$L(0) = \lambda$$

$$A(n + 6) = FF[R(n)]A(n + 5)$$

$$B(n + 6) = FF[L(n + 3)]FF[L(n + 2)]FF[L(n + 1)]$$

$$L(n + 1) = FL(n)$$

$$R(n + 6) = B(n + 6)A(n + 6).$$

Indichiamo con T i termini della sottosegnatura $\Sigma_0 = \{R, +, 0, 1\}$ e con A l'alfabeto $\{F, [,]\}$. Il linguaggio delle stringhe che rappresentano gli stati di sviluppo di un'alga rossa è costituito da

$$\{\alpha \in A^* \mid RA \vdash t = \alpha, t \in T_{\Sigma_0}\}.$$

Per capire il vantaggio di una tale formalizzazione riportiamo le regole di una rappresentazione alla Lindenmayer:

$$0 \rightarrow 10$$

$$1 \rightarrow 32$$

$$2 \rightarrow 3[4]$$

$$3 \rightarrow 3$$

$$4 \rightarrow 56$$

$$5 \rightarrow 37$$

$$6 \rightarrow 58$$

$$7 \rightarrow 3[9]$$

$$8 \rightarrow 50$$

$$9 \rightarrow 39$$

$$[\rightarrow [$$

$$] \rightarrow].$$

Si verifica, ma non è affatto facile, che partendo da 4, sostituendo simultaneamente ad ogni passo ciascun simbolo con la parte destra della regola relativa, si ottengono stringhe che rappresentano i vari stati evolutivi dell'alga (ogni cifra rappresenta lo stesso tipo di cellula e le parentesi racchiudono i rami laterali):

4

56

3558

33[9]3750

33[39]33[9]3710

33[339]33[39]33[9]3210.

Per induzione si dimostra che per $n > 6$ la stringa x_n che si ottiene è:

$$33[3^{(n-4)}9]33[3^{(n-5)}9]33[3^{(n-6)}9]33[x_{n-6}]33[x_{n-7}]33...33[x_2]33[x_1]3210$$

che verifica appunto la legge evolutiva prima determinata in termini di accrescimento basale e apicale.

Come si può intuire da questo esempio, le teorie monoidali si rivelano uno strumento molto potente nella descrizione unificata di molti sistemi simbolici e nella definizione di sistemi complessi suggeriti da fenomeni biologici (accrescimenti, evoluzioni, metabolismi) e dei modelli di calcolo ad essi ispirati. Utilizzando teorie monoidali si riescono a descrivere logicamente forme di accrescimento di tipo frattale riscontrabili in natura (arbusti, alberi, ...) e spesso le descrizioni monoidali assumono naturalmente forme equazionali.

Esercizio 4.8 *L'alga verde è un organismo con tre tipi di cellule $\{a, b, c\}$, i cui primi due stadi di sviluppo sono b e a , mentre negli stadi successivi si ha una cellula c che si aggiunge all'intero organismo nello stadio precedente, più un ramo uguale all'organismo di due stadi precedenti (l'angolo dei rami laterali è alternativamente positivo o negativo rispetto alla direzione principale di accrescimento). Si dia una teoria monoidale che determina tutti gli stadi evolutivi di tale alga.*

4.5. Rappresentazione logica delle macchine di Turing

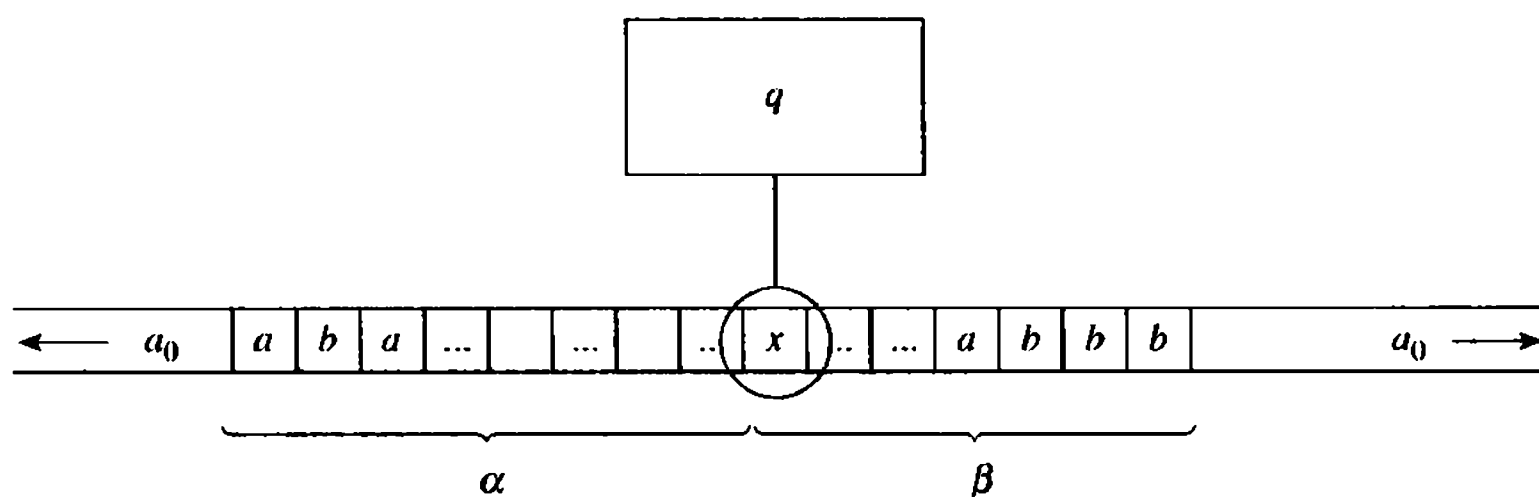
Le *macchine di Turing* costituiscono il primo e più famoso modello matematico di calcolo. Una macchina di Turing è un automa che, presa in ingresso una stringa su un nastro, quando si trova nel suo stato iniziale, ne

legge il primo simbolo a sinistra dopodiché la elabora compiendo le seguenti operazioni elementari, che dipendono dallo stato in cui si trova e dal simbolo letto: I) *spostamento*, a destra o sinistra, II) *sostituzione* di un simbolo (eventualmente lo stesso) al posto di quello letto e III) *cambio* di stato (eventualmente lo stesso). Da un punto di vista formale una macchina di Turing $M = (A, a_0, Q, q_0, \rightarrow, Q_f)$ è caratterizzata da: un alfabeto A ; un simbolo speciale a_0 detto *bianco*; stati Q ; uno stato iniziale q_0 ; stati finali Q_f ; un insieme finito $\rightarrow$, di regole di transizione del tipo:

$$(q, x, q', y, \delta)$$

che la macchina M esegue in questo modo: nello stato q , leggendo il simbolo x , passa allo stato q' , rimpiazza x con y e compie lo spostamento δ dell'organo di lettura. Lo spostamento può avvenire a destra oppure a sinistra (dx, sn) e il simbolo bianco può essere aggiunto alle estremità della stringa corrente. Gli stati in corrispondenza dei quali non vi è alcuna istruzione applicabile sono finali, ovvero determinano l'arresto della macchina. L'uscita di una computazione che termina è costituita dalla porzione della stringa ottenuta all'ultimo passo che è compresa tra i due simboli (inclusi) più estremi che sono diversi dal simbolo bianco. Indichiamo con $L(M)$ l'insieme di stringhe che si possono ottenere come uscite della macchina M .

La seguente teoria TT è una descrizione logica delle macchine di Turing. Intuitivamente $T(\alpha q \beta)$ esprime che sul nastro di input della macchina si trova la parola $\alpha\beta$, la macchina è nello stato q , legge il primo simbolo della parola β , che occupa la parte destra del nastro, mentre alla sinistra della cella di lettura si trova la parola α . La formula $S(x)$ indica che x è un simbolo, $S_0(x)$ che x è il simbolo speciale *bianco* e $C(x)$ che x è un simbolo diverso dal bianco, $Q(q)$ che q è uno stato e $Q_0(q)$ che q è lo stato iniziale. La formula $R(qx, q'y)$ esprime l'istruzione (q, x, q', y, dx) , mentre $L(qx, q'x)$ esprime (q, x, q', y, sn) . La formula $F(q)$ indica che q è uno stato finale; il predicato D serve a cancellare, nel nastro finale, i simboli bianchi estremi; e la formula $O(x)$ dice che x è l'uscita ottenuta quando la macchina si ferma. Tutte le lettere latine minuscole sono variabili.



Gli assiomi TT (*Turing theory*) che seguono sono formule condizionali di Horn (vedi § 3.3):

$$Q_0(q) \rightarrow T(q)$$

$$S_0(x) \rightarrow S(x)$$

$$C(x) \rightarrow S(x)$$

$$Q_0(q) \wedge T(qx) \wedge S(y) \rightarrow T(qxy)$$

$$R(qx, q'y) \wedge T(wqxz) \rightarrow T(wyq'z)$$

$$S_0(x) \wedge Q(q) \wedge T(zq) \rightarrow T(zqx)$$

$$L(qx, q'y) \wedge T(wuqxz) \wedge S(u) \rightarrow T(wq'uyz)$$

$$S_0(x) \wedge Q(q) \wedge T(qz) \rightarrow T(xqz)$$

$$T(xqy) \wedge F(q) \rightarrow D(xy)$$

$$S_0(x) \wedge D(xy) \rightarrow D(y)$$

$$S_0(y) \wedge D(xy) \rightarrow D(x)$$

$$D(\lambda) \rightarrow O(\lambda)$$

$$D(x) \wedge C(x) \rightarrow O(x)$$

$$D(xyz) \wedge C(x) \wedge C(z) \rightarrow O(xyz).$$

Consideriamo una particolare macchina di Turing $M = (A, \mathbf{a}_0, Q, \mathbf{q}_0, \rightarrow_r, Q_f)$. La teoria $\text{Th}(M)$, che specifica i simboli, gli stati, il simbolo bianco, lo stato iniziale, le istruzioni e gli stati finali della macchina di Turing M (le lettere latine minuscole in neretto, anche con sottoscritte, sono costanti individuali) è data dalle seguenti proposizioni

$$S_0(\mathbf{a}_0)$$

$$Q_0(\mathbf{q}_0)$$

$$C(\mathbf{a}) \quad \text{per ogni } \mathbf{a} \in A, \mathbf{a} \neq \mathbf{a}_0$$

$$Q(\mathbf{q}) \quad \text{per ogni } \mathbf{q} \in Q$$

$$F(\mathbf{q}) \quad \text{per ogni } \mathbf{q} \in Q_f$$

$$R(\mathbf{qa}, \mathbf{q'b}) \quad \text{per ogni } (\mathbf{q}, \mathbf{x}, \mathbf{q'}, \mathbf{y}, \mathbf{dx}) \in \rightarrow_r$$

$$L(\mathbf{qa}, \mathbf{q'b}) \quad \text{per ogni } (\mathbf{q}, \mathbf{x}, \mathbf{q'}, \mathbf{y}, \mathbf{sn}) \in \rightarrow_r.$$

La seguente proposizione è conseguenza immediata della costruzione della teoria TT.

Proposizione 4.5

$$\text{TT} \cup \text{Th}(M) \models O(\alpha) \Leftrightarrow \alpha \in L(M).$$

Definizione 4.5 *Un linguaggio L si dice semidecidibile se esiste una macchina di Turing tale che $L = L(M)$.*

Tesi di Church *Ogni linguaggio definito tramite un procedimento effettivo è semidecidibile nel senso della definizione precedente.*

Si dimostra che la classe dei linguaggi semidecidibili coincide con la classe *RE* dei linguaggi generati da grammatiche di tipo 0.

4.6. Semidecidibilità e decidibilità

A partire dai risultati precedenti mostreremo l'esistenza di un linguaggio semidecidibile per cui non può esistere un metodo generale ed effettivo per decidere se un dato elemento gli appartiene. Nel seguito A indicherà un alfabeto arbitrariamente prefissato.

Definizione 4.6 *Un linguaggio L si dice decidibile se esso e il suo complementare sono entrambi semidecidibili.*

Consideriamo delle enumerazioni senza ripetizione: $(\alpha_i | i \in \omega)$, di tutte le parole sull'alfabeto A , e $(M_i | i \in \omega)$, di tutte le macchine di Turing su tale alfabeto.

Proposizione 4.6 *Sia K il linguaggio di tutte le parole sull'alfabeto A ciascuna delle quali è generata dalla macchina avente lo stesso indice. Tale linguaggio è semidecidibile.*

Dimostrazione Basta numerare tutte le coppie di naturali, e, in corrispondenza di una coppia (i, j) , eseguire j passi di derivazione (secondo una qualche nozione di passo) nella teoria che rappresenta M_i . Se con questo procedimento la parola di indice i compare in corrispondenza di qualche coppia (i, j) , allora essa si considera generata. In tal modo vengono evidentemente generate tutte e sole le parole di K ; quindi, in base alla tesi di Church, K risulta semidecidibile. ■

Proposizione 4.7 (diagonalizzazione di Turing) *Sia K' il linguaggio complementare di K . Tale linguaggio non è semidecidibile.*

Dimostrazione Se esistesse una macchina di Turing che lo genera, considerato l'indice d di una tale macchina si otterrebbe la solita contraddizione diagonale del teorema di Russell e del teorema di Cantor. ■

Proposizione 4.8 (non decidibilità della fermata) *Il linguaggio K non è decidibile.*

Dimostrazione Abbiamo visto che K è semidecidibile. Se fosse decidibile, allora il suo complementare dovrebbe essere semidecidibile, ma ciò è escluso dalla proposizione precedente. ■

Capitolo 5

Indecidibilità e incompletezza

Per le macchine di Turing abbiamo scoperto dei limiti intrinseci che, per la tesi di Church, si estendono a un qualsiasi metodo di calcolo. In particolare, dato un linguaggio L e una stringa α , alla domanda se α appartenga a L ($\alpha \in L$) non sempre si può dare risposta. Vi sono casi in cui nessun formalismo di calcolo ci assicura la fermata con un “sì” o con un “no”. Abbiamo anche visto che spesso il problema non è costituito dal “sì”, quanto piuttosto dal “no”. Infatti, vi sono linguaggi i cui elementi possono essere tutti generati da un procedimento di calcolo (ricorsivamente enumerabili), per i quali tuttavia, se a un certo punto non si è ancora generato un elemento, non si può mai escludere che non venga generato più tardi. Tali sono i linguaggi semidecidibili, per i quali si può sempre scoprire se un elemento vi appartiene, ma non si può in generale escludere che un dato elemento vi appartenga. La proposizione che segue ci dice che i limiti scoperti per i calcoli implicano limiti per la deduzione. In effetti, mediante una rappresentazione monoidale un calcolo di una macchina di Turing si trasforma in una deduzione. Da ciò la logica eredita l'impossibilità di decidere già dimostrata per le macchine di Turing.

Proposizione 5.1 (teorema di Church) *La relazione $\models$ di conseguenza logica non è decidibile.*

Dimostrazione La rappresentazione di una macchina di Turing come teoria logica (con numero finito di assiomi) implica che non può esistere un metodo effettivo per stabilire se una formula è conseguenza logica di un numero finito di assiomi. Infatti, se così fosse, si consideri la teoria TT_K che rappresenta la macchina di Turing che genera K . Se si potesse sempre decidere quando una formula consegue da tale teoria, allora si potrebbe facilmente decidere sempre se una parola appartiene o non appartiene a K , ma ciò non è possibile perché K non è decidibile.

Definizione 5.1 *Una teoria Φ su una segnatura Σ dicesi completa se, data una qualsiasi formula φ della segnatura, vale che o $\varphi \in \Phi$ o $\neg \varphi \in \Phi$.*

Proposizione 5.2 (completamento di Lindenbaum) *Una teoria soddisfacibile può essere sempre estesa a una teoria soddisfacibile e completa.*

Dimostrazione Dimostriamo innanzitutto che, data una teoria Φ soddisfacibile, allora per ogni formula φ della sua segnatura o $\Phi \cup \{\varphi\}$ o $\Phi \cup \{\neg \varphi\}$ è soddisfacibile. Infatti, supponiamo che entrambe tali teorie fossero insoddisfacibili, allora si avrebbe contemporaneamente:

$$\Phi \cup \{\varphi\} \models \perp$$

$$\Phi \cup \{\neg \varphi\} \models \perp$$

ma queste implicherebbero rispettivamente $\Phi \models \varphi$ e $\Phi \models \neg \varphi$ e quindi anche Φ sarebbe insoddisfacibile, contro le ipotesi. A questo punto enumeriamo (o bene ordiniamo) tutte le proposizioni della segnatura: $\varphi_1, \varphi_2, \dots$. Quindi, consideriamo la catena di teorie (ordinate rispetto all'inclusione): $(\Phi_i \mid i \in \omega)$, ove $\Phi_0 = \Phi$ e Φ_{i+1} è ottenuta da Φ_i aggiungendogli φ_i se questa non appartiene già a Φ_i e se $\Phi_i \cup \{\varphi_i\}$ è soddisfacibile, e ponendo $\Phi_{i+1} = \Phi_i$ altrimenti. Per quanto osservato sopra, l'unione di tale catena è completa, perché, data una proposizione φ , prima o poi una delle due proposizioni φ o $\neg \varphi$ sarà inclusa in una teoria della catena. Inoltre tale unione è soddisfacibile, perché se non lo fosse, allora, in base alla compattezza, un qualche suo sottoinsieme finito sarebbe insoddisfacibile e quindi sicuramente qualche teoria della catena sarebbe già tale. ■

Richiamiamo l'attenzione sui molteplici usi del termine *completezza* (ordinamenti completi, reticoli completi, calcoli completi, Σ_1 -completezza, teorie complete). In particolare, la completezza di una logica o di un calcolo (stabilità, per esempio, dal teorema di completezza del metodo dei tableau) è propriamente una *completezza deduttiva*, del tutto diversa dalla completezza di una teoria come sopra definita che è invece una *completezza assiomatica*.

Esempi importanti di teorie complete sono le teorie del tipo $\text{Th}(\mathcal{M})$ costituite da tutte le proposizioni valide in un modello $\mathcal{M}$.

Definizione 5.2 *Due modelli $\mathcal{M}$ e $\mathcal{M}'$, sulla stessa segnatura, si dicono elementarmente equivalenti sse $\text{Th}(\mathcal{M}) = \text{Th}(\mathcal{M}')$.*

La definizione precedente indica che le teorie complete sono molto importanti in quanto individuano classi di modelli elementarmente equivalenti. Notiamo che l'equivalenza elementare individua una nozione più debole dell'isomorfismo tra strutture, in quanto per i teoremi di Löwenheim-Skolem due modelli elementarmente equivalenti possono avere cardinalità distinte.

Definizione 5.3 *Una teoria assiomatica è l'insieme di tutte le conseguenze logiche, dette teoremi, di un insieme decidibile di formule dette assiomi. Una teoria è assiomatizzabile se esiste un insieme di assiomi il cui insieme di teoremi coincide con la teoria, in tal caso si dice che gli assiomi la assiomatizzano.*

Lemma 5.1 *Una teoria Φ assiomatizzabile e completa è anche decidibile.*

Dimostrazione Se Φ è completa, data una formula φ , tale formula o la sua negazione sono teoremi della teoria Φ . Poiché gli assiomi sono un insieme decidibile, i teoremi della teoria sono un insieme effettivamente enumerabile (facile da verificare). Si consideri una loro enumerazione: se a un certo punto si genera φ , si risponde affermativamente alla appartenenza, se si genera $\neg \varphi$ vi si risponde negativamente; una delle due deve prima o poi essere generata per l'ipotesi di completezza. ■

Definizione 5.4 *Una teoria consistente si dice gödeliana se essa può rappresentare tutti i linguaggi semidecidibili (rispetto a una prefissata codifica dei relativi alfabeti).*

Ovviamente TT è gödeliana. Si dimostra facilmente che Th(SEQ) è gödeliana e da ciò, utilizzando la β di Gödel, si dimostra che anche Th(AR) è gödeliana. Infine, dal fatto che Th(AR) è gödeliana, segue, per la Σ_1 -completezza (cfr. proposizione 4.1) che RR e PA sono gödeliane.

Proposizione 5.3 (primo teorema di incompletezza di Gödel) *Non può esistere alcuna teoria assiomatizzabile, gödeliana, e completa.*

Dimostrazione Se Φ fosse una teoria assiomatizzabile e completa, per il lemma precedente sarebbe decidibile, ma allora non potrebbe essere gödeliana, perché in quanto decidibile non potrebbe rappresentare K. ■

Corollario 5.1 *Le teorie TT, PA, RR, SS non sono complete.*

Dimostrazione Segue dal teorema precedente e dal fatto che tali teorie sono assiomatizzabili e gödeliane. ■

Corollario 5.2 *Th(AR) e Th(SEQ) non sono assiomatizzabili.*

Dimostrazione Segue dal teorema precedente e dal fatto che tali teorie sono gödeliane e complete. ■

5.1. Dall'ideografia di Frege ai teoremi di Gödel

Dopo le ricerche di Leibniz, i primi progressi essenziali verso una realizzazione del progetto di definizione di un linguaggio logico furono compiuti da Boole nel fondamentale *An Investigation of the Laws of Thought* (1854). Una completa descrizione formale in senso moderno, della logica predicativa, con un formalismo logico in cui intervengono connettivi e quantificatori, si è avuta nel 1879 ad opera di Frege con il *Begriffsschrift*, ovvero, come recita il sottotitolo, "un linguaggio di formule, modellato su quello dell'aritmetica, per il puro pensiero".¹ La semantica della logica predicativa in termini matematici è stata sviluppata intorno agli anni Trenta fondamentalmente per opera di Alfred Tarski, il cui metodo interpretativo ha avuto un impatto enorme per lo sviluppo e la chiarificazione dei concetti logici dando il via a una branca importantissima della logica matematica nota come teoria dei modelli.

La comparsa dell'implicazione materiale si può fare risalire ai logici stoici, e precisamente a Filone di Megara (IV sec. a. C.). Tale nozione di implicazione è stata ampiamente dibattuta sin dalla antichità e agli albori della logica matematica, con controversie talora molto accese tra i logici.

Nel 1930 Gödel dimostrò la completezza deduttiva del calcolo logico predicativo, risalente essenzialmente a Frege. Negli stessi anni le ricerche di Turing e Church fondavano la teoria matematica della calcolabilità. Gli anni Trenta si pongono quindi come periodo di transizione tra la prima fase della logica matematica e la fase dei grandi risultati che la trasformeranno in disciplina matematica matura e fondamentale.

Il programma, intrapreso da D. Hilbert e la sua scuola, di formalizzazione di tutta la matematica nell'ambito di una teoria aritmetica predicativa fallì quasi subito, quando, nel 1931, Gödel dimostrò il suo famoso teorema di incompletezza: non esiste alcun insieme finito di proposizioni, esprimibili con formule predicative, da cui discendono tutte le proposizioni aritmetiche vere.

Un risultato analogo fu dimostrato dopo poco tempo da Tarski. Entrambe le dimostrazioni di Gödel e Tarski sono basate su metodi diagonali analoghi a quello con cui si dimostra la paradossalità della classe di Russell. L'indecidibilità della logica predicativa fu dimostrata nel 1936 da Church come conseguenza dei suoi studi sulla nozione di effettiva calcolabilità.

La logica predicativa risulta il linguaggio naturale entro cui esprimere formalmente le teorie della matematica classica. Nuove teorie e applicazioni hanno richiesto tuttavia l'elaborazione di altre logiche. Per esempio, la

¹ Trad. it. *Ideografia*, in *Logica e aritmetica*, a cura di C. Mangione, Boringhieri, Torino 1977.

logica intuizionista è stata introdotta per meglio esprimere il modo di operare matematico costruttivo. Sulla base della logica intuizionista sono state introdotte varie logiche per descrivere nuovi sistemi di programmazione. La mole di ricerche in questo settore è enorme e in continua espansione, come testimoniano i ponderosi *Handbooks* in parecchi volumi comparsi di recente sui vari settori applicativi della logica matematica (linguaggio naturale, intelligenza artificiale, programmazione). (Cfr. Bibliografia).

5.2. Relazioni strutturali tra modelli e teorie

Su modelli e teorie si possono definire nozioni che sono alla base di varie costruzioni sviluppate entro la teoria dei modelli e il cui studio non è stato ancora affrontato in modo sistematico, pur essendo rilevante in diversi contesti di applicazione delle formalizzazioni logiche e soprattutto nella specifica formale di sistemi complessi. Prima di entrare nei dettagli vorremmo sottolineare un aspetto interessante che illustra molto bene il ruolo della formalizzazione nello sviluppo della logica matematica. Usualmente si considera la teoria dei modelli come la parte più strettamente matematica della logica matematica. Nel famoso testo di Chang-Keisler² tale disciplina veniva sinteticamente descritta come *algebra universale + logica*, ovvero un'estensione dello studio generale delle strutture matematiche in cui il linguaggio predicativo sostituisce quello equazionale. Tale prospettiva coglie solo un aspetto. Un paragone forse più illuminante si trova in un recente testo di Hodges,³ in cui si afferma che la teoria dei modelli è una generalizzazione della geometria algebrica, ove si descrivono proprietà e relazioni geometriche attraverso equazioni e sistemi di equazioni algebriche (su *corpi*, negli sviluppi più astratti). Analogamente in teoria dei modelli la struttura di riferimento è una qualsiasi struttura matematica e il linguaggio non è equazionale, ma predicativo. Solitamente si attribuisce a Cartesio il merito di avere individuato la corrispondenza tra la retta e l'insieme dei numeri reali. Si tratta di un evidente errore storico, perché come noto, la definizione numerica del sistema dei reali ad opera di Weiestrass, Dedekind, Cauchy, è di molto posteriore a Cartesio, per il quale la nozione di numero rimase quella geometrica della matematica greca, quale rapporto di segmenti. Il merito di Cartesio fu quello di individuare un linguaggio algebrico con cui esprimere e studiare le usuali relazioni geometriche; la corrispondenza numeri-punti è una lettura a posteriori del metodo cartesiano. L'introduzione del linguaggio algebrico in geometria ha dato avvio a una grande rivoluzione matema-

² C. C. Chang e H. J. Keisler, *Model Theory*, North-Holland, Amsterdam-London 1973 [trad. it. *Teoria dei modelli*, Boringhieri, Torino 1980].

³ W. Hodges, *A Shorter Model Theory*, Cambridge University Press, Cambridge 1977.

rica. Quello che la logica predicativa ha permesso di fare con la teoria dei modelli è quindi un passo ulteriore nella linea cartesiana. Come detto prima, la generalizzazione della teoria dei modelli è duplice: strutture qualsivoglia hanno sostituito lo spazio e il linguaggio predicativo ha sostituito quello algebrico equazionale.

Lo studio di molte operazioni e relazioni strutturali riconduce al concetto di traduzione tra sistemi simbolici diversi e in ultima analisi alla rappresentazione logica di relazioni entro modelli e teorie.

Per esempio, i concetti algebrici di morfismo, isomorfismo, sottostruttura, congruenza, quoziente e modelli di termini si generalizzano in modo naturale ai modelli di una data segnatura tramite la nozione chiave di formula *f-preservata*.

Data una funzione f dal dominio D di un Σ -modello $\mathcal{M}$ a quello di un altro $\mathcal{M}'$, diciamo che una formula $\varphi(a, b, \dots)$ di $F_{\Sigma, D}$ è *f-preservata* se $\mathcal{M} \models \varphi(a, b, \dots) \Rightarrow \mathcal{M}' \models \varphi(f(a), f(b), \dots)$ per ogni $a, b, \dots \in D$. Data una teoria Φ , una funzione f tra (domini di) modelli è una *Φ -funzione* se tutte le formule di Φ sono *f-preservate*.

La nozione di *Σ -morfismo* si può formulare in modo logico dicendo che un morfismo è una funzione tra due Σ -modelli $\mathcal{M}_1, \mathcal{M}_2$ di domini D_1, D_2 che preserva tutte le formule atomiche sulla segnatura di F_{Σ, D_1} . Un *Σ -isomorfismo* è un Σ -morfismo biunivoco. Un concetto più forte di morfismo è quella di *Σ -immersione* come funzione iniettiva tra Σ -modelli che preserva i letterali. Infine una *Σ -immersione elementare*, da un Σ -modello di dominio D a un altro Σ -modello, è un'immersione che preserva tutte le formule di $F_{\Sigma, D}$. Una *Σ -sottostruttura* è individuata da un sottoinsieme del dominio la cui funzione identica di inclusione nel dominio è un'immersione. Se tale immersione è elementare si ha una *Σ -sottostruttura elementare*. Due Σ -modelli sono *elementarmente equivalenti* se verificano le stesse formule sulla segnatura Σ . Si verifica che un Σ -modello $\mathcal{M}$ è *sottostruttura elementare* di un Σ -modello $\mathcal{M}'$ sse $\text{Th}(\mathcal{M}_\Delta) \subseteq \text{Th}(\mathcal{M}'_\Delta)$ e che $\mathcal{M}$ è un'immersione elementare in $\mathcal{M}'$ sse $\mathcal{M}$ è isomorfo a una sottostruttura elementare di $\mathcal{M}'$.

Una nozione strettamente connessa alle immersioni elementari è quella di *model-completezza*, introdotta da Robinson per studiare la completezza di teorie. Una teoria è *model-completa* se un'immersione tra due suoi modelli è sempre elementare.

Una *Σ -congruenza* su un Σ -modello $\mathcal{M}$ è una relazione di equivalenza tale che: 1) tutti gli elementi di ogni sua classe di equivalenza possono essere interpretati in uno stesso individuo di un Σ -modello $\mathcal{M}'$ e 2) la funzione di interpretazione è un Σ -morfismo da $\mathcal{M}$ in $\mathcal{M}'$. In tal caso il modello $\mathcal{M}'$ dicesi *Σ -quoziente* di $\mathcal{M}$ (rispetto alla congruenza considerata). Il modello di Herbrand di una Σ -teoria Φ dicesi un *Σ -modello di termini*. Ogni modello è quoziente di un opportuno modello di termini.

Nuove nozioni, rispetto a quelle algebriche classiche, intervengono quando si confrontano modelli e teorie di signature diverse. Le più immediate sono quelle di *riduzione* ed *estensione* in cui si riduce o si estende la segnatura con nuovi simboli e di conseguenza si riduce o si estende un modello o una teoria sulla segnatura considerata. La riduzione di un Σ -modello $\mathcal{M}$ alla sottosegnatura Σ' si indica con $\mathcal{M}|\Sigma'$ e quella di una Σ -teoria Φ con $\Phi|\Sigma'$.

Un'estensione Φ' di una teoria Φ si dice *estensione conservativa* se tutte le formule della segnatura di Φ che sono deducibili in Φ lo sono anche in Φ' . Consideriamo un'estensione di una teoria in cui si aggiungono *definizioni* di nuovi simboli, ovvero $R(x, \dots) \leftrightarrow \varphi(x, \dots)$ se R è un nuovo simbolo relazionale, e formule del tipo $x = c \leftrightarrow \varphi(x)$, o $x = f(\dots) \leftrightarrow \varphi(x, \dots)$ nel caso di una nuova costante c o di un nuovo simbolo di funzione f , dove φ sono formule della segnatura non estesa. Per completare tali definizioni si aggiungono inoltre delle *condizioni di correttezza* facilmente formulabili (esistenza ed unicità degli oggetti definiti). In tali ipotesi, se la teoria estesa Φ' è una estensione conservativa di Φ , essa si dice più propriamente un'*estensione definizionale* di Φ .

Un'*interpretazione definizionale* di una teoria Φ in una teoria Ψ è un'estensione definizionale Ψ' di Ψ da cui conseguono tutte le formule di Φ .

Due teorie sono *definizionalmente equivalenti* se sono sottoteorie di una teoria (nell'unione delle due signature) che è estensione definizionale di entrambe.

Un esempio particolarmente semplice di equivalenza definizionale si ha tra una teoria dell'addizione usuale sui naturali, espressa con un simbolo di funzione binaria, e un'altra teoria in cui la somma è assiomatizzata tramite un simbolo di relazione ternaria. Ovviamente si tratta di un mero cambiamento sintattico. Si verifica facilmente che le due teorie sono definizionalmente equivalenti.

Come si dimostra che un'estensione Φ' di una teoria Φ non è definizionale? Basta determinare due modelli distinti di Φ' che ristretti alla segnatura di Φ determinino uno stesso modello di tale teoria. Infatti, in tal caso le formule definitorie non verificano la condizione di unicità e quindi tali condizioni non possono valere nella teoria Φ' .

Esercizio 5.1 *Si dia una teoria assiomatica dei naturali con la somma; si determini una sua estensione che assiomatizza il prodotto; si dimostri che la seconda teoria non può essere un'estensione definizionale della prima.*

Un altro fenomeno interessante è costituito dalla *relativizzazione* di un modello o di una teoria entro un altro modello o teoria. Sia P un predicato unario e φ una formula predicativa. Definiamo per induzione la relativizza-

zione φ_P di tale formula al predicato P . Se φ è atomica $\varphi_P = \varphi$; $(\neg \varphi)_P = \neg \varphi_P$; $(\varphi \vee \psi)_P = \varphi_P \vee \psi_P$; $(\varphi \wedge \psi)_P = \varphi_P \wedge \psi_P$; $(\forall x \varphi(x, \dots))_P = \forall x(P(x) \rightarrow \varphi_P(x, \dots))$; $(\exists x(\varphi(x, \dots)))_P = \exists x(P(x) \wedge \varphi_P(x, \dots))$. Data una teoria Φ e un predicato unario P , la sua P -relativizzata è costituita dall'insieme delle formule che sono P -relativizzate di formule di Φ . Consideriamo due modelli $\mathcal{M}'$, $\mathcal{M}''$ di domini D' , D'' tali che $\mathcal{M}'$ sia sottostruttura di $\mathcal{M}''$. Aggiungiamo alla segnatura di $\mathcal{M}''$ un nuovo predicato unario la cui interpretazione coincida con D' . In tal modo possiamo comporre le due strutture in una struttura $\mathcal{M}$ che ristretta alla segnatura di $\mathcal{M}''$ coincida con questa struttura e sia tale che una formula φ valga in $\mathcal{M}'$ sse φ_P vale in $\mathcal{M}$. In tal caso $\mathcal{M}'$ si dice un *ridotto relativizzato* di $\mathcal{M}$ e si indica con $\mathcal{M}_P$.

In modo analogo si può definire una *somma relativizzata* di due modelli, considerando l'unione dei due domini, aggiungendo due predicati di relativizzazione e ottenendo un nuovo modello dove una formula vale nel modello di partenza se solo se la corrispondente relativizzata vale nella somma relativizzata. Questo metodo si presta a costruire modelli composti da varie parti. Il passaggio da modelli con predicati di relativizzazione a *modelli sortati* o eterogenei è molto semplice. Dato un modello con predicati di relativizzazione, si introducono tante *sorte* quanti sono i predicati di relativizzazione e per ciascuna sorta un insieme di variabili. A questo punto una formula φ con una variabile di sorta corrispondente al predicato P è considerata come abbreviazione della formula φ_P .

Esercizio 5.2 Si assiomatizzi la definizione di topologia su un insieme, utilizzando una sorta per gli intorni e una sorta per gli elementi (per gli intorni si impongano assiomi mutuati opportunamente da ZFC).

Esercizio 5.3 Si assiomatizzi la definizione di multigrafo orientato e di categoria, utilizzando due sorte.

Un *arricchimento espressivo* di un modello o di una teoria consiste in un'estensione della classe dei termini o delle formule del modello o della teoria. Anche in questo caso si può avere un arricchimento definizionale o no. Un esempio di arricchimento definizionale si ha introducendo nella teoria degli insiemi ZFC dei termini per esprimere operazioni su classi, sortando gli individui in insiemi e classi, aggiungendo un assioma per asserire che ogni insieme è una classe e formulando (in modo molto più semplice) gli assiomi di ZFC utilizzando le operazioni su classi. Questo procedimento conduce essenzialmente da ZFC alla teoria NBG.

Altri esempi di arricchimenti definizionali sono costituiti dagli *operatori descrittivi* di scelta. L'operatore di scelta ε di Hilbert, data una formula $\varphi(x)$

con una variabile libera, individua un individuo a scelta che la soddisfa (se esiste). La sua definizione è (per ogni formula $\varphi(x)$ con una variabile libera):

$$\psi(\varepsilon x. \varphi(x)) \equiv \exists y \psi(y) \wedge \varphi(y).$$

In modo analogo l'operatore $!$ di Peano-Russell determina l'unico individuo (se esiste) che soddisfa una data formula.

Altri esempi di arricchimenti definizionali sono costituiti da tutti gli operatori tipici dell'analisi (limite, derivata, integrale). Una loro trattazione formale si trova nel testo di Kalish e Montague, dove è presentata una teoria completamente formalizzata della convergenza sui reali utilizzando arricchimenti definizionali di teorie predicative.

Altri arricchimenti definizionali molto utili si hanno quando si introducono simboli di operazioni parziali come abbreviazioni di relazioni. Per esempio, sia $R(x, y)$ una relazione binaria; allora si può porre $f_R(x) = y \leftrightarrow \exists! y R(x, y)$. In tal modo $f_R(x)$ non è un termine in senso stretto, ma possiamo di fatto usarlo come tale utilizzando la definizione considerata. Questo è un metodo, adottato spesso implicitamente, per esprimere operazioni parziali in teorie predicative.

Esercizio 5.4 *Si dia un'assiomatizzazione delle pile (push, pop, top) e delle code (first, rest, add) su prefissati elementi, utilizzando due sorte ed arricchimenti definizionali per operazioni parziali.*

Arricchimenti non definizionali sono quelli in cui si estendono le formule predicative per esprimere meccanismi computazionali tipici della programmazione. Consideriamo un termine $t(x)$ con una variabile e una formula $\varphi(x)$ con una variabile libera. Indichiamo con $t^\varphi(x)$ un nuovo termine che intuitivamente esprime l'iterazione di t , ovvero $t(t(t(\dots x \dots)))$, finché vale la formula φ . La definizione di un tale termine non è *esplicita* (*definiendum* $\leftrightarrow$ *definiens*, ove il *definiendum* non occorre come parte del *definiens*), ma *implicita* (ecco perché non si tratta di arricchimento definizionale):

$$(\neg \varphi(x) \rightarrow t^\varphi(x) = x) \wedge (\varphi(x) \rightarrow t^\varphi(x) = t^\varphi(t(x))).$$

Come si capisce, un tale costrutto esprime un meccanismo di programmazione di tipo *while* ("finché vale φ si applichi t ") e quindi permette di costruire dei programmi. Ovviamente il discorso può essere ulteriormente esteso fino a giungere a vere e proprie semantiche logiche di linguaggi programmativi. Tale via è stata seguita in varie direzioni e porta con prospettive anche molto diverse a teorie logico-algebriche della programmazione, all'identificazione di nuove logiche, a meccanismi di calcolo tramite deduzione e via dicendo.

Altri importanti rapporti strutturali tra modelli e teorie intervengono nella costruzione di teorie composte da vari moduli e nella determinazione

di modelli particolari di date teorie. Tale settore ha ricevuto un notevole impulso dallo sviluppo dei cosiddetti *linguaggi di specifica* (quali OBJ, CLEAR, OBSCURE, GÖDEL) di tipi di dati e programmi. Consideriamo per esempio la teoria delle sequenze e la teoria dei naturali. Come comporre per ottenere la teoria delle sequenze dei naturali? In situazioni del genere intervengono i concetti di *parametro*, *polimorfismo*, *incapsulamento*, *astrazione*, *ereditarietà*.

Un altro aspetto cruciale consiste nei metodi con cui, data una teoria, si sceglie un suo particolare modello come modello canonico per certi scopi e lo si *costruisce con procedimenti effettivi*. In questo ambito si sono sviluppati metodi logico-algebrici per la costruzione di *modelli generici*, *minimali* o *iniziali*, *massimali* o *finali* (rispetto a opportuni ordinamenti tra strutture). I principi generali che sovrintendono a tali costruzioni sono intrinsecamente legati alla natura dei linguaggi logici, alle teorie e ai modelli con essi descrivibili.

Nella letteratura si trovano varie formulazioni del concetto di *interpretazione*, legate ad applicazioni specifiche; per esempio, Tarski e i suoi seguaci hanno fatto un uso massiccio di interpretazioni per ottenere risultati di indecidibilità di teorie. Qui presentiamo alcuni schemi generali entro cui rientrano varie nozioni di interpretazione.

Date due teorie Φ, Φ' di signature Σ, Σ' , un'interpretazione della prima nella seconda è una funzione $g: F_{\Sigma}(V) \rightarrow F_{\Sigma'}(V)$ (V è un insieme di variabili) tale che

$$\Phi \models \varphi \Leftrightarrow \Phi' \models g(\varphi)$$

ove g può essere definita tramite una preliminare funzione di traduzione dei termini di Σ in quelli di Σ' .

Esercizio 5.5 *Si verifichi che un'interpretazione definizionale di una teoria in un'altra determina un'interpretazione secondo la definizione appena data.*

Nel caso di interpretazioni tra modelli bisogna utilizzare due funzioni di traduzione: una per gli individui e una per le formule. Consideriamo due modelli $\mathcal{M}, \mathcal{M}'$ di domini D, D' . Indichiamo con $\text{Seq}(\mathcal{M})$ le sequenze finite di elementi del dominio di un modello $\mathcal{M}$ e con $\text{Seq}(\mathcal{M}')$ quelle del modello $\mathcal{M}'$. Sia f una funzione che manda D in $\text{Seq}(\mathcal{M}')$ (f si dice *n-dimensionale* se l'immagine di un elemento di D è sempre una n -pla su D'). Una tale funzione si estende naturalmente a una funzione f^* da $\text{Seq}(\mathcal{M})$ in $\text{Seq}(\mathcal{M}')$. Indichiamo con $\text{Rel}(\mathcal{M})$ e $\text{Rel}(\mathcal{M}')$ le relazioni rappresentabili rispettivamente nei due modelli. Un'interpretazione covariante di $\mathcal{M}$ in $\mathcal{M}'$ è una coppia (f, g) di funzioni tali che

$$f: D \hookrightarrow \text{Seq}(\mathcal{M}')$$

$$g: \text{Rel}(\mathcal{M}) \rightarrow \text{Rel}(\mathcal{M}')$$

e per le quali valga la seguente condizione di commutazione, per ogni $\alpha \in \text{Seq}(\mathcal{M})$, $R \in \text{Rel}(\mathcal{M})$:

$$\alpha \in R \Leftrightarrow f^*(\alpha) \in g(R).$$

Un'interpretazione controvariante di $\mathcal{M}$ in $\mathcal{M}'$ è una coppia (f, g) di funzioni tali che

$$f: D' \rightarrow \text{Seq}(\mathcal{M})$$

$$g: \text{Rel}(\mathcal{M}) \rightarrow \text{Rel}(\mathcal{M}')$$

e per le quali la condizione di commutazione diventi, per ogni $\alpha \in \text{Seq}(\mathcal{M}')$, $R \in \text{Rel}(\mathcal{M})$,

$$f^*(\alpha) \in R \Leftrightarrow \alpha \in g(R).$$

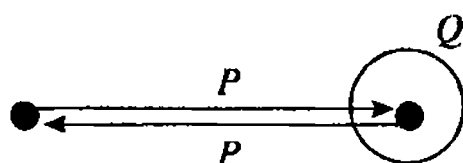
Esercizio 5.6 *Si dia un'interpretazione covariante e una controvariante del modello SEQ nel modello AR.*

Suggerimento Si usi la funzione β di Gödel.

Capitolo 6

Esercizi finali

Esercizio 6.1 Si consideri il seguente modello sulla segnatura $\{P \dashv\!\!\dashv, Q \dashv\!\!\dashv\}$:



Si dica quali delle seguenti formule sono vere e quali sono false in tale modello, giustificando le risposte:

1. $\forall xy(P(x, x) \rightarrow P(x, y))$
2. $\forall xy(P(x, y) \rightarrow P(y, x))$
3. $\forall xy(P(x, y) \wedge P(y, x) \rightarrow Q(x))$
4. $\forall xy(P(x, y) \rightarrow \exists xQ(x))$
5. $\forall xyP(x, y)$
6. $\forall xy(P(x, y) \vee Q(y))$
7. $\exists xy(Q(x) \rightarrow P(x, y))$
8. $\exists x \neg P(x, x)$
9. $\forall x(P(x, x) \vee Q(x)).$

Esercizio 6.2 Si consideri il modello raffigurato dal diagramma del primo esercizio sulla segnatura $\{P \dashv\!\!\dashv, Q \dashv\!\!\dashv\}$. Si determini:

1. quali sono le proposizioni sulla segnatura considerata, di complessità 2 e con un solo connettivo;
2. quali sono le proposizioni di complessità 2 che valgono nel modello;
3. quali sono le proposizioni di complessità 2 e senza connettivi binari, che valgono nel modello.

Esercizio 6.3 *Si dimostri con il metodo dei tableau che i seguenti schemi predicativi sono logicamente validi:*

1. $\forall x(Px \wedge Qx \rightarrow Rx) \rightarrow \forall x(Px \rightarrow (Qx \rightarrow Rx))$
2. $\forall x(Px \wedge (Px \rightarrow \exists yRy) \rightarrow (\exists yRy \wedge Px))$
3. $\forall x(Px \rightarrow (Qx \rightarrow Rx)) \rightarrow (\forall x(Px \wedge Qx) \rightarrow \forall xRx)$
4. $\forall x(Px \rightarrow \exists yQy \wedge \forall yRy) \rightarrow \forall x(Px \wedge \exists yQy) \wedge \forall x(Px \rightarrow Rx)$
5. $\forall x(Px \vee \neg Qx) \wedge \exists y(Py \vee Qy) \rightarrow \exists xPx.$

Esercizio 6.4 *Si pongano in forma di Skolem le seguenti formule:*

1. $\forall x(Px \wedge Qx) \rightarrow (\forall xPx \rightarrow \forall xQx)$
2. $\forall x(Px \wedge \exists yQy) \rightarrow (\exists xPx \rightarrow \exists xQx)$
3. $\exists xPx \rightarrow \exists xQx \vee \forall xPx$
4. $\forall x(Px \rightarrow \exists yQy \wedge \forall yRy) \rightarrow \forall x(Px \wedge \exists yQy) \wedge \forall x(Px \rightarrow Rx)$
5. $\forall x(Px \rightarrow \exists y(Qy \wedge Ry)) \rightarrow (\forall x(Px \wedge Qx) \rightarrow \forall x(Px \wedge Rx)).$

Esercizio 6.5 *Si dimostri con il metodo di deduzione naturale che i seguenti schemi proposizionali sono logicamente validi:*

1. $(\varphi \wedge (\varphi \rightarrow \psi)) \rightarrow (\psi \wedge \varphi)$
2. $\neg \varphi \rightarrow ((\varphi \vee \psi) \rightarrow \psi)$
3. $(\varphi \rightarrow (\gamma \rightarrow \psi)) \rightarrow (\varphi \wedge \gamma \rightarrow \psi)$
4. $(\varphi \rightarrow (\gamma \wedge \psi)) \rightarrow (\varphi \rightarrow \gamma) \wedge (\varphi \rightarrow \psi)$
5. $(\psi \rightarrow \varphi) \rightarrow (\gamma \wedge \psi \rightarrow \varphi).$

Esercizio 6.6 *Si rappresentino logicamente le seguenti proposizioni nel modello aritmetico AR:*

1. *Ogni numero primo il cui successore è multiplo di 4 è somma di due quadrati.*
2. *Tra un numero e il suo doppio vi è sempre un numero primo.*
3. *m e k hanno in comune con n gli stessi divisori pari.*
4. *x è un primo di Mersenne, cioè un primo che è predecessore di una potenza di 2.*
5. *Il resto della divisione di x^2 per 4 è o zero o uno, ed è uguale a uno esattamente quando x è dispari.*

Esercizio 6.7 *Rappresentare logicamente nel modello SEQ le seguenti proposizioni:*

1. *Nella sequenza α tutte le sottostringhe non interrotte di 1, poste tra due numeri diversi da 1, hanno una lunghezza pari.*
2. *α è una stringa binaria che inizia con 0 finisce con 1 e non contiene occorrenze consecutive della stessa cifra.*
3. *Nella sequenza α vi sono due occorrenze non contigue della sequenza β .*
4. *Nella sequenza α ogni occorrenza della stringa β sta tra (è preceduta e seguita da) due stringhe di lunghezza pari.*
5. *Nella sequenza α ogni occorrenza di un numero pari è preceduta da quella di un numero dispari, ma non tutte le occorrenze di un numero dispari sono seguite da un pari.*

Esercizio 6.8 *Si consideri la teoria AX con i seguenti assiomi:*

1. $\forall xy(R(x, y) \rightarrow Q(x))$
2. $\forall xy(R(x, y) \rightarrow R(y, x)).$

Si determini (rispettivamente mediante i tableau o mediante contromodello) quale delle due formule che seguono è una conseguenza logica di AX e quale non lo è:

1. $\forall xy(R(x, y) \rightarrow (Q(x) \wedge Q(y)))$
2. $\forall xy((Q(x) \wedge Q(y)) \rightarrow R(y, x)).$

Esercizio 6.9 *Si consideri la seguente teoria:*

1. $\forall x(Q(x) \rightarrow \exists yP(x, y) \wedge \neg \forall xT(x))$
2. $\forall x(T(x) \wedge \exists yT(y) \rightarrow \forall xyP(x, y)).$

Si determini una sua forma di Skolem e se ne determini l'universo di Herbrand associato.

Esercizio 6.10 *Si consideri la teoria con i seguenti assiomi:*

1. *Elena ha una sorella bionda che è sposata con un italiano.*
2. *Ogni italiano che è sposato con una donna bionda ama una donna castana.*
3. *Vi è un italiano che ama una donna castana.*

a) *Si esprima tale teoria in forma predicativa utilizzando la costante individuale e per Elena, e i simboli S, B, C, M, A, I per i predicati: $S(x, y) \leftrightarrow x$ è sorella di y , $B(x) \leftrightarrow x$ è bionda, $C(x) \leftrightarrow x$ è castana, $M(x, y) \leftrightarrow x$ è sposato/a con y , $A(x, y) \leftrightarrow x$ ama y , $I(x) \leftrightarrow x$ è italiano.*

b) Si consideri la teoria predicativa data e si dimostri con il metodo dei tableau o con quello della risoluzione che il terzo assioma è conseguenza logica dei primi due. Si stabilisca inoltre se la teoria è completa. Infine, si dimostri, utilizzando un contromodello finito che da essa non segue logicamente la proposizione: “Ogni donna bionda non è castana”. Qual è un contromodello minimale sufficiente a tal riguardo?

Esercizio 6.11 Si consideri la teoria con i seguenti assiomi:

1. $\forall xyz(D(x, y) \wedge T(z, x) \rightarrow T(z, y))$
2. $\forall x \exists y T(x, y)$
3. $\forall x \neg T(x, x)$
4. $\forall x D(x, x)$
5. $\forall x \exists y \neg D(y, x)$.

a) Si determini se il quinto assioma segue dagli altri assiomi.

b) Si determini se il quarto assioma segue dagli altri assiomi.

In caso di risposta positiva si dia una dimostrazione sia con il metodo dei tableau che con quello della risoluzione. In caso di risposta negativa si dia un contromodello.

Esercizio 6.12 Si consideri la segnatura con simbolo di predicato binario R e simbolo di predicato unario Q . Consideriamo in tale segnatura la seguente formula φ :

1. $\forall xy(R(x, y) \rightarrow (Q(x) \wedge \neg Q(y)))$.

Si mostri con il metodo dei tableau e con quello di risoluzione che

1. $\forall xyz(R(x, y) \rightarrow \neg R(z, x))$
2. $\neg \exists x R(x, x)$.

Si fornisca un modello di φ e si dimostri che le seguenti formule non sono sue conseguenze logiche:

1. $\exists x \forall y R(x, y)$
2. $\neg \forall xyuv \exists (R(x, u) \wedge R(y, v) \rightarrow \exists z R(x, z) \wedge R(y, z))$.

Esercizio 6.13 Consideriamo la segnatura con un simbolo di operazione binaria $\cdot$, un simbolo di costante nil , e due simboli di predicato C e R . Consideriamo i seguenti assiomi T :

1. $\forall x C(nil, x, x)$

2. $\forall x, y, z, u [C(x, y, z) \rightarrow C(u \cdot x, y, u \cdot z)]$
3. $R(\text{nil}, \text{nil})$
4. $\forall x, y, u, z [R(x, y) \wedge C(y, u \cdot \text{nil}, z) \rightarrow R(u \cdot x, z)].$

a) Si mostri che

$$T \models \forall x, y [R(x \cdot (y \cdot \text{nil}), y \cdot (x \cdot \text{nil}))]$$

fornendo due dimostrazioni, una con il metodo dei tableau e una con il metodo di risoluzione.

b) Si stabilisca se dagli assiomi dati nel punto precedente segue:

$$\forall x, y (R(x, y) \rightarrow R(y, x)).$$

Esercizio 6.14 Consideriamo i seguenti assiomi T nel linguaggio della riproduzione sessuata comprendente i predicati unari $M(x)$, $F(x)$ (x è maschio, x è femmina) e il predicato binario $G(x, y)$ (x è genitore di y):

1. $\forall x \exists y (M(y) \wedge G(y, x))$
2. $\forall x \exists y (F(y) \wedge G(y, x))$
3. $\forall x (F(x) \vee M(x))$
4. $\forall x (F(x) \rightarrow \neg M(x)).$

Si stabilisca se:

- a) $T \models \forall x \exists y (\neg F(y) \wedge G(y, x))$
- b) $T \models \exists x \forall y (G(x, y))$

sviluppando una dimostrazione via tableau oppure un controesempio.

Esercizio 6.15 Si risolva uno dei due punti dell'esercizio precedente con il metodo di risoluzione. A tal fine si introducano le funzioni di Skolem, si pongano le ipotesi e la negazione della tesi in forma di clausole, e si ottenga una contraddizione tramite la risoluzione.

Esercizio 6.16 Si formalizzi con una formula del primo ordine nel linguaggio della riproduzione sessuata, con l'aggiunta del simbolo di costante "Carla", il fatto che Carla ha un solo zio e che lo zio di Carla non ha figli (lo zio è il fratello o la sorella di uno dei due genitori).

Esercizio 6.17 Consideriamo i seguenti assiomi T nel linguaggio contenente il predicato unario R e i predicati binari A e P :

1. $\forall xy (P(x, y) \rightarrow \neg \exists z (A(z, x) \wedge A(z, y)))$

2. $\forall xy(P(x, y) \rightarrow R(x) \wedge R(y))$
3. $\forall x(R(x) \rightarrow \exists yA(y, x))$
4. $\exists xR(x)$.

Una possibile interpretazione è: $R(x) \equiv$ “ x è una retta”, $P(x, y) \equiv$ “ x e y sono due rette parallele”, $A(x, y) \equiv$ “il punto x appartiene alla retta y ”. Si stabilisca se:

- a) $T \models \forall x \neg P(x, x)$
- b) $T \models \forall xyz(P(x, y) \wedge P(y, z) \rightarrow P(x, z))$

sviluppando una dimostrazione formale oppure un controesempio.

Esercizio 6.18 *Un numero si dice triangolare se è della forma $n(n+1)/2$. Si formalizzi con una formula del primo ordine il fatto che ogni quadrato è la somma di due numeri triangolari. Si usi un linguaggio contenente le costanti 0, 1, la relazione $P(x, y, z)$, interpretata come “ z è il prodotto di x e y ”, e la relazione $A(x, y, z)$, interpretata come “ z è la somma di x e y ”.*

Esercizio 6.19 *Consideriamo i seguenti assiomi T nel linguaggio contenente due simboli di relazione binaria I e V :*

1. $I(x, z) \wedge I(y, z) \rightarrow V(x, y)$
2. $V(x, y) \rightarrow V(y, x)$
3. $I(x, x)$.

Si trovi un modello infinito di T e si stabilisca se:

- a) $T \models \forall xy(I(x, y) \rightarrow V(x, y))$
- b) $T \models \forall xyz(I(x, y) \wedge I(y, z) \rightarrow I(x, z))$

sviluppando una dimostrazione formale oppure un controesempio.

Esercizio 6.20 *Si ponga T del punto precedente in forma a clausole e si dimostri, usando il principio di risoluzione, che T con l'aggiunta delle clausole $\{I(x, y), \neg V(x, y)\}$ è inconsistente.*

Esercizio 6.21 *Rappresentare logicamente in una teoria monoidale sui simboli $\{a, b\}$ i seguenti linguaggi su $\{a, b\}^*$:*

1. $\{ab^n b^m a^m : n, m \in \omega\}$
2. $\{a^{2^n} b^{n+1} : n \in \omega\}$.

Esercizio 6.22 *Rappresentare logicamente in una teoria monoidale sui simboli $\{a, b\}$ il seguente linguaggio su $\{a, b\}^*$:*

$$\{a^n b^{(n^2)} : n \in \omega\}$$

Suggerimento Si utilizzi l'uguaglianza $(n + 1)^2 = n^2 + 2n + 1$.

Esercizio 6.23 *Rappresentare logicamente in una teoria monoidale sui simboli $\{a, b\}$ il linguaggio delle stringhe su $\{a, b\}^*$ in cui il numero delle occorrenze di a uguaglia il numero di occorrenze di b .*

Esercizio 6.24 *Rappresentare logicamente in una teoria monoidale sui simboli $\{a, b\}$ la seguente relazione su $\{a, b\}^*$:*

La stringa α ha lunghezza doppia della stringa β .

Suggerimento Si utilizzi un predicato $S(x)$ per indicare che x è composta da un solo simbolo e $D(x, y)$ per indicare che x è lunga il doppio di y .

1. Introduzione

Vi parlerò di cose piuttosto insolite: del potere innovativo delle grandi idee, di teorie, e del calcolatore come concetto filosofico.

Noi tutti sappiamo che i computer sono strumenti utilissimi nel mondo reale. Ci pagano gli stipendi! Ma chi crederebbe – in effetti sto esagerando – che il computer è stato inventato per aiutarci a chiarire questioni filosofiche sui fondamenti della matematica?

Per quanto possa sembrare assurdo, c'è un fondo di verità in questa affermazione. Vi sono un gran numero di fili sottili che legano gli odierni computer e la loro tecnologia alla logica matematica e alle questioni più generali circa i limiti e le possibilità della matematica.

Turing, il pioniere del calcolatore, fu ispirato proprio da tali questioni. Stava cercando di risolvere un problema posto da Hilbert che riguardava la filosofia della matematica, quando ebbe l'idea della macchina che prese il suo nome e che non è altro che un modello matematico di calcolatore. All'epoca i calcolatori non c'erano ancora: fu proprio Turing in Inghilterra, a iniziare la costruzione.

Von Neumann, che ebbe un ruolo decisivo nel promuovere la tecnologia dei calcolatori negli Stati Uniti (sfortunatamente in relazione allo sforzo bellico e alla costruzione della bomba atomica), conosceva assai bene i lavori di Turing. In effetti, io stesso fui introdotto alle idee di Turing dagli scritti di von Neumann, che ne mettevano in luce la grande importanza.

¹ Traduzione, liberamente adattata, di una conferenza tenuta il 30 aprile 1999 presso UMass-Lowell, pubblicata con il titolo *A Century of Controversy over the Foundations of Mathematics* in C. S. Calude e G. Păun (a cura di), *Finite Versus Infinite: Contributions to an Eternal Dilemma*, Springer-Verlag, London 2000, pp. 75-100.

Quindi, quello che ho appena detto sulle origini del calcolatore non è propriamente una bugia, ma solo un frammento dimenticato di storia intellettuale. Lasciatemi cominciare dalle conclusioni di questo mio discorso. In un certo senso buona parte di queste ricerche è frutto del lavoro di Hilbert, famoso matematico tedesco degli inizi del xx secolo, il quale propose di formalizzare completamente la matematica, più precisamente il ragionamento matematico, cioè il processo deduttivo. Questa sua proposta fu un fallimento. Un glorioso fallimento!

Un fallimento clamoroso, poiché risultò che una tale formalizzazione è assolutamente impossibile (questo è, in sostanza, il famoso teorema di Gödel del 1931, di cui parlerò più avanti). Ma, per un altro verso, Hilbert ebbe ragione, perché il formalismo è stato uno dei più grandi successi del secolo. Non per ragionare matematicamente o dedurre verità matematiche, com'era nelle intenzioni di Hilbert, ma per programmare e calcolare. Nei linguaggi formali dei logici dell'inizio del secolo, concepiti per la matematica e la logica simbolica, è possibile in effetti ravvisare le prime forme di linguaggi di programmazione, del tutto simili ai formalismi con cui oggi molti lavorano e con cui, in modo più o meno diretto, tutti siamo continuamente a contatto: una tecnologia importantissima!

I formalismi per ragionare non funzionano: i matematici non ragionano con linguaggi formali. Ma i formalismi per calcolare e programmare sono in un certo senso la parte corretta di una visione che risale a Hilbert agli inizi del Novecento, introdotta per chiarire questioni epistemologiche e filosofiche della matematica. Vi racconterò ora questa storia che ha risvolti sorprendenti.

2. La crisi della teoria degli insiemi

Normalmente si pensa alla matematica pura come a qualcosa di statico e di immutabile, qualcosa di perfetto e di assolutamente corretto: la verità assoluta. La fisica può essere approssimata, ma in matematica le cose sono certe! Bene, le cose non stanno propriamente in questi termini. Nel Novecento, il secolo che ci lasciamo alle spalle, vi fu una grande disputa sui fondamenti stessi della disciplina, su come si dovesse fare matematica, su cosa fosse o non fosse matematicamente corretto e su cosa dovesse intendersi per dimostrazione valida. Fu quasi versato sangue su queste questioni. Nel fuoco delle polemiche qualcuno finì per andare fuori di senno. È un capitolo decisamente interessante della storia delle idee, di cui non si sa molto.

La gente è molto più informata sulle controversie riguardanti la teoria della relatività. Einstein all'inizio fu violentemente attaccato, come del resto la meccanica quantistica (l'altra grande rivoluzione della fisica novecentesca).

Ma ci sono state grandi rivoluzioni anche nella matematica pura, ed è di questo che vorrei parlarvi.

Tutto cominciò, poco più di un secolo fa, con l'invenzione da parte di Cantor, di una teoria degli insiemi infiniti. Fu un fatto realmente rivoluzionario, una cosa *estremamente* avventurosa. Vediamo perché.

Prendiamo, disse Cantor, 1, 2, 3, ... Tutti sappiamo che questi sono numeri. Aggiungiamo in fondo un numero infinito (lui lo chiamò ω):

$$1, 2, 3, \dots, \omega.$$

Quindi disse, perché mai fermarsi qui? Continuiamo a estendere la serie numerica, scrivendo omega più uno, omega più due, e così via infinite volte:

$$1, 2, 3, \dots \omega, \omega + 1, \omega + 2, \dots$$

Che cosa mettiamo alla fine? È ovvio, due volte omega (in effetti, per ragioni tecniche, sarebbe bene dire omega volte 2):

$$1, 2, 3, \dots \omega, \omega + 1, \omega + 2, \dots, 2\omega.$$

Avremo quindi due omega più uno, due omega più due, due omega più tre, due omega più quattro ...:

$$1, 2, 3, \dots \omega, \omega + 1, \omega + 2, \dots, 2\omega, 2\omega + 1, 2\omega + 2, 2\omega + 3, 2\omega + 4, \dots$$

Che cosa ci sarà dopo? Tre omega, quattro omega, cinque omega, sei omega, ...:

$$1, 2, 3, \dots \omega, \dots, 2\omega, \dots, 3\omega, \dots, 4\omega, \dots, 5\omega, \dots, 6\omega, \dots$$

Bene, cosa viene dopo tutti questi numeri? Omega per omega, cioè omega al quadrato!

Quindi si può continuare ancora, e avremo omega al quadrato più uno, omega al quadrato più sei, omega al quadrato più otto, ... Si può continuare ancora per molto, e qual è il numero interessante che viene dopo omega al quadrato? Omega al cubo!, e quindi omega alla quarta, alla quinta ecc.:

$$1, 2, 3, \dots \omega, \dots, \omega^2, \dots, \omega^3, \dots, \omega^4, \dots, \omega^5, \dots$$

E dopo un bel po' omega alla omega! E dopo ancora più passi, omega alla omega infinite volte:

$$1, 2, 3, \dots \omega, \dots, \omega^2, \dots, \omega^\omega, \dots, \omega^{\omega^{\omega^{\omega^{\dots}}}}, \dots$$

Se non erro, questo numero viene chiamato epsilon zero:

$$\epsilon_0 = \omega^{\omega^{\omega^{\omega^{\dots}}}}, \dots$$

Roba da far venire il capogiro! Ma dopo le cose si complicano ancora di più. E questa era proprio una piccolezza per Cantor, un semplice esercizio

di riscaldamento per la sua fatica più importante che consisteva nel misurare gli insiemi infiniti. Era una teoria immaginosa, e i matematici si divisero: alcuni ne furono entusiasti, altri pensarono che l'autore fosse da internare in un manicomio! In effetti, egli ebbe un esaurimento nervoso come risultato delle critiche che gli vennero mosse contro. Il suo lavoro ebbe un'influenza fortissima, portando alla nascita della topologia e di altre branche astratte della matematica del Novecento, ma fu anche bersaglio di critiche. C'è chi disse che era teologia, non realtà, una fantasticheria che non aveva nulla a che fare con la matematica seria. Cantor non raggiunse mai una posizione accademica prestigiosa e restò confinato per tutta la vita in università di secondo livello.

3. I paradossi di Bertrand Russell

Con Bertrand Russell, uno dei miei eroi giovanili, la crisi della matematica doveva peggiorare.

Bertrand Russell era un filosofo inglese e scrisse saggi bellissimi, molto personali, e sarà per questo, credo, che vinse il premio Nobel per la letteratura.

Aveva cominciato come matematico, era degenerato nella filosofia ed infine nelle discipline umanistiche; una discesa molto rapida! Comunque, scoprì una serie di imbarazzanti paradossi nella teoria di Cantor, poi nella logica stessa. Aveva trovato che in certi casi un ragionamento apparentemente ineccepibile porta a una contraddizione.

Io credo che Bertrand Russell abbia contribuito in modo determinante a creare la convinzione che la crisi della matematica era una cosa seria e in qualche modo doveva essere risolta. I paradossi che egli scoprì suscitarono un grande interesse, ma stranamente solo uno finì per essere associato al suo nome. (Per esempio, uno di questi paradossi è chiamato paradosso di Burali-Forti solo perché Russell, in una nota a piè di pagina del suo articolo, aveva dichiarato che a suggerirglielo era stato uno scritto di Burali-Forti. Nei lavori di questo autore, tuttavia, non ce n'è traccia).

A mio giudizio, si deve soprattutto a Bertrand Russell se i matematici presero coscienza del fatto che *c'era del marcio in Danimarca*, che la loro costruzione poggiava su qualcosa di profondamente sbagliato, che il ragionamento era alla bancarotta e che era urgente correre ai ripari. Anche dalla ricostruzione dello storico della matematica Alejandro Garciadiego emerge che Russell ebbe una parte decisiva, non solo nella formulazione del paradosso che va sotto il suo nome, ma anche nella scoperta dei paradossi di Burali-Forti e di Berry, di cui mise in luce il significato profondo. Spiegava a tutti quanto fossero importanti e che non si trattava di ingenui giochi di parole.

Il più famoso di tali enunciati è universalmente noto come paradosso di Russell. Considerate l'insieme di tutti gli insiemi che *non* sono elementi di

se stessi.² Domandatevi: “Questo insieme appartiene a se stesso o no?” Se è elemento di se stesso, allora per definizione non appartiene a se stesso, e viceversa. È come il barbiere di un piccolo sperduto villaggio che rade tutti gli uomini del villaggio che non si radono da sé. Sembra che non ci sia nulla di strano in questo barbiere, finché non ci si domanda: “Si rade da sé?” Egli si rade solo se non si rade da sé, quindi non può applicare a se stesso la regola di rasatura del villaggio.

Ora voi potreste dire: “Che ci importa di questo barbiere!” Era una regola stupida, e comunque ogni regola ha le sue eccezioni! Certo, ma quando si parla di *insiemi*, che sono concetti matematici, non è così facile liquidare il problema. Non è così facile glissare quando si costruisce un ragionamento che sembra corretto e si giunge a una contraddizione.

Tra l'altro, il paradosso di Russell è una versione insiemistica di un precedente paradosso, conosciuto nell'antica Grecia e detto da alcuni filosofi paradosso di Epimenide, ovvero paradosso del mentitore. Consideriamo una frase del tipo: “Ciò che sto dicendo è falso, è una bugia”, o anche “Questa proposizione è falsa”. Bene, è un'affermazione falsa? Se lo è, allora non corrisponde al vero; quindi vale il contrario di quel che dice; quindi è vera. Se invece è vera, allora siccome afferma di dire il falso, è vero che dice il falso; quindi è falsa. Ciascuna delle due possibilità porta a contraddizione.

Allora non si può raggiungere un valore di verità definitivo: ogni alternativa si commuta nell'altra e quindi l'affermazione del mentitore non può considerarsi né vera né falsa. Potreste dire che si tratta di vuoti giochi di parole, che non è serio. Kurt Gödel, che più tardi costruì il suo lavoro intorno a tali paradossi, era di diverso avviso.

Gödel prese Russell sul serio, non pensò minimamente a uno scherzo. Russell aveva fatto la splendida scoperta che le nostre intuizioni logiche e matematiche sono autocontraddittorie, incoerenti.

Parliamo ora del piano di emergenza di Hilbert per uscire dalla crisi iniziata con la teoria degli insiemi di Cantor e con i paradossi di Russell.

4. La soluzione assiomatico-formale di David Hilbert

Una delle possibili vie d'uscita alla crisi provocata dalla teoria di Cantor era rappresentata dal *formalismo*. Se un ragionamento apparentemente corretto conduce a situazioni paradossali, allora una soluzione era quella di servirsi della logica simbolica e creare un linguaggio artificiale ove le regole del gioco fossero esattamente definite, così da non giungere a contraddi-

² [Ad esempio, l'insieme dei numeri naturali non è un numero naturale, mentre l'insieme degli insiemi non vuoti è ancora un insieme non vuoto].

zioni. Poiché vi sono forme di ragionamento che sembrano corrette, ma non lo sono, ci piacerebbe eliminarle. Il linguaggio naturale è ambiguo (al punto che talvolta non si capisce a chi si riferisca un pronome). Creiamo allora un linguaggio artificiale rendendo tutto talmente preciso da eliminare ogni possibilità di contraddizione. Questa era l'essenza del formalismo.

Non credo che Hilbert pensasse realmente che tutti i matematici dovessero lavorare in un linguaggio siffatto. Si trattava di una specie di linguaggio di programmazione, ma per ragionare e fare matematica; per dedurre, non per calcolare. Ovviamente non si esprime in questi termini, poiché all'epoca non vi erano linguaggi di programmazione.

L'idea sottostante al progetto di Hilbert è l'importanza del metodo assiomatico. Essa ha le sue radici nella matematica greca e in particolare nella geometria di Euclide che è un sistema matematico meraviglioso e nitido. Ma il metodo assiomatico non era tutto. Bisognava, sosteneva Hilbert, usare la logica simbolica. E la logica simbolica ha anch'essa una lunga storia: Leibniz, Boole, Frege, Peano, ... Tutti questi matematici volevano rendere il ragionamento simile all'algebra. La proposta di Leibniz era di abolire ogni possibile disputa (forse pensava a dispute di tipo politico o religioso) semplicemente calcolando di chi fosse la ragione. Anziché accapigliarsi, sarebbe bastato sedersi a un tavolo e dire: "Signori, calcoliamo!" Una bella fantasia.

La logica matematica sarebbe stata come l'aritmetica: si sarebbe potuta ottenere una conclusione senza incertezza e senza questioni di interpretazione. Usando un linguaggio matematico artificiale basato su una logica simbolica si sarebbe finalmente raggiunto un *perfetto rigore*. L'idea era che un argomento o è giusto o è sbagliato, niente vie di mezzo. Una dimostrazione formulata in un sistema assiomatico formale doveva essere assolutamente chiara e rigorosa.

In altre parole, l'idea di Hilbert era quella di una completa precisione circa le regole del gioco – le definizioni, i concetti elementari, la grammatica e il linguaggio – in modo tale che tutti potessero concordare su come la matematica andasse fatta. In pratica sarebbe eccessivamente gravoso usare un tale sistema, ma esso sarebbe di grande interesse filosofico perché stabilirebbe una volta per tutte se un certo ragionamento matematico è corretto oppure no.

Era un'idea del tutto ragionevole e in linea con la tradizione assiomatica e formale della matematica. In questo, Hilbert era tutt'altro che rivoluzionario. La cosa stupefacente, come ho già detto, fu scoprire che questo piano non poteva assolutamente funzionare, e che, di fatto, era irrealizzabile.

L'idea di mettere insieme metodo assiomatico, logica simbolica e formalismo, quindi, non era che un'estrema ed esagerata versione dell'idea, onnipresente in matematica, che le regole del gioco si possano decidere e concordare tutte e una volta per tutte. Hilbert si sbagliava, ma in una maniera

assai fruttuosa, poiché si era posto ottime domande e rispondendo a queste aveva creato un campo completamente nuovo della matematica chiamato *metamatematica*.

La metamatematica è una matematica che guarda a se stessa, in cui si studiano gli obiettivi che la matematica può o non può porsi.

5. Che cos'è la metamatematica

La metamatematica è il mio campo. In essa si guarda la matematica dall'alto e si usa il ragionamento matematico per studiare fin dove il ragionamento stesso può arrivare. L'idea di fondo è la seguente. Una volta che si è costretta la matematica entro un linguaggio artificiale alla Hilbert, e si è stabilito un sistema assiomatico completamente formale, allora ci si può dimenticare completamente del suo significato e procedere come in un gioco che si gioca con segni sulla carta e che permette di dedurre teoremi dagli assiomi di partenza: il gioco del ragionamento matematico, una manipolazione combinatoria di simboli.

Quando si studia dall'esterno un sistema assiomatico quali domande ci si pone?

Ci si può domandare, ad esempio, se si può provare che 0 è uguale a 1 . Si spera di no, ma come essere certi? In generale, la *consistenza* (o *coerenza*) di un sistema comporta l'impossibilità di provare una proposizione (A) e la sua negazione ($\neg A$). Un'altra domanda riguarda la *completezza* del sistema, e cioè se si possa, data una qualsiasi proposizione A , dimostrare A o la sua negazione $\neg A$.

E così Hilbert ebbe l'idea di studiare la matematica dopo averla completamente assiomatizzata e formalizzata. Infatti, finché nel ragionamento matematico permangono dei significati, c'è un elemento soggettivo di interpretazione. Ovviamente, se si fa matematica è perché essa ha un senso, ma se si vuole studiare la matematica in sé, la sua potenza, con metodi matematici, allora si deve "essiccare", "cristallizzare" eliminando il significato e lasciare un linguaggio artificiale con regole perfettamente definite, e un algoritmo simbolico che verifichi le dimostrazioni.

In tal modo chiunque avesse dubbi su una dimostrazione potrebbe utilizzare un procedimento completamente automatico che risponderebbe: "Dimostrazione corretta perché conforme alle regole", oppure, "Dimostrazione sbagliata perché non conforme alle regole". Questo sarebbe un criterio di verità matematica del tutto obiettivo, privo di elementi interpretativi soggettivi, ridotto a puro calcolo. Non ci sarebbe più bisogno di sottomettere gli articoli matematici a giudici umani che impiegano circa due anni per pronunciarsi sulla loro validità. Basterebbe darli alla macchina, e questa

sentenzierebbe: “Dimostrazione OK”, oppure “Errore ortografico in riga 4”, oppure “Impossibile derivare la riga 4 dalla riga 3”. Fine del discorso.

Di certo, Hilbert non mirava a ridurre la matematica a un lavoro meccanico. Semplicemente, intendeva studiarne la potenza deduttiva con assoluto rigore.

Avere un unico sistema formale che includesse tutte le forme di ragionamento matematico: quella sarebbe stata la perfezione! Conoscendo tutte le regole del gioco, avremmo potuto usare la metamatematica per stabilire se un sistema fosse coerente e completo. In tal modo si sarebbe definitivamente risposto alla domanda: “Quando una dimostrazione è corretta? Cosa è una verità matematica?” E tali risposte sarebbero state completamente oggettive.

In altre parole, se una dimostrazione matematica deve essere qualcosa di assolutamente oggettivo, o vera o falsa, allora ci vogliono delle regole per stabilirlo e queste non devono dipendere dalle possibili interpretazioni: basterà esplicitare completamente tutti i singoli passaggi dimostrativi. Il ruolo della logica matematica consisteva proprio nello scomporre il ragionamento matematico in passaggi atomici in cui niente fosse lasciato all’immaginazione, niente restasse escluso e tutti i passi potessero essere controllati.

D’altra parte, anche intuitivamente è del tutto ragionevole pretendere che ci sia una sola verità. Potete immaginare allora come fosse sconcertante apprendere, nel 1931, che ciò non era per niente ragionevole, che era assolutamente irrealizzabile!

6. Kurt Gödel scopre l’incompletezza

All’epoca della sua scoperta Gödel si trovava a Vienna. Egli era di origine ceca, nato a Brno, dopo si trasferì all’Institute for Advanced Study di Princeton. Il suo famoso teorema di incompletezza rivoluziona completamente la visione della matematica. C’è un bel libro di Nagel e Newman, *La prova di Gödel*, che spiega di che cosa si tratta.³ Lo lessi quando ero ragazzo e ancora oggi dopo quarant’anni è in stampa.

Qual è il risultato sensazionale di Gödel? La scoperta che Hilbert sbagliava, che non c’è modo di derivare, entro una teoria assiomatica, tutte le verità matematiche.

Più precisamente, Gödel scoprì che al di dentro dell’aritmetica elementare: 0, 1, 2, 3, 4, ... con somma e moltiplicazione, è impossibile trovare un gruppo di assiomi (quali gli assiomi di Peano) da cui conseguano tutte le proposizioni vere del sistema; neppure questo *semplice* compito è realizza-

³ E. Nagel e J. R. Newman, *Gödel’s Proof*, New York University Press, New York 1958 [trad. it. *La prova di Gödel*, Bollati Boringhieri, Torino 1974, 2ª ed. accresciuta 1992].

bile. Se ammettiamo che gli assiomi non consentano di dedurre teoremi falsi, vi saranno verità aritmetiche non deducibili da quegli assiomi.

Era un risultato assolutamente devastante. Di tutta la filosofia della matematica rimase un mucchio di cenere! Certamente nel 1931 in Europa c'era ben altro di cui preoccuparsi. Una grande depressione e la guerra era alle porte. Non tutto è matematica! E la vita è più importante dell'epistemologia! Comunque, ci si può chiedere: se neppure la tradizione secolare della matematica era corretta, di che cosa fidarsi?

Come fece Gödel ad ottenere il suo risultato? La sua dimostrazione, tutta condotta sul filo del paradosso, è veramente intelligente. Infatti egli partì proprio dal paradosso del mentitore: "Questa proposizione è falsa", che come sappiamo non è né vera né falsa. Solo che Gödel sostituisce, all'attributo "falso", "non deducibile" e considera l'affermazione:

"Questa proposizione non è deducibile".

Com'è facile capire, se si riesce a determinare, nel sistema dell'aritmetica elementare, una proposizione G che di se stessa dice "non sono deducibile", ci si trova nei guai. Perché se G è deducibile dagli assiomi, allora è falsa, e il sistema dà luogo ad affermazioni false. Se invece G non è deducibile, allora è vera, nel qual caso abbiamo una proposizione vera che non può essere derivata dagli assiomi, e il sistema è incompleto.

La dimostrazione originale di Gödel è piuttosto difficile poiché la costruzione di G richiese molti accorgimenti tecnici. Ma leggendo l'articolo del 1931 mi sembra di ritrovarci un mucchio di programmazione LISP, o almeno qualcosa di molto simile. La dimostrazione introduce una grande quantità di funzioni definite ricorsivamente che manipolano liste, proprio quello che si fa in LISP. Quindi anche se allora non vi erano ancora linguaggi di programmazione, con il senno di poi, nel lavoro originale di Gödel si trova un linguaggio di programmazione strettamente connesso all'essenza del LISP puro (senza effetti collaterali). Questo è un altro aspetto estremamente interessante del lavoro di Gödel che spesso non viene considerato.

Ora il prossimo passo fondamentale si ha solo dopo cinque anni, nel 1936, ad opera di Alan Turing.

7. Alan Turing scopre l'indcidibilità

Turing considerò la cosa da un punto di vista completamente diverso e ben più profondo. Portò allo scoperto qualcosa che fa luce completa sulla questione: il calcolatore! Questo era già implicito nel lavoro di Gödel, ma non era visibile agli ordinari mortali, non a quelli di allora. Alan Turing lo fece vedere.

Hilbert aveva detto che ci doveva essere un procedimento *meccanico* per decidere se una dimostrazione era conforme alle regole o no, ma non aveva mai chiarito cosa dovesse intendersi per procedimento meccanico; era solo un modo di dire. Turing disse finalmente come doveva essere una macchina per un tale compito, ovvero una macchina di Turing (ovviamente, lui non la chiamava così). Infatti, nel lavoro si trova, come in quello di Gödel, qualcosa che oggi chiameremmo linguaggio di programmazione. Tuttavia i due linguaggi di programmazione sono completamente diversi. Il linguaggio di Turing non è di alto livello, quale il LISP, è piuttosto simile a un linguaggio macchina, un orribile linguaggio macchina che nessuno oggi userebbe perché troppo semplice.

Turing comprese che, sebbene le sue macchine fossero troppo semplici, e il loro linguaggio macchina troppo primitivo, tuttavia esse erano molto flessibili: erano macchine *general-purpose*. Infatti, egli riteneva che qualsiasi calcolo eseguibile da un uomo potesse essere svolto da una opportuna macchina di Turing. A questo punto il suo pensiero prese una svolta spettacolare. Egli si domandò: cos'è che tali macchine possono fare o non possono fare? Quasi immediatamente egli scoprì un problema che nessuna macchina di Turing può risolvere. Si tratta del cosiddetto *halting problem* (o *problema della fermata*) che è quello di decidere a priori se una data macchina di Turing terminerà un certo calcolo.

La cosa sorprendente di questo lavoro del 1936 è che egli avesse già chiara la nozione di calcolatore universale o *general-purpose*, cioè di una macchina che può fare il lavoro di una qualsiasi altra macchina. E subito fece vedere che c'è un limite a quello che una tale macchina universale può fare. E come fece a scoprirlo? È semplice: domandiamoci, anzitutto, se un programma che gira su un calcolatore a un certo punto conclude il suo calcolo.

Se si pongono limiti di tempo, allora la risposta è semplicissima. Per sapere se un programma si fermerà entro un anno, basta aspettare un anno. A quel punto il programma si sarà fermato oppure no. Quello che Turing dimostra è che siamo nei guai se non si pongono limiti di tempo. Uno potrebbe obiettare: "Ma che programma sarà mai un programma che impiega più di un anno, o più di mille anni? Deve pur esserci un limite temporale!" Sono d'accordo, questa è matematica pura, non è il mondo reale. È solo l'*infinito* a creare guai! Ma Turing dimostra che se non si pone un limite temporale, si va incontro a grosse difficoltà.

Riconsideriamo l'*halting problem*. Se un programma si ferma, alla fine, pur di essere pazienti nell'attendere, si scoprirà che si è fermato. Il vero problema è quando smettere di aspettare. Turing, riprendendo il ragionamento *diagonale* di Cantor,⁴ dimostra in modo molto semplice che tale problema è

⁴ [L'argomento diagonale di Cantor è quello che dimostra la non esistenza di una cor-

insolubile.⁵ Nessun programma può dire se un qualsiasi altro programma si fermerà o meno. E il vero problema non è la fermata, ma la non-fermata, ovvero il problema di sapere quando smettere.

A questo punto Turing deduce un interessante corollario. Se non c'è alcuna possibilità di *calcolare* a priori se il programma si fermerà o meno, risulterà ugualmente impossibile stabilirlo per via *deduttiva*, col ragionamento. Nessun sistema assiomatico sarà in grado di dedurre una proposizione che ci informi sulla fermata o non-fermata di un programma.

Infatti, se si potesse dedurre una tale proposizione entro un sistema assiomatico formale, allora vi sarebbe un modo di calcolarlo. Basterebbe semplicemente elencare tutte le possibili deduzioni eseguibili nel sistema ordinandole in base alla loro lunghezza, esaminarle una dopo l'altra e verificarne la validità, fino a trovare quella della fermata o della non-fermata. (Un compito proibitivo, ma in teoria fattibile).

Una tale procedura non necessita di un matematico, essa può essere eseguita da un computer, in quanto la verifica della correttezza di una deduzione è puramente meccanica. Se vi fosse un sistema formale in grado di dimostrare se un programma si ferma o no, avremmo quindi trovato un modo per rispondervi tramite un calcolo. Ma ciò è impossibile, in quanto incorreremmo in un paradosso simile a quello del mentitore. Avremmo un programma che si ferma se e solo se non si ferma: lo stesso argomento del paradosso di Russell!

Turing, quindi, andò più a fondo di Gödel. Quando da studente lessi la dimostrazione di Gödel, potevo seguirne i singoli passi. Ma non riuscivo a sentire di averla del tutto afferrata nell'essenza. L'argomento mi sembrava troppo sottile, troppo fragile, mi sembrava addirittura superficiale. Vi era qualcosa di nascosto, intimamente collegato alla programmazione, che non si riusciva a toccare con mano.

rispondenza biunivoca tra i numeri naturali e i numeri reali, o più in generale, di una corrispondenza 1-1 tra gli elementi di un insieme e tutti i suoi sottoinsiemi].

⁵ [In genere si dimostra l'impossibilità di un problema più ristretto. Si consideri una numerazione (senza ripetizione) di tutte le macchine di Turing (sono in effetti programmi su un opportuno linguaggio e in quanto tali esprimibili con sequenze finite di simboli) $M_1, M_2, M_3, \dots$. Si consideri quindi un'enumerazione (senza ripetizione) di tutte le possibili parole in ingresso alle macchine di Turing: $\alpha_1, \alpha_2, \alpha_3, \dots$. Diciamo che, rispetto a tali enumerazioni, la parola α_i *corrisponde* alla macchina M_i e viceversa che M_i *corrisponde* alla parola α_i . Dimostriamo che non può esistere una macchina di Turing U che si ferma su un ingresso α se e solo se la macchina corrispondente ad α non si ferma su α . La dimostrazione è un'ulteriore applicazione dello schema dimostrativo diagonale di Cantor e Russell. Per ogni macchina di Turing M definiamo l'insieme $L(M)$ di tutte le parole *terminanti* di M come quelle che, date in ingresso a M , producono calcoli che si concludono in un tempo finito. Consideriamo quindi il seguente insieme (relativo alle enumerazioni sopra indicate): $\{\alpha_i \mid \alpha_i \notin L(M_i), i \in N\}$. Tale insieme non può costituire l'insieme delle parole terminanti di nessuna macchina di Turing. Infatti, se così fosse, una tale macchina dovrebbe avere un indice, diciamolo h , e quindi presa la parola α_h si determina il solito *paradosso diagonale*: $\alpha_h \in L(M_h)$ se e solo se $\alpha_h \notin L(M_h)$].

Turing era giunto al nocciolo della questione, mostrando che il problema non riguardava un particolare sistema, quale quello studiato da Gödel, ma che nessun sistema formale di una certa complessità poteva funzionare. Va detto che il contesto era diverso. Gödel studiava l'aritmetica, con somma e moltiplicazione, mentre Turing considerava una cosa un po' strana dal punto di vista matematico, la fermata dei programmi. Una questione che non si era ancora presentata all'epoca del lavoro di Gödel. Come si vede, Turing lavorava con concetti completamente nuovi.

Ma il risultato di Gödel non è solamente tremendamente intelligente, giacché Gödel aveva avuto il coraggio di immaginare che Hilbert potesse sbagliare. A quel tempo vi era un altro grande matematico, von Neumann, probabilmente non meno acuto di Gödel, al quale tuttavia non venne mai in mente una simile possibilità. Quando ascoltò Gödel spiegare il suo risultato, ne capì subito la portata e cominciò a valutarne le implicazioni. Ma la sua conclusione fu: "Me lo sono lasciato scappare!" Gödel, in questo, fu molto più profondo.

Anche il lavoro di Turing era pieno di dettagli tecnici, come quello di Gödel, perché anche lì c'era un linguaggio di programmazione. C'era pure un lungo programma, che naturalmente aveva dei difetti (*bugs*), perché non si poteva farlo girare e correggerlo, era il programma di una macchina di Turing universale. Ma l'idea di fondo era da togliere il respiro! Penso che Turing sia andato oltre Gödel, ma devo riconoscere che Gödel aveva fatto il primo passo, quello più difficile, che richiede più coraggio.

8. Gregory Chaitin scopre la casualità nella matematica pura

Bene, cosa avvenne in seguito? Cominciò la seconda guerra mondiale. Turing cominciò ad occuparsi di crittografia, von Neumann di calcoli sulla bomba e per un po' ci si dimenticò dell'incompletezza.

A questo punto entro in scena io. La generazione di matematici che si erano interessati a questi problemi ne erano praticamente usciti con la seconda guerra. Negli anni Cinquanta ricordo che ero appena un ragazzo quando, nel 1956, negli Stati Uniti, lessi su "Scientific American" l'articolo di Nagel e Newmann, che poi divenne libro.

Non capivo proprio come i matematici si fossero dimenticati di Gödel. Io ero affascinato dall'incompletezza e volevo comprenderla fino in fondo. Il risultato di Gödel mi avvinceva, ma c'era qualcosa che mi sfuggiva... La visione di Turing, certo, era più profonda, ma anche lì non ero del tutto soddisfatto, volevo capirne di più. Finché un bel giorno mi venne un'idea curiosa sulla casualità. Stavo leggendo un mucchio di cose su un altro argomento assai stimolante, una questione sui fondamenti della fisica. Vi erano discussioni circa la relatività e la cosmologia e ancora di più sulla meccanica

quantistica, su quanto accade nell'atomo. Sembra che quando tutto diventa piccolo, il mondo fisico si comporti in un modo stranissimo, molto diverso da come gli oggetti si comportano nella realtà osservabile: Nell'atomo, difatti, tutto è casuale, imprevedibile. Intrinsecamente imprevedibile. Ad Einstein questo non piaceva: "Dio non gioca a dadi" diceva. Fra l'altro, lui e Gödel erano grandi amici a Princeton.

Stavo leggendo tali cose, quando mi si profilò, quasi inconsciamente, l'idea che potesse esistere la casualità anche in matematica.

L'idea di base della meccanica quantistica è che la casualità è fondamentale, una caratteristica essenziale dell'universo. Nella vita di tutti i giorni sappiamo che gli eventi sono imprevedibili, ma nella fisica newtoniana e anche in quella relativistica, che si definiscono classiche in opposizione alla fisica quantistica, si può teoricamente prevedere il futuro. Le equazioni, infatti, sono *deterministiche*. Conoscendo esattamente, con infinita precisione, le condizioni iniziali di un sistema, esse consentono di predire con infinita precisione lo stato del sistema in ogni istante futuro e anche passato, poiché lavorano ugualmente in entrambe le direzioni.

Questa meravigliosa possibilità è talvolta definita come *determinismo laplaciano*. Penso che sia dovuto all'*Essai philosophique sur les probabilités* di Laplace, un libro pubblicato circa due secoli fa ove si spiega, all'inizio, che applicando a un dato sistema fisico le equazioni di Newton un demone che conoscesse con infinita esattezza le condizioni iniziali potrebbe teoricamente predire il futuro arbitrariamente lontano, o anche il passato arbitrariamente lontano. Qui non si parla di libero arbitrio e di responsabilità morale, ma per chi faccia calcoli fisici è un mondo eccezionale, perché si può calcolare ogni cosa.

Ma negli anni Venti, con la meccanica quantistica, si cominciò a vedere in che modo Dio gioca a dadi nell'atomo: difatti l'equazione fondamentale della meccanica quantistica è l'equazione di Schrödinger, ed essa parla appunto della *probabilità* che un elettrone faccia qualcosa. La quantità di base è una probabilità ed è un'equazione d'onda, un'onda di probabilità. È un tipo completamente differente di equazione; nella fisica newtoniana si può calcolare la traiettoria precisa di una particella e sapere esattamente come si comporterà, mentre nella meccanica quantistica l'equazione fondamentale fornisce solo dei comportamenti probabili.

Non si può sapere esattamente dove si trova un elettrone e al tempo stesso qual è il suo vettore della velocità (in che direzione si muove e con quanta rapidità). L'elettrone non è in uno stato specifico, conoscibile con precisione infinita, come nella fisica classica. Se si conosce con grande precisione la sua posizione, la sua velocità risulterà irrimediabilmente incerta. Viceversa, se si conosce esattamente la sua velocità, ecco che la sua posizione diventa enormemente incerta. Questo è il famoso *principio di indeterminazione*

di Heisenberg: vi è una sorta di complementarità nella conoscibilità delle caratteristiche di un fenomeno fisico.

È un fatto storicamente interessante che in passato i fisici aborrissero una cosa del genere – vedi appunto Einstein – mentre oggi pensano a come utilizzarla. C'è ad esempio un nuovo campo, chiamato *quantum computing*, dove si progettano nuove tecniche di calcolo basate sul cosiddetto *parallelismo quantico*. Se è vero che un calcolatore quantistico è indeterminato, forse si può convertire l'incertezza nella possibilità di portare avanti moltissimi calcoli in parallelo! Quindi invece che combattere una tale incertezza, si pensa di utilizzarla, il che sarebbe una grande idea.

Io ero ancora un ragazzo quando si dibattevano tali questioni. Albert Einstein che pure era stato un pioniere nella costruzione della meccanica quantistica, si ostinava nel rifiutarla e di lui si diceva: "Poveretto, ha fatto il suo tempo".

Cominciai a pensare che forse vi è della casualità anche nella matematica pura e che forse questa poteva essere *la ragione reale dell'incompletezza*. Un esempio è l'aritmetica elementare, dove vi sono questioni aperte veramente difficili. Consideriamo i numeri primi. Individualmente si comportano in un modo veramente imprevedibile. È vero che obbediscono a certe regolarità statistiche. Vi è un *teorema fondamentale dei numeri primi* che prevede con grande esattezza la distribuzione media dei primi, ma la distribuzione individuale sembra del tutto casuale!

Pensando e ripensando alla casualità intuii che poteva essere questa la ragione dell'incompletezza in matematica. Negli anni Sessanta io e altri, indipendentemente, elaborammo nuove idee in proposito. Mi piace chiamare questo complesso di nuove idee *teoria algoritmica dell'informazione*.

La denominazione è un po' altisonante, ma l'idea di fondo è semplicemente quella di considerare la dimensione dei programmi. Come si vede, si tratta di una misura di complessità, di una *complessità computazionale*.

La prima volta che sentii parlare di complessità di calcolo fu proprio da von Neumann. Turing arrivò al concetto di un calcolatore come oggetto matematico, un calcolatore perfetto che non commette errori e ha tutto il tempo e lo spazio che occorrono per il suo funzionamento: è sempre finito, ma può proseguire nel calcolo fin quando è necessario. Il passo successivo, quello più logico per un matematico, è di studiare il tempo, il lavoro che occorre per eseguire un calcolo, la sua complessità. E infatti, credo intorno al 1950, von Neumann suggerì in qualche occasione che si sarebbe dovuto sviluppare un nuovo settore di ricerca che considerasse la complessità temporale dei calcoli, settore che ora è ben sviluppato. Quindi, mi sembrò naturale, visto che se ne occupavano in tanti, fare qualcos'altro!

La mia idea fu quella di prescindere dal tempo, e di considerare la dimensione dei programmi, la quantità di informazione che bisogna fornire a un

calcolatore perché compia un dato lavoro. Da un punto di vista pratico è più interessante il tempo di esecuzione, poiché naturalmente per i computer è molto importante lavorare il più velocemente possibile. Ma da un punto di vista concettuale, la cosa è diversa. Da un punto di vista filosofico, è più importante, a mio avviso, la dimensione del programma, in quanto la complessità dimensionale dei problemi si connette a fatti fondamentali della fisica.

Come si sa, in fisica vi è una nozione cruciale detta *entropia*, che determina il grado di disordine di un sistema. L'entropia ebbe un ruolo cruciale nel lavoro del famoso fisico tedesco Ludwig Boltzmann, e compare in meccanica statistica e in termodinamica. Essa misura quanto disordinato e caotico è un sistema fisico. Un cristallo ha un'entropia bassa, mentre un gas ad alta temperatura ha entropia alta. La quantità di caos o disordine è appunto una sorta di nozione di casualità che piace ai fisici.

L'entropia è a sua volta connessa con l'importante questione filosofica della *freccia del tempo*, un'altra famosa controversia. Quando Boltzman inventò quella bellissima cosa chiamata meccanica statistica, una teoria che ora è considerata uno dei capolavori della fisica del Novecento (tutta la fisica è ora fisica statistica) i fisici dissero che era *ovviamente* sbagliata. Infatti nella teoria di Boltzmann l'entropia tende ad aumentare nel tempo e quindi impone una direzionalità temporale. Le equazioni della fisica newtoniana, invece, sono reversibili rispetto al tempo. Non c'è differenza nel predire il futuro o il passato. Se si conosce esattamente come stanno le cose in un certo istante, si può andare indifferente in una delle due direzioni, per le equazioni non cambia nulla, sia in avanti che all'indietro.

Ma nella vita di ogni giorno e nella meccanica statistica di Boltzmann, vi è una bella differenza tra l'andare in avanti o all'indietro. I vetri si rompono, ma non tornano spontaneamente all'indietro per ricompattarsi. Secondo la teoria di Boltzmann i sistemi tendono a un aumento di entropia in quanto il disordine tende ad aumentare nel tempo. "Non lo puoi dedurre dalle equazioni della fisica newtoniana!" gli dicevano i colleghi, ma Boltzmann pretendeva di dedurlo. Egli considerava un gas. Gli atomi di un gas rimbalzano come le palle in un biliardo e ogni interazione è reversibile. Se facessimo girare un film all'indietro, non ci accorgeremmo di alcuna differenza di comportamento. Se si guarda per un breve tempo una piccola porzione di gas non potremmo accorgerci se stiamo vedendo il film nella direzione giusta o in quella sbagliata.

Ma la teoria dei gas di Boltzmann diceva che c'è una freccia del tempo, un sistema parte con un certo grado di ordine e finisce in uno stato in cui le cose si rimescolano disordinandosi. Vi è un'espressione tedesca terribile che indica ciò come "morte termica" (*Wärmetod*). Secondo la concezione di Boltzmann, l'universo va verso uno stato orribilmente triste di massima en-

tropia. Una previsione angosciante! È possibile che le critiche rivolte alla sua teoria abbiano portato Boltzmann alla decisione di togliersi la vita.

C'è un legame tra le mie idee e quelle di Boltzmann, perché la dimensione di un programma è un concetto molto vicino a quello di disordine di un sistema fisico. Un gas richiede un programma enorme per dire dove sono tutte le sue molecole, mentre per un cristallo, che ha una struttura molto regolare, ne basta uno più semplice. Entropia e complessità dimensionale di un programma sono cose molto simili.

Questa idea di complessità come dimensione di un programma è anche connessa con la filosofia sottostante al metodo scientifico. Avrete sentito parlare del rasoio di Occam, dell'idea che la teoria migliore è la più semplice. Ora, che cos'è una teoria se non un programma per predire osservazioni? L'idea che la teoria più semplice è la migliore si traduce quindi nel dire che più breve è il programma più concisa è la teoria. Cosa succede se non abbiamo una teoria concisa, se il programma più breve che riproduce un certo insieme di dati sperimentali ha la stessa dimensione dell'elenco dei dati? In questo caso la teoria non è buona, è degenerata, i dati sono incompressibili, ovvero casuali. La teoria non serve a nulla. Una teoria è buona nella misura in cui riesce a comprimere i dati entro un insieme più piccolo di assunzioni iniziali. Maggiore è la compressione, tanto meglio è!

L'idea di complessità come dimensione di programma ha forti suggestioni filosofiche e permette di definire la casualità o l'entropia massima come qualcosa di assolutamente incompressibile. Un oggetto casuale può essere descritto semplicemente dicendo: "Eccolo qui!" Esso non ha nessuna regolarità, nessuna struttura, nessuna descrizione lo identifica in modo più conciso del mostrarlo:

Casualità = Incompressibilità.

All'estremo opposto vi sono oggetti molto grandi, ma con una struttura molto regolare – per esempio potremmo dire “un milione di 0” o “mezzo milione di ripetizioni di 01”, coppie 01, 01, 01 ... ripetute mezzo milione di volte – che possono essere descritti in modo molto conciso. Altri oggetti grandi descrivibili in modo conciso sono le *efemeridi*, le tavole che danno la posizione giornaliera dei pianeti nel cielo nell'arco dell'anno. Tutte queste informazioni astronomiche possono essere compresse in un programmino in FORTRAN che usa le formule newtoniane per calcolare la posizione dei pianeti nel cielo, ogni notte.

Se invece guardiamo il comportamento della ruota della roulette, allora non riusciamo a trovare alcuna regola che possa comprimere la successione dei suoi risultati. Se vi fosse una tale regola i casinò non farebbero buoni affari. Il fatto che guadagnino un sacco di soldi dimostra che è impossibile

prevedere il comportamento della roulette: non c'è regolarità di struttura e quindi il loro lavoro è assicurato!

Di qui l'idea di utilizzare la complessità dei programmi come misura della casualità. Ma la cosa interessante, quando si comincia a pensare in termini di complessità informativa, piuttosto che di complessità temporale, è che l'incompletezza si ritrova ovunque. Si ritrovano cose che sfuggono al ragionamento matematico, come pure del più potente dei programmi.

In sole tre tappe siamo passati da Gödel, in cui troviamo, sorprendentemente, i limiti della matematica, a Turing, in cui tali limiti si spiegano in modo naturale come limiti di calcolo, ed infine, guardando le dimensioni dei programmi, l'incompletezza e i limiti della matematica vi stanno davanti e vi colpiscono in faccia! Perché? Proprio la *prmissima questione* che pone la mia teoria solleva subito problemi. La misura della complessità di qualcosa viene definita come la dimensione del più piccolo programma in grado di generarla. Ma come essere sicuri di avere trovato il più piccolo programma?

Supponiamo di avere un particolare calcolo, un certo insieme di dati e un bel programma sintetico che li produca in uscita. Finora non siamo riusciti a trovare un programma migliore. Abbiamo provato a renderlo più breve, più conciso, ma sembra proprio che sia impossibile. Ma come esserne sicuri? La risposta è: non si può mai essere sicuri. Non c'è mai la certezza che un programma sia quello che io dico *elegante*, ovvero una tale cosa, sorprendentemente va al di là delle possibilità del ragionamento matematico.

Ma per qualsiasi processo di calcolo, una volta fissati il linguaggio di programmazione e un possibile risultato in uscita, allora deve pur esservi almeno un programma di dimensione minima che dia quel risultato. Potrà esserci qualche ridondanza, diverse ridondanze, ma ce ne sarà pur uno più piccolo degli altri. Eppure non si può mai essere sicuri di averlo trovato!

Il risultato preciso al riguardo, che costituisce la mia formulazione preferita di incompletezza è che, se si hanno assiomi di N bit, è impossibile provare che un programma è elegante (di lunghezza minima) se è più lungo di N bit. La cosa funziona essenzialmente in questi termini. Ogni insieme di assiomi, ogni sistema assiomatico formale alla Hilbert, può solo provare l'eleganza di un numero *finito* di programmi.

Per essere più precisi, è impossibile provare l'eleganza di un programma se questo è più lungo della versione computerizzata degli assiomi. Questa può essere identificata con il programma che verifica la correttezza dimostrativa, relativamente agli assiomi dati, di tutte le possibili dimostrazioni. Fissato un particolare linguaggio di programmazione, consideriamo un programma che implementa un sistema assiomatico formale, ovvero che realizza il relativo algoritmo di *proof-checking* per verificare la correttezza dei teoremi. Se un tale programma ha una certa dimensione e un programma

scritto nello stesso linguaggio ha una dimensione maggiore, l'eleganza di quest'ultimo programma non potrà mai essere dimostrata (secondo gli assiomi del sistema formale considerato).

Quindi vi è un'infinità di programmi eleganti la cui eleganza è indimostrabile. Per ogni processo di calcolo vi sarà almeno un programma elegante che lo realizza e forse parecchi, ma tale eleganza non può essere provata se non in un numero finito di casi.

Come faccio a dirlo? La ragione per usare gli assiomi è che questi sono semplici e del tutto affidabili. Quindi gli assiomi che la matematica usa abitualmente sono notevolmente concisi, altrimenti chi crederebbe in loro! Questo significa che in pratica ci sono innumerevoli verità matematiche al di fuori di essi, un'infinita quantità di informazione, della quale ogni insieme finito di assiomi cattura solo una piccola parte! È questo il motivo dei nostri problemi, questa la mia conclusione finale, questo il vero dilemma.

Sintetizzando, posso spiegare in due modi perché l'incompletezza di Gödel è tutt'altro che misteriosa e sorprendente, ma naturale e inevitabile. Il primo è che l'idea di casualità in fisica, la possibilità dell'incomprimibilità, possa occorrere anche in matematica. La seconda è che le verità matematiche presuppongono una quantità infinita di informazione, ma ogni particolare sistema assiomatico ne racchiude una quantità finita perché i principi su cui possiamo concordare, le regole del gioco, sono necessariamente un insieme finito. E non appena una proposizione racchiude più informazione di quella racchiusa negli assiomi, allora è del tutto naturale che essa sfugga a tali assiomi.

Come si constata, il modo con cui la matematica progredisce è la banalizzazione di tutto! Si considera un risultato che originariamente richiedeva uno sforzo immenso e lo si riduce a un corollario banale di una teoria più generale. Prendiamo l'esempio dell'ultimo teorema di Fermat, l'asserzione che

$$x^n + y^n = z^n$$

non ha soluzioni tra gli interi positivi con n maggiore di 2. La recente dimostrazione di Andrew Wiles impiega un centinaio di pagine, ma probabilmente fra altri cento anni si troverà una dimostrazione di una pagina. Ma quella dimostrazione di una pagina richiederà un intero libro per inventare gli strumenti che rendano naturali i concetti relativi al teorema di Fermat. E quando si lavorerà con tali concetti risulterà immediatamente evidente che la prova di Wiles, incastonata nel contesto teorico appropriato, ne costituisce uno sviluppo naturale.

La stessa cosa sta accadendo ora con l'incompletezza. Il risultato di Gödel, come ogni risultato veramente fondamentale, sembrò a tutta prima esoterico e complicato, con una dimostrazione lunga e impenetrabile. Della

prova di Gödel, come per la teoria della relatività di Einstein, si disse che c'erano meno di cinque persone al mondo in grado di capirla.

Quando venne pubblicato, il lavoro di Gödel appariva estremamente difficile. I dettagli oggi li definiremmo di programmazione, un tipo di complessità che oggi sappiamo come trattare, ma allora sembravano del tutto misteriosi. Era un articolo matematico degli anni Trenta, e tutta la fatica da fare era essenzialmente programmazione LISP, trent'anni prima dell'invenzione del LISP, e non c'erano neanche i calcolatori.

Se andiamo a Turing, vediamo che egli rende il risultato di Gödel molto più naturale, e io penso che la mia idea di complessità algoritmica e di informazione, come quantità di complessità algoritmica, renda il risultato di Gödel ancora più naturale, lo rende quasi ovvio, inevitabile. Ma le cose vanno proprio così, questo è il modo con cui la matematica progredisce.

9. Dove siamo diretti?

Se le cose stessero realmente in tali termini, se tutto fosse così semplice, saremmo davvero giunti alla fine della metamatematica. Sarebbe proprio triste, perché significherebbe che tale campo di ricerca sarebbe morto. Ma io non credo proprio che sia così!

Nel corso degli anni ho avuto più volte modo di illustrare i temi di questa conferenza. In queste presentazioni mi piaceva dare esempi di cose che paiono sfidare le possibilità del normale ragionamento matematico. I miei cavalli di battaglia erano l'ultimo teorema di Fermat, l'ipotesi di Riemann⁶ e il problema dei quattro colori. Quando ero ragazzo erano queste le tre grandi questioni ancora aperte in matematica.

Ma è avvenuto qualcosa di buffo. Dapprima il problema dei quattro colori è stato risolto al calcolatore, e recentemente la dimostrazione è stata notevolmente migliorata. L'ultima versione ha molte più idee e molta meno programmazione: un grande passo in avanti. Quindi Wiles è venuto a capo dell'ultimo teorema di Fermat. All'inizio la dimostrazione conteneva un errore, ma nessuno dubita che la versione più recente sia corretta.

Fortunatamente rimane ancora aperta l'ipotesi di Riemann, per quanto ne so!

Ero solito citare l'ultimo teorema di Fermat come possibile esempio di incompletezza di una teoria matematica, come esempio di qualcosa che potrebbe essere troppo difficile da affrontare con gli abituali metodi matematici.

Ora che quella fortezza è stata espugnata ho un serio problema. La teoria algoritmica dell'informazione è molto bella e mostra che vi sono molte cose

⁶ [Una congettura riguardante gli zeri complessi della cosiddetta funzione zeta di Riemann, di fondamentale importanza nella teoria dei numeri].

indimostrabili, ma cosa dice al riguardo di singole questioni matematiche aperte? Dice qualcosa nei riguardi di un reale problema matematico? La risposta è no, i miei metodi non sono così generali come sembrano. Vi sono dei limiti tecnici che impediscono di applicare la teoria algoritmica dell'informazione allo studio dell'ultimo teorema di Fermat. (Fortunatamente! Poiché se avessi annunciato che alla luce di quella teoria il problema era insolubile, oggi sarei in serio imbarazzo).

Allora la domanda diventa: "Com'è che, nonostante tali risultati limitativi, i matematici riescono a progredire tanto?" Io non sono un pessimista, ma i miei risultati danno questa sensazione, sono estremamente pessimisti.

Penso che sia ora di guardare ai risultati positivi. Vi sono già troppi risultati negativi! A prenderli alla lettera potrebbe sembrare che non vi è più modo di fare matematica, che la matematica sia impossibile. Fortunatamente non sembra affatto che la situazione sia questa. Le questioni fondamentali, come le grandi questioni filosofiche, sono grandi perché non si esauriscono mai. Ogni generazione fa qualche passo in avanti. Penso che vi sia ancora una grande quantità di lavoro in questo campo.

Vi è un'altra questione molto interessante: la dimensione dei programmi è una misura di complessità, e noi sappiamo che in metamatematica il concetto funziona, ma cos'ha a che fare con la complessità del mondo reale? Per esempio, cosa dire della complessità di un organismo biologico? Cosa dire della teoria dell'evoluzione?

Von Neumann parlava di una teoria generale sull'evoluzione della vita e il primo passo, diceva, sarebbe stato la definizione della complessità. Quella da noi utilizzata non sembra in effetti la più adatta per gli scopi di una biologia teorica. Ma una tale biologia, a tutt'oggi, non esiste neppure!

Come matematico, mi piacerebbe che qualcuno dimostrasse matematicamente che in certe circostanze, molto generali, la vita deve evolversi. Ma non saprei come definire la vita in un simile contesto. Certo sappiamo riconoscere la vita quando la vediamo, ma come matematico io non saprei dire qual è la differenza tra un bel daino che attraversa la strada e il bidone della spazzatura che il mio vicino di casa ha lasciato fuori dalla porta. Infatti, la spazzatura è sicuramente collegata alla vita, sono detriti, prodotti da processi vitali.

Paragoniamo invece un daino con una roccia. La roccia è più dura. Ma questa non sembra essere la differenza essenziale, quanto invece il fatto che il daino è vivo mentre la roccia è un oggetto inerte. È facile vedere la differenza in pratica, ma qual è la differenza intrinseca? Come può essere afferata matematicamente?

Quello che von Neumann cercava era proprio una teoria generale. Von Neumann inventava continuamente nuove teorie matematiche. Ne inventava una prima di colazione tutti i giorni: la teoria dei giochi, la teoria degli

automi autoriproduttivi, la formulazione della meccanica quantistica negli spazi di Hilbert (era stato allievo di Hilbert e scrisse un libro sull'argomento).

Fin da quando ero un ragazzo, von Neumann era un mio eroe – parlava di Gödel, di Turing – e così, mentre mi chiedevo quali possibilità di successo avesse una simile impresa, pensai che valesse la pena di tentare. Von Neumann suggerì, fra le altre cose, una teoria della complessità computazionale. Egli non fece alcun passo in tal senso, ma penso si possa trovare, da qualche parte, che lo considerava un campo di grande interesse, e certamente aveva ragione.

Von Neumann era dell'idea che una teoria generale dell'evoluzione non dovesse tener conto di dati biochimici o geologici. Bisognava, disse, porsi a un livello più generale, perché se Darwin aveva ragione, l'evoluzione è una cosa molto generale. Concordo.

Per esempio, vi è ora l'idea di una *programmazione genetica* che corrisponde a una versione computerizzata dell'evoluzione. Invece di scrivere un programma che faccia qualcosa, si decide di farlo evolvere per tentativi ed errori. Sembra che funzioni incredibilmente bene, ma come si può spiegare ciò? Considerate *Tierra* di Tom Ray. Alcuni di questi modelli biologici sembrano funzionare fin troppo bene, il problema è che non vi è nessuna comprensione teorica del perché ciò avviene. Io sto cercando una teoria generale che dica innanzitutto cos'è un organismo e come si misura la sua complessità e che sulla base di queste definizioni dimostri la necessità dell'evoluzione di organismi sempre più complessi.

Se si potesse fare, ciò getterebbe nuova luce sul carattere generale dell'evoluzione e sulla probabilità o meno di forme di vita extraterrestre. Naturalmente, anche se i matematici non giungeranno mai a una tale teoria, forse la troveremo visitando nuovi posti e guardando se lì c'è vita. Comunque, von Neumann pose questa come questione interessante, e ci fu un momento, nella mia giovinezza, in cui pensai che la complessità dimensionale dei programmi potesse avere a che fare con l'evoluzione. Ora non lo penso più, perché non sono giunto a nulla seguendo questa pista.

In conclusione, penso che vi sia un grande lavoro da fare, e che stiamo vivendo in un'epoca entusiasmante (anche troppo, alle volte). Io spero che se questa conferenza fosse fatta nel 2099, ci sarebbe un altro secolo di dispute matematiche avvincenti da raccontare, sicuramente con argomenti e preoccupazioni diverse. Sarebbe interessante sentire una tale conferenza tra cent'anni!

Lecture consigliate

1. G. J. Chaitin, *The Unknowable*, Springer-Verlag 1999.
2. G. J. Chaitin, *The Limits of Mathematics*, Springer-Verlag 1998.

Elenco dei teoremi fondamentali¹

1. **Paradosso di Russell (Russell, 1902)**
Proposizione 1.1.
2. **Lemma di König (König, 1927)**
Proposizione 1.2.
3. **Induzione noetheriana (Noether, von Neumann, 1926)**
Proposizione 1.3.
4. **Buon ordinamento (Zermelo, 1904-1908)***
Proposizione 1.5.
5. **Diagonalizzazione di Cantor (Cantor, 1873)***
Proposizione 1.6.
6. **Ordinamento dei cardinali (Cantor, Schröder, Bernstein, 1897)***
Proposizione 1.10.
7. **Forme disgiuntive e congiuntive (Post, 1921)***
Proposizione 2.7.
8. **Compattezza proposizionale (Malcev, 1941)**
Proposizione 2.9.
9. **Completezza predicativa (Gödel, 1930)***
Proposizione 2.12.
10. **Espansione di Herbrand (Herbrand, Skolem, 1930)***
Proposizione 2.18.

¹ Gli asterischi rimandano a un intero gruppo di proposizioni di cui il teorema indicato costituisce l'epicentro. Tra parentesi vi è l'indicazione dell'autore, o degli autori (generalmente riconosciuti tali), della prima dimostrazione o di una dimostrazione direttamente collegata; l'anno è quello di pubblicazione della prima versione del teorema.

11. Teorema di Löwenheim-Skolem (Löwenheim, Skolem, 1915)*
Proposizione 2.22.
12. Teorema di deduzione (Herbrand, Tarski, 1930)
Proposizione 3.1.
13. Diagonalizzazione di Turing (Turing, 1936)*
Proposizione 4.7.
14. Non-decidibilità della logica predicativa (Church, 1936)
Proposizione 5.1.
15. Completamento di Lindenbaum (Lindenbaum, 1930)
Proposizione 5.2.
16. Primo teorema di incompletezza di Gödel (Gödel, 1931)*
Proposizione 5.3.

Alfabeto greco

1.	α	A	alfa	13.	ν	N	ni
2.	β	B	beta	14.	ξ	Ξ	xi
3.	γ	Γ	gamma	15.	o	O	omicron
4.	δ	Δ	delta	16.	π	Π	pi
5.	ε	E	epsilon	17.	ρ	P	ro
6.	ζ	Z	zeta	18.	σ	Σ	sigma
7.	η	E	eta	19.	τ	T	tau
8.	θ	Θ	theta	20.	υ	Y	ipsilon
9.	ι	I	iota	21.	φ	Φ	fi
10.	κ	K	kappa	22.	χ	X	chi
11.	λ	Λ	lambda	23.	ψ	Ψ	psi
12.	μ	M	mi	24.	ω	Ω	omega

Elenco dei simboli

$=$	$*$	$\leftrightarrow$	Mod_{Σ}
$\Rightarrow$	$\parallel$	$\forall$	$\text{Mod}_{\Sigma,D}$
$\Leftrightarrow$	$\rightarrow$	$\exists$	$\text{Mod}_{\Sigma,D}(\varphi)$
$\equiv$	$\hookrightarrow$	$\exists!$	$\text{Mod}_{\Sigma,D}(\Phi)$
$\in$	$\rightarrow$	$\perp$	$\text{Mod}_{\Sigma}(\varphi)$
$\subseteq$	ω	$\models$	$\text{Mod}_{\Sigma}(\Phi)$
$\{\}$	Ω	$\vdash$	$\text{Th}(\mathcal{M})$
$\emptyset$	$\mathbb{N}_0$	Σ	$\text{Diag}(\mathcal{M})$
$\times$	$\mathbb{N}$	T_{Σ}	AR
$\cup$	$\cong$	F_{Σ}	SEQ
$\cap$	$\perp$	$T_{\Sigma}(V)$	PA
$/$	$\mapsto$	$F_{\Sigma}(V)$	SS
$\mathcal{P}$	$\wedge$	$T_{\Sigma,D}$	TT
$\circ$	$\vee$	$F_{\Sigma,D}$	ZF
			MN

Bibliografia

- Abramsky S., Gabbay D.M. e Maibaum T.S.E. (a cura di), *Handbook of Logic in Computer Science*, 5 voll., Clarendon Press, Oxford 1993-2000.
- Asperti A. e Ciabattoni A., *Logica a Informatica*, McGraw-Hill Italia, Milano 1997.
- Barwise J. (a cura di), *Handbook of Mathematical Logic*, North-Holland, Amsterdam 1977.
- Bell J.L. e Machover M., *A Course in Mathematical Logic*, North-Holland, Amsterdam 1977.
- Benthem van J. e Ter Meulen A. (a cura di), *Handbook of Logic and Language*, Elsevier, Amsterdam 1996.
- Buss S.R. (a cura di), *Handbook of Proof Theory*, Elsevier, Amsterdam 1998.
- Cameron P.J., *Sets, Logic and Categories*, Springer, London 1999.
- Chaitin G.J., *The Limits of Mathematics*, Springer-Verlag, London 1998.
- *The Unknowable*, Springer-Verlag, London 1999.
- Chang C.C., Keisler H.J., *Model Theory*, North-Holland, Amsterdam-London 1973 [trad. it. *Teoria dei modelli*, Boringhieri, Torino 1980].
- Church A., *Introduction to Mathematical Logic I*, Princeton University Press, Princeton 1956¹⁰.
- Cohen P.J., *Set Theory and the Continuum Hypothesis*, Benjamin, New York 1966 [trad. it. di G. Lolli, *La teoria degli insiemi e l'ipotesi del continuo*, Feltrinelli, Milano 1973].
- Cori R., Lascar D., *Mathematical Logic*, Oxford University Press, Oxford 2000.
- Crossley J.N., Ash C.J., Brickhill Ch. J., Stillwell J.C. e Williams N.H., *What is Mathematical Logic*, Oxford University Press, London 1972 [trad. it. *Che cos'è la logica matematica?*, Boringhieri, Torino 1976].
- Dalen van D., *Logic and Structure*, Springer-Verlag, Berlin 1981.
- Davis M., *The Undecidable*, Raven Press, New York 1965.
- Devlin K., *The Joy of Sets. The Fundamentals of Contemporary Set Theory*, Springer-Verlag, Berlin 1993.
- Enderton H.B., *A Mathematical Introduction to Logic*, Academic Press, New York 1972.
- Ebbinghaus H.D., Flum J. e Thomas W., *Mathematical Logic*, Springer-Verlag, New York 1984.

- Feferman S., *In the Light of Logic*, Oxford University Press, New York 1998.
- Fitting M., *First-Order Logic and Automated Theorem Proving*, Springer-Verlag, Berlin 1996.
- Fraenkel A. A., *Set Theory and Logic*, Addison-Wesley, Reading, Mass., 1966 [trad. it. *Teoria degli insiemi e logica*, Astrolabio, Roma 1970].
- Gödel K., *Collected Works* (1929-1974), 3 voll., a cura di S. Feferman, Oxford University Press, New York - Clarendon Press, Oxford 1986-1995 [trad. it. vol. 1, *Opere* (1929-1936), a cura di E. Ballo, S. Bozzi, G. Lolli e C. Mangione, Bollati Boringhieri 1999].
- Goldblatt R., *Lectures on the Hyperreals*, Springer, New York 1991.
- Gries D. e Schneider F., *A Logical Approach to Discrete Math*, Springer-Verlag, New York 1993.
- Heijenoort van J., *From Frege to Gödel: A Source Book in Mathematical Logic, 1879-1931*, Harvard University Press, Cambridge, Mass., 1967.
- Hilbert D. e Ackermann W., *Grundzüge der theoretischen Logik*, Springer-Verlag, Berlin 1928, 2^a ed. riveduta 1938 [trad. ingl. *Principles of Mathematical Logic*, Chelsea Publishing Co./American Mathematical Society, Providence, RI, 2000].
- Hintikka J. (ed.), *From Dedekind to Gödel*, Kluwer Academic, Dordrecht 1995.
- Hodges W., *Elementary Predicate Logic*, in D. Gabbay e F. Guenther (a cura di), *Handbook of Philosophical Logic*, vol. 1: *Elements of Classical Logic*, Reidel, Dordrecht 1983, pp. 1-131.
- *A Shorter Model Theory*, Cambridge University Press, Cambridge 1997.
- Hrbacek K., Jech T., *Introduction to Set Theory*, Third Edition, Revised and Expanded, Marcel Dekker, Inc., New York 1999.
- Kalish D. e Montague R., *Logic: Techniques of Formal Reasoning*, Harcourt Brace & Co., London-New York 1964.
- Keisler H. J., *Elementary Calculus: An Infinitesimal Approach*, Prindle, Weber & Schmidt, Boston 1976 [trad. it. *Elementi di analisi matematica*, a cura di Ferro R., Sambin G., Colussi L., Facchini A., Le Danne A., Piccin, Padova 1982].
- Kleene S. C., *Intoduction to Metamathematics*, Van Nostrand, New York 1952.
- Lolli G., *Introduzione alla logica formale*, Il Mulino, Bologna 1991.
- Lyndon R. C., *Notes on Logic*, Van Nostrand, New York 1966.
- Manca V., *Formal Logic*, in J. Webster (a cura di), *Encyclopedia of Electrical and Electronics Engineering*, John Wiley & Sons, New York 1999, vol. 7, pp. 675-87.
- *Logical string rewriting*, in “Theoretical Computer Science” (in corso di stampa).
- Mendelson E., *Introduction to Mathematical Logic*, Van Nostrand, Princeton, N.J., 1972 [trad. it. *Introduzione alla logica matematica*, Boringhieri, Torino 1972].
- More G. H., *Logic and Set Theory*, in I. Grattan-Guinness (a cura di), *Companion Encyclopedia of the History and Philosophy of Mathematical Sciences*, vol. 1, Routledge, London 1994, pp. 635-43.
- Mostowski A., *Thirty Years of Foundational Studies*, Acta Philosophica Feunica 17, Helsinki 1965.
- Nerode A. e Shore R. A., *Logic for Applications*, Springer, New York, 1997².
- Odifreddi P., *Logic and Computer Science*, Academic Press, London 1990.
- Prawitz D., *Natural Deduction: a Proof-Theoretical Study*, Almqvist & Wiksell, Stockolm 1965.

- Rosen K. H. (a cura di), *Discrete and Combinatorial Mathematics*, CRC Press, London 1999.
- Rozenberg G. e Salomaa A. (a cura di), *Handbook of Formal Languages*, 3 voll. Springer-Verlag, Berlin-Heidelberg 1997.
- Russell B., *The Principles of Mathematics*, Allen & Unwin, London 1903 [trad. it. *I principi della matematica*, Longanesi, Milano 1988].
- Shoenfield J. R., *Mathematical Logic*, Addison-Wesley, Reading, Mass., 1967 [trad. it. *Logica matematica*, Boringhieri, Torino 1980].
- Smoryński C., *Logical Number Theory*, Springer-Verlag, Berlin 1991.
- Smullyan R. M., *Theory of Formal Systems*, Princeton University Press, Princeton, N.J., 1961.
- *First-Order Logic*, Springer-Verlag, Berlin 1968.
 - *Logical Number Theory*, Springer-Verlag, Berlin 1991.
- Tarski A., *Introduction to Logic*, Oxford University Press, Oxford 1965 [trad. it. *Introduzione alla logica*, Bombiani, Milano 1978²].
- Tarski A. e Givant S., *A Formalization of Set Theory without Variables*, in “Colloquium Publications of the American Mathematical Society”, vol. 41, 1987.
- Toffalori C. e Cintoli P., *Logica Matematica*, McGraw-Hill, Milano 2000.
- Troelstra A. S. e Schwichtenberg H., *Basic Proof Theory*, in *Cambridge Tracts in Theoretical Computer Science*, Cambridge University Press, Cambridge, vol. 43, 2000².

Indice analitico

- Calcolo, 72, 98, 143
 - completezza, 73, 90, 115, 123
 - correttezza, 85, 115
 - equivalenza, 71, 112
- Classe, 18
 - appartenenza, 18
 - comprensione, 24
 - dicotomia, 24
 - differenza, 25
 - estensione, 24
 - inclusione, 18
 - intersezione, 25
 - prodotto cartesiano, 25
 - propria, 26
 - unione, 25
 - vuota, 18
- Deducibilità, 80, 98, 107, 114
 - assioma, 36, 42, 64, 98, 150
 - assunzione, 102
 - deduzione, 81, 98, 100, 114
 - conclusione, 102
 - ipotesi, 101
 - premessa, 101
 - regola d'inferenza, 98
 - sequente, 110
 - tableau, 78
 - tesi, 102
- Formula, 55
 - complessità, 58
 - chiusa, 58
 - clausola, 94
 - forma normale, 72, 92
 - forma di Skolem, 93
 - formula proposizionale, 62
 - legge logica, 67
 - letterale, 62
 - predicato, 55
 - prenessa, 92
 - proposizione, 54
 - segnatura, 54
 - simbolo, 17, 55
 - schema proposizionale, 67
 - schema predicativo, 66
- Funzione, 27
 - biunivoca, 28
 - codominio, 27
 - composizione, 28
 - controimmagine, 28
 - dominio, 27
 - identità, 28
 - immagine, 28
 - iniettiva, 28
 - surgettiva, 28
- Induzione, 36
 - completa, 37
 - strutturale, 37
 - transfinita, 40
- Insieme, 26
 - assiomi, 125
 - coppia, 24
 - coppia ordinata, 24
 - fondazione, 125
 - infinito, 45
 - numerabile, 28
 - parti, 25
 - rappresentabile, 118
 - rimpiazzamento, 28
 - scelta, 42
 - separazione, 26

Linguaggio, 31, 129

- automa, 196
- decidibile, 146
- grammatica, 134
- indecidibile, 147
- monoide, 121, 129
- rappresentabile, 137
- semidecidibile, 146

Modello, 55, 64

- compattezza, 77, 91
- conseguenza, 61
- diagramma, 62
- dominio, 33, 59
- finitezza, 91
- indipendenza, 64
- implicazione formale, 74
- implicazione materiale, 74
- tautologia, 62
- validità, 60
- verità, 61-62

Numero, 18

- cardinale, 43
- naturale, 18, 36
- ordinale, 40

Operatore logico, 78

- connettivo, 54
- congiunzione, 54, 74
- disgiunzione, 54
- equivalenza, 54
- implicazione, 54, 74
- quantificatore, 54

Operazione, 18

- applicazione, 18, 28
- arietà, 20
- argomento, 18
- associativa, 21
- chiusa, 20

Relazione, 22

- binaria, 22
- equivalenza, 22, 29
- ordinamento, 22-23
- partizione, 29

Sequenza, 29

- concatenazione, 30
- lunghezza, 29
- stringa, 30

Struttura, 33

- albero, 34
- algebra, 33
- categoria, 35
- grafo, 34
- modello, 55
- topologia, 35
- struttura relazionale, 34

Teoria, 62

- assiomatizzabile, 150
- completa, 149
- consistente, 89
- Gödeliana, 150
- numerabile, 97
- soddisfacibile, 61

Termine, 55

- chiuso, 58
- costante individuale, 55
- espressione, 32
- λ -espressione, 32
- liberamente sostituibile, 57

Variabile, 32

- assegnamento, 32, 69-70
- formale, 32
- libera, 57
- sintattica, 32
- sostituzione, 58
- vincolata, 33, 57