UNIVERSITÀ DI PISA

DIPARTIMENTO DI MATEMATICA

Laurea Triennale in Matematica

Modelli ricorsivi di frammenti dell'aritmetica

Relatore:

Prof. Marcello Mamino

Candidato:

Andrea Snaidero

ANNO ACCADEMICO 2023/2024

Indice

Introduzione

Questa tesi studia i frammenti dell'aritmetica rispetto all'esistenza di modelli nonstandard ricorsivi. Già nel 1954, al simposio sull'interpretazione matematica dei sistemi formali di Amsterdam, Skolem parlò dei suoi tentativi di trovare un modello nonstandard ricorsivo per l'aritmetica [Goo65, Primo capoverso]. Successivamente, Tennenbaum (1959) dimostrò l'impossibilità di costruire un modello computabile degli assiomi di Peano (espressi nel linguaggio dell'aritmetica del primo ordine). D'altro canto Shepherdson (1964) mostrò che un sottoinsieme degli assiomi di Peano (detto Open Induction) ammette modelli nonstandard ricorsivi. Lavori successivi di Scott e McAloon hanno poi migliorato i risultati di Tennenbaum: il primo ha osservato che nemmeno l'addizione da sola può essere ricorsiva; il secondo (1982) ha indebolito le ipotesi di questi risultati: ha mostrato che già nel sottoinsieme degli assiomi di Peano noto come $I\Delta_0$, né l'addizione né la moltiplicazione possono essere ricorsive [Wil85, Abstract]. Lavori successivi, fra cui ricordiamo per esempio G. Wilme (1985) [Wil85] e Berarducci-Otero (1994) [BO96], hanno precisato ulteriormente la distinzione fra le aritmetiche che ammettono modelli ricorsivi, e quelle che non la ammettono. L'obiettivo di questa tesi è quello di sviluppare le basi della metamatematica dell'aritmetica al fine di presentare i risultati di Tennenbaum, nella forma migliorata di McAloon, e i risultati di Sheperdson.

Per introdurre i risultati principali contenuti in questa tesi, conviene ricordare che il linguaggio dell'aritmetica del primo ordine è costituito dalle operazioni $+$, $*$, la relazione $\leq$, i connettivi logici $\wedge$, $\vee$, $\neg$, $\rightarrow$ e i quantificatori $\forall$, $\exists$ applicati solo a variabili numeriche (non è consentito quantificare su insiemi o funzioni, per esempio). In questo linguaggio è possibile esprimere gli assiomi dell'aritmetica di Peano, avendo cura di trasformare l'assioma di induzione

$$(P(0) \wedge \forall x P(x) \rightarrow P(x+1)) \ \rightarrow \ \forall x P(x)$$

in una collezione infinita di assiomi, uno per ogni proprietà P definita da una formula aritmetica. La teoria così ottenuta, che chiamiamo PA, ha come modello $\mathbb{N}$, però, come è ben noto, ammette altresì modelli nonstandard (ossia estensioni del modello $\mathbb{N}$ contenenti numeri infinitamente grandi). Comunemente, per esempio, si costruiscono modelli nonstandard con la tecnica dell'ultrapotenza. Questo metodo sfrutta l'assioma di scelta, in quanto si basa sull'esistenza di un ultrafiltro non principale. La domanda si pone quindi: è possibile esibire un modello non standard di PA in modo esplicito?

Formalmente, possiamo intendere che un modello "esplicito" di PA sia un modello computabile. Chiamiamo modello computabile il dato di un insieme computabile di stringhe, che rappresentano gli elementi del modello, e due funzioni $+$ e $*$, anch'esse computabili, che soddisfano PA. Il primo risultato che presentiamo dice che non ci sono modelli non standard computabili di PA (teorema di Tennenbaum). L'idea della dimostrazione è che esistono insiemi non computabili, per esempio il cosiddetto insieme della fermata. Usando gli assiomi di Peano e alcune proprietà dei modelli non standard dell'aritmetica, possiamo vedere che, in un modello non standard di PA, c'è necessariamente un numero N, di grandezza infinita, che codifica l'insieme della fermata nel senso seguente. Il numero standard n appartiene all'insieme della fermata se e solo se l'n-esimo primo divide N. Lo strumento fondamentale per mostrare l'esistenza di tale numero codificante è il lemma di overspill, che ci consente di estendere una proprietà che vale per tutti i numeri finiti, a numeri infiniti sufficientemente piccoli. Se ci fosse un modello nonstandard computabile di PA, questo conterrebbe la codifica dell'insieme della fermata, che quindi sarebbe rappresentata da una certa stringa. Usando questa stringa e dei sottoprogrammi che calcolano $+$ e $*$ nel modello, sarebbe possibile scrivere un programma che riconosce l'insieme della fermata. Ne abbiamo quindi un assurdo.

Il risultato di Tennenbaum è valido, in realtà, già per la teoria $I\Delta_0$, ossia il sottoinsieme degli assiomi di Peano in cui l'induzione è ristretta a proprietà P esprimibili mediante formule limitate. Dove chiamiamo *formula limitata* una in cui i quantificatori possono comparire solo nella forma $\exists x \leq y$ o $\forall x \leq y$ (cioè $\exists x$ e $\forall x$ sono vietati se non quando è posto un limite superiore al range di x). In questa tesi daremo una dimostrazione di quest'ultimo risultato, che è dovuto a McAloon.

Un secondo risultato presentato in questa tesi, ottenuto da Sheperdson, riguarda l'esistenza di un modello non standard computabile del sottoinsieme della teoria di Peano noto come Open Induction (OI). Questo si ottiene restringendo l'induzione alle formule senza quantificatori (aperte, ossia sono permesse variabili libere). Questo secondo risultato si ottiene tramite una elegante caratterizzazione algebrica dei modelli di OI. Precisamente un semianello ordinato N è un modello di OI se e solo se è costituito dagli elementi non negativi di una parte intera di un campo reale chiuso. Un campo reale chiuso è un campo ordinato in cui ogni polinomio di grado dispari ha una radice e in cui ogni valore positivo ammette una radice quadrata. Una sua parte intera è un sottoanello discreto che, per ogni elemento x del campo, contiene a che soddisfa $a \leq x < a+1$. Per costruire un modello computabile di OI, ci basiamo sulla costruzione del campo delle serie di Puiseux a coefficienti nel campo dei reali algebrici. Questo è un campo reale chiuso per il teorema di Newton-Puisex, e possiamo dare una descrizione computabile di una sua parte intera appoggiandoci al teorema di eliminazione dei quantificatori per campi reali chiusi di Tarski.

Capitolo 1

Nozioni e fatti preliminari

1.1 Logica e teoria dei modelli

Linguaggi e prime definizioni

Fissiamo il linguaggio dell'aritmetica L, che è costituito dai seguenti simboli specifici di questo linguaggio: $\{S, +, *, 0, \leq\}$, in cui S rappresenta la funzione successore. A questi vanno aggiunti i connettivi logici i quantificatori e il simbolo dell'uguaglianza: $\{\wedge, \vee, \neg, \rightarrow, \forall, \exists, =\}$. In ogni linguaggio inoltre è presente una quantità numerabile di variabili; possiamo esprimere le variabili mediante i simboli $x_1, x_2, \ldots$, però possiamo anche più informalmente usare qualunque lettera dall'alfabeto. Le espressioni algebriche di senso compiuto che sono realizzabili mediante i simboli $\{S, +, *, 0\}$ e le variabili si dicono termini; mentre le proposizioni di senso compiuto esprimibili nel linguaggio si chiamano formule (del prim'ordine). In questo contesto, l'espressione "senso compiuto" può essere definita rigorosamente in modo tale che essa mantenga il suo significato intuitivo. Per essere più precisi dovremmo parlare di L-termini e L-formule, dato che termini e formule dipendono dal linguaggio, ma noi, dovendo lavorare esclusivamente, ometteremo il riferimento al linguaggio quando questo sarà L. Introduciamo ora le sostituzioni. Data una formula φ, un termine t e una variabile x, indichiamo con $\varphi[t/x]$ la formula ottenuta sostituendo t alla variabile x (più precisamente alle sue occorrenze non quantificate) in φ; se x non è una variabile libera in φ, ovvero se non compare in un contesto in cui non è quantificata, allora la sostituzione lascia inalterata la formula. Quando scriviamo tale sostituzione, supponiamo che essa sia legale, ovvero che nessuna variabile libera di t sia quantificata nelle sottoformule in cui compaiono le occorrenze di x non quantificate. Scrivere "$\varphi(x)$" non dà informazioni aggiuntive sulla formula φ rispetto allo scrivere semplicemente "φ", tuttavia la prima forma permette di usare la scrittura "$\varphi(n)$" in luogo di "$\varphi[n/x]$" nel prosieguo del testo.

Vediamo ora come interpretare le formule nel conteso di un insieme specifico di elementi. Fissiamo insieme M dotato di due funzioni binarie, una funzione unaria e una relaziona binaria. Fissando una corrispondenza fra le funzioni e le relazioni del linguag-

gio e quelle di M, e decidendo a quale elemento di M attribuire il valore 0, possiamo interpretare qualunque formula su M mediante la così detta semantica di Tarski, che formalizza l'interpretazione intuitiva delle formule; in questo modo, fissata un interpretazione, ogni formula risulta soddisfatta da M oppure non soddisfatta. Tuttavia formula φ potrebbe essere aperta, ovvero potrebbe contenere delle variabili non quantificate; in tale caso non è chiaro cosa significa interpretare tale formula in M, perché il suo valore di verità potrebbe dipendere dal valore che viene attribuito alle variabili. Per affrontare la questione introduciamo il concetto di valutazione delle variabili. Una valutazione delle variabili (o ambiente) è una funzione che assegna un elemento di M a ciascuna variabile. Consideriamo una valutazione che assegna $a_i \in M$ a x_i. Adesso siamo in grado di dare un'interpretazione parziale alla formula $\varphi(x_1, \ldots, x_n)$ contenente le variabili libere $x_1, \ldots, x_n$; in questo ambiente M soddisfa φ se soddisfa $\varphi(a_1, \ldots, a_n)$, dove quest'ultima scrittura corrisponde al concetto di sostituzione precedentemente descritto in cui sostituiamo elementi di M al posto delle variabili. In generale diciamo che M soddisfa una formula φ se la soddisfa in ogni ambiente. Nel caso in cui un insieme M sia dotato di funzioni e relazioni in modo tale che sia possibile interpretare le formule, diciamo che M è una struttura del linguaggio dell'aritmetica, o semplicemente struttura. Un insieme generico di formule è chiamato teoria; se una struttura M soddisfa tutte le formule contenute in una data teoria T diciamo che M è modello della teoria T e scriviamo $M \vDash T$. Data una teoria T e una formula φ, se per ogni modello M di T accade che $M \vDash \varphi$, allora si dice che φ è conseguenza logica di T e scriviamo $T \vDash \varphi$. Due strutture sono isomorfe se esiste una biezione fra di esse che preserva le relazioni e le funzioni delle stesse. In tal caso ogni formula valida in uno dei modelli è valida anche nell'altro; quest'ultima relazione fra modelli, più debole dell'isomorfismo, si dice equivalenza elementare. Un'ultima osservazione sui modelli è la seguente: dato un modello M e una formula chiusa φ, ovvero senza variabili libere, in virtù del principio del terzo escluso, una delle seguenti asserzioni deve essere vera: $M \vDash \varphi$; $M \vDash \neg\varphi$.

Oltre al concetto di conseguenza logica possiamo introdurre il concetto di deduzione. Possiamo infatti fissare un sistema di deduzione logica, ad esempio la deduzione naturale, che ci permette di definire rigorosamente il concetto di dimostrazione. Un sistema logico di deduzione naturale è il dato una teoria T e di un insieme di regole di inferenza. Le regole di inferenza rappresentano i passaggi logici elementari che costituiscono una dimostrazione. Esse permettono di ottenere una formula, detta conclusione, a partire da un insieme finito di formule, dette premesse, le quali, in una dimostrazione, devono già essere state dimostrate precedentemente (oppure devono essere assiomi). Precisamente, una dimostrazione è una lista di formule tali che ognuna di esse è un assioma oppure può essere ottenuta tramite una regola di inferenza a partire dalle formule precedentemente elencate; la tesi di una dimostrazione è semplicemente l'ultima formula elencata. Un esempio di regola di inferenza è quella che ci permette di dedurre la formula $\varphi \wedge \psi$ a partire dalle formule φ e ψ, oppure quella che permette di dedurre $\varphi \vee \psi$ a partire da φ. Come mostrano questi esempi, le regole di inferenza

rappresentano ragionamenti basilari presenti in qualunque dimostrazione matematica, sono relativamente poche e sono ovvie; pertanto non le elencheremo e assumiamo che il lettore possa immaginarsele. Se a partire da una data teoria T possiamo dimostrare tramite la deduzione naturale la formula φ, allora diciamo che T dimostra φ e scriviamo $T \vdash \varphi$. È noto che il concetto di conseguenza logica e quello di dimostrazione formale coincidono, ovvero $T \vDash \varphi \iff T \vdash \varphi$. Questo risultato, noto sotto ai nomi di teorema di completezza ($\Rightarrow$) e teorema di correttezza ($\Leftarrow$), ci risparmierà dal guaio di dover dare dimostrazioni formali per dimostrare enunciati del tipo $T \vdash \varphi$. Introduciamo ora il concetto di formule equivalenti e diamo alcune definizioni. Si dice che due formule φ e ψ sono equivalenti se vale che $\varphi \vdash \psi$ e $\psi \vdash \varphi$. Data una teoria T diciamo che essa è completa se per ogni formula φ si che $T \vdash \varphi$ o $T \vdash \neg\varphi$, diciamo che è coerente se T non dimostra il falso, o non nega il principio di non contraddizione $\varphi \vee \neg\varphi$. Per il teorema di completezza una teoria è coerente se e solo se ammetta un modello in quanto in nessun modello è possibile dimostrare nessuna della due cose. Per concludere citiamo il teorema di compattezza: dato che ogni dimostrazione è costituita da un numero finito di passaggi logici, deve contenere un numero finito di assiomi. Questo è equivalente a dire che, presa una teoria T, se $T \vdash \varphi$, allora esiste un insieme finito $T_0 \subset T$ tale che $T_0 \vdash \varphi$.

Introduciamo ora un concetto molto importante: quello degli insiemi definibili. Cominciamo fissando una struttura M. In modo non troppo sorprendente, a ogni formula contenente delle variabili aperte possiamo assegnare un insieme: l'insieme dei valori che soddisfano tale formula.

Definizione 1.1. Sia M una struttura. Data una formula $\varphi(x_1, \ldots, x_n)$, specificate (o sottintese) n variabili $x_1, \ldots, x_n$, indichiamo con $\varphi[M^n]$ l'insieme di tutte le n-uple $(a_1, \ldots, a_n) \in M^n$ tali che $\mathbb{N} \vDash \varphi(a_1, \ldots, a_n)$.

Osserviamo che scrivere ogni formula usando esclusivamente i simboli elementari del linguaggio L, ovvero quelli elencati a inizio sezione, comporterebbe uno lavoro dispendioso e in larga parte superfluo. Infatti, potremmo servirci di abbreviazioni. In altre parole potremmo introdurre simboli o notazioni nuove per rappresentare intere formule, in questo modo renderemmo facilmente comprensibili formule elaborate grazie a una stesura chiara e concisa. Introduciamo quindi le seguenti abbreviazioni:

Definizione 1.2. (1) $xy \equiv x * y$
(2) x è un divisore y: $x|y \equiv (\exists z)(x * z = y)$
(3) $x^n \equiv \underbrace{x * x * \cdots * x}_{n \text{ volte}}$
(4) Quantificatori limitati: $(\forall x \leq y)(\varphi) \equiv (\forall x)(x \leq y \to \varphi)$; $(\exists x \leq y)(\varphi) \equiv (\exists x)(x \leq y \wedge \varphi)$

I quantificatori che compaiono nell'ultima definizione si dicono *limitati*, in questo esempio la variabile x si dice *limitata* e y è il *limite* con cui limitiamo x. Inoltre, potremmo stabilire alcune convenzioni per aumentare la leggibilità. Infatti, per ridurre le fonti di confusione, cercheremo di adottare lettere specifiche per rappresentare specifiche tipologie di oggetti; ad esempio useremo le ultime lettere dell'alfabeto, x, y, z, u, v,

per denotare le variabili, le lettere t, s per indicare i termini, le lettere n, m, o, i, j, h, k per indicare numeri naturali e, nel contesto in cui M sia un modello aritmetico, useremo le lettere a, b, c, d per indicare gli elementi di M, chiamati anche parametri.

Frammenti dell'aritmetica

Consideriamo adesso la teoria $\mathrm{T}_{\mathbb{N}}$, composta da tutte formule vere in $\mathbb{N}$. Il teorema di incompletezza di Gödel afferma che ogni teoria aritmetica computabile e coerente non può essere completa. In altre parole, se in un dato sistema logico per l'aritmetica abbiamo una procedura per verificare la correttezza delle dimostrazioni (il sistema è ricorsivo), allora o tale sistema permette di dimostrare qualunque formula (è incoerente), oppure esiste una formula tale che né lei né la sua negazione sono dimostrabili (è incompleto). Questo risultato mostra che $\mathrm{T}_{\mathbb{N}}$ non è ricorsiva dato che è completa e coerente (si spera, in realtà la coerenza di $\mathbb{N}$ non è dimostrabile per via del secondo teorema di incompletezza di Gödel, nondimeno la matematica si basa sull'assunzione che $\mathbb{N}$ sia coerente).

Dato che non c'è speranza di avere una teoria ricorsiva completa dell'aritmetica dobbiamo accontentarci di sottoinsiemi incompleti di $\mathrm{T}_{\mathbb{N}}$; queste teorie sono chiamate frammenti dell'aritmetica. La teoria dell'aritmetica più nota è l'aritmetica di Peano, indicata con le lettere PA, di cui diamo adesso gli assiomi:

(P1) $$S(x) \neq 0$$

(P2) $$S(x) = S(y) \to x = y$$

(P3) $$x + 0 = x$$

(P4) $$x + S(y) = S(x + y)$$

(P5) $$x * 0 = 0$$

(P6) $$x * S(y) = x * y + x$$

(P7) $$x \leq y \leftrightarrow (\exists z)(x + z = y)$$

(P8) $$(\varphi(0) \wedge \varphi(x) \to \varphi(S(x))) \to (\forall x)(\varphi(x))$$

Osserviamo che l'ultimo elencato non è un assioma, bensì uno schema di assiomi, ovvero un insieme contenente un assioma per ogni formula φ. In particolare P8 è lo schema di assiomi per l'induzione. Per ogni formula φ diciamo che $(\varphi(0) \wedge \varphi(x) \to \varphi(S(x))) \to (\forall x)(\varphi(x))$ è un istanza dello schema di induzione. Allo estremo opposto dello spettro dei frammenti dell'aritmetica troviamo l'aritmetica di Robinson, indicata con la lettera

Q. Diamo adesso i suoi assiomi:

(Q1) $$S(x) \neq 0$$

(Q2) $$S(x) = S(y) \to x = y$$

(Q3) $$x + 0 = x$$

(Q4) $$x + S(y) = S(x + y)$$

(Q5) $$x * 0 = 0$$

(Q6) $$x * S(y) = x * y + x$$

(Q7) $$x \leq y \leftrightarrow (\exists z)(x + z = y)$$

(Q8) $$x \neq 0 \to (\exists y)(S(y) = x)$$

Osserviamo che questa teoria è composta da un numero finito di assiomi, e che sono presenti tutti gli assiomi di PA ad eccezione dello schema di induzione. L'unico residuo dello schema di induzione di PA è l'assioma Q8, il quale afferma che tutti i numeri ad eccezione dello zero hanno un predecessore. Questa teoria può a buon diritto essere considerata il più debole segmento dell'aritmetica poiché è un insieme minimale di assiomi per cui rimane valido il primo teorema di incompletezza di Gödel. Infatti, con l'espressione "teoria aritmetica", che abbiamo usato enunciando Gödel, ci riferiamo a una teoria capace di dimostrare Q. Fra Q e PA esiste una gerarchia infinita di frammenti dell'aritmetica. Per introdurli, è necessario definire la gerarchia aritmetica della formule.

La gerarchia aritmetica è una classificazione delle formule definita per ricorsione. Gli insiemi considerati sono di tre tipi: Δ_n, Π_n e Σ_n. Come passo base, poniamo che Δ_0 sia l'insieme delle formule limitate, ovvero delle formule in cui non compaiono quantificatori che non siano limitati. Per completare il passo base poniamo $\Delta_0 = \Sigma_0 = \Pi_0$. Ora per ricorsione poniamo che Π'_{n+1} sia l'insieme delle formule della forma $(\forall x)(\varphi)$ dove $\varphi \in \Sigma_n$, viceversa, poniamo che Σ'_{n+1} sia l'insieme delle formule della forma $(\exists x)(\varphi)$ dove $\varphi \in \Pi_n$. Per completare la definizione, poniamo che Π_{n+1} sia l'insieme delle formule φ tali che esiste $\psi \in \Pi'_{n+1}$ tale che φ e ψ sono equivalente, viceversa, poniamo che Σ_{n+1} sia l'insieme delle formule φ tali che esiste $\psi \in \Sigma'_{n+1}$ tale che φ e ψ sono equivalenti. Infine poniamo che Δ_n sia l'insieme $\Pi_n \cap \Sigma_n$.

Queste classi godono di alcune proprietà. Tutte le classi definite sono chiuse per le operazioni date dall'apposizione di quantificatori limitati e dalla congiunzione mediante i connettivi logici $\wedge$ e $\vee$. In altre parole, se φ e ψ appartengono alla medesima classe, allora anche $(\forall x \leq y)(\varphi)$, $(\exists x \leq y)(\varphi)$, $\varphi \wedge \psi$ e $\varphi \vee \psi$ appartengono alla stessa classe a cui appartengono φ e ψ. Le classi Σ_n sono chiuse rispetto all'apposizione di quantificatori esistenziali e le classi Π_n sono chiuse rispetto all'apposizione di quantificatori universali. Ovvero se $\varphi \in \Sigma_n$ e $\psi \in \Pi_n$, allora $(\exists x)(\varphi) \in \Sigma_n$ e $(\forall x)(\psi) \in \Pi_n$. Inoltre la negazione di una formula di classe Σ_n produce una formula Π_n; al contrario la negazione di una formula Π_n produce. Da questo segue facilmente le classi Δ_n sono chiuse per negazione.

Data una classe della gerarchia C, diciamo che un insieme X definito è di classe C se è definito da un formula di classe C.

Introduciamo ora il frammento dell'aritmetica Open Induction, abbreviato con le lettere OI. Questa teoria è composta da tutti gli assiomi di Q a cui aggiungiamo le istanze degli assiomi di induzione per le formule aperte, ovvero aggiungiamo l'assioma $(\varphi(0) \wedge \varphi(x) \to \varphi(S(x))) \to (\forall x)(\varphi(x))$ per ogni φ formula aperta. Introduciamo anche i frammenti $I\Sigma_n$ e $I\Pi_n$, ottenuti aggiungendo a Q rispettivamente le istanze dell'induzione per le formule di classe Σ_n e Π_n. La teoria $I\Pi_0 = I\Sigma_0$ cade anche sotto al nome di $I\Delta_0$.

Modelli aritmetici

$\mathbb{N}$ è modello per ogni frammento aritmetico. Dato M un modello di Q, diciamo che M è nonstandard se non è isomorfo a $\mathbb{N}$. Sia M un modello di Q non standard. In M deve esistere un elemento 0_M a cui viene attribuito il valore 0, infatti, dato che il simbolo della costante 0 appartiene al linguaggio L esso deve essere attribuito a un elemento di M per definizione interpretazione. Inoltre, sempre poiché l'interpretazione del simbolo di una funzione di L deve essere una funzione di M della stessa arietà, deve esistere una funzione successore $S_M : M \to M$. Ovvero, dato un elemento $a \in M$, deve esistere $b \in M$ tale che $b = S_M(a)$.

Sulla base di questo, possiamo definire per ricorsione una funzione da $\mathbb{N}$ a M. Poniamo $f(0) = 0_M$ e $f(n+1) = S(f(n))$. Dall'iniettività della funzione successore garantita dall'assioma Q2, e dall'assioma Q1, che garantisce che 0 non ha predecessori, otteniemo che la funzione f è iniettiva. Inoltre, sulla base di quanto verrà dimostrato nella prima sezione del prossimo capitolo, f preserva le operazioni e le relazioni, ovvero per ogni n, $m \in \mathbb{N}$ valgono le seguenti relazioni: $f(n) +_M f(m) = f(n+m)$, $f(n) *_M f(m) = f(n*m)$ e $f(n) \leq f(m) \iff n \leq m$. Una funzione iniettiva tra strutture che rispetta operazioni, relazioni e costanti, si dice immersione. La funzione f è dunque un'immersione, e sarebbe anche un isomorfismo se fosse surgettiva. Tuttavia, dato che abbiamo assunto che M sia nonstandard, la funzione f non può essere un isomorfismo di strutture per definizione, quindi esistono degli elementi di M che stanno al di fuori dell'immagine di f, diamo a tali elementi il nome di valori nonstandard.

Vogliamo mostrare ora che la funzione f appena definita è l'unica immersione di $\mathbb{N}$ in M. Sia dunque $g : \mathbb{N} \to M$ un'immersione. Per definizione g deve rispettare le costanti e le funzioni, quindi $g(0) = 0_M$ e $g(S(n)) = S_M(g(n))$; ma poiché in $\mathbb{N}$ la funzione successivo equivale a sommare uno, si dimostra facilmente per induzione che $g = f$. Definiamo ora un'abbreviazione. Dato $n \in \mathbb{N}$ indichiamo con $\bar{n}$ il termine $\underbrace{S(...S(}_{\text{n volte}}0)...)$, che chiamiamo numerale. Si dimostra facilmente per induzione che per ogni $n \in \mathbb{N}$ esiste un unico elemento $a \in M$ che soddisfa in M la formula $a = \overline{n}$. Gli elementi di M di quella forma si chiamano numeri standard. Esiste altra caratterizzazione degli elementi nonstandard: $a \in M$ è nonstandard se esiste un catene infinita di elementi $a_i \in M$ tale che $a_0 = a$ e $S(a_i) = a_{i+1}$. Basta definire gli a_i per ricorsione, se poi troviamo a_n che non ha predecessori allora deve essere 0 per l'assioma Q8 e quindi

$a = \overline{n}$, contro l'ipotesi che fosse nonstandard. Similmente si mostra che nessun numero nonstandard può essere minore di numero standard.

Quanto abbiamo appena detto potrebbe suggerire che i numeri nonstandard siano infinitamente grandi, nel senso che sono sempre maggiori dei numeri standard. Questo sarebbe auspicabile, ma non è sempre vero; vediamo perché. L'assioma Q7 definisce la relazione $\leq$, tuttavia non dobbiamo cadere nell'impressione che questa sia necessariamente una relazione d'ordine. Si consideri infatti il seguente insieme $\mathbb{N} \cup \{\infty_p, \infty_d\}$, dove p sta per pari e d sta per dispari. Definiamo le operazioni nel modo ovvio: somma, moltiplicazione e funzione successore ristrette a $\mathbb{N}$ sono quelle usuali; somme e prodotti che coinvolgono numeri infiniti danno come risultato un numero infinito la cui parità è determinata dalle regole sulla parità, ovvero somma di pari o somma di dispari è pari, somma di pari e dispari è dispari e il prodotto è pari se e solo se uno dei fattori e pari; infine la funzione successore applicata a un infinito dà come risultato l'altro infinito. Si verifica facilmente che questa struttura è un modello di Q, tuttavia $\infty_p \leq \infty_d \leq \infty_p$ ma $\infty_p \neq \infty_d$.

Si consideri ora un estensione del modello precedente:

$$\mathbb{N} \cup \{\infty_p, \infty_d, \infty_p^i, \infty_d^i\},$$

dove i sta per inaccessibile. Dato che è un estensione, le operazioni ristrette al modello precedente sono le stesse del modello precedente; rimane definire somme e prodotti e successore che coinvolgono infiniti inaccessibili. Il successore di infiniti inaccessibili è inaccessibile. Le regole sulla parità di somme e prodotti sono le stesse, diamo ora le seguenti regole: "infinito inaccessibile" + "numero finito" = "infinito inaccessibile"; "qualunque cosa" + "infinito inaccessibile" = "infinito"; "infinito inaccessibile" + "infinito" = "infinito". Diamo anche la regola che nessun prodotto può dare come risultato un infinito inaccessibile; e ovviamente se un fattore è infinito anche il prodotto deve essere infinito, a meno che il fattore di destra non sia 0, in quel caso il prodotto è 0. Si verifica che questo è un modello di Q e che la relazione $0 \leq \infty_p^i$ è falsa.

Un altro modello possibile di Q è il sottoinsieme $M \subset \mathbb{Z}[X]$ dei polinomi a coefficienti interi costituito dal polinomio nullo e dei polinomi con coefficiente direttore positivo. Le operazione sono quelle usuali, la funzione successore coincide con il sommare 1, e $p(x) \leq q(x)$ se e solo se $q(x) - p(x)$ ha coefficiente direttore positivo. In questo modello la relazione $\leq$ è una relazione d'ordine totale, inoltre tale modello è un modello computabile. In senso intuitivo questo significa che è possibile scrivere su carta un qualunque suo elemento e esistono algoritmi per sommare e moltiplicare i suoi elementi. In senso rigoroso lo vedremo più avanti.

La teoria OI è molto più forte di Q, infatti, ad esempio, in ogni suo modello $\leq$ è una relazione d'ordine totale, e quindi, in ogni modello di OI i numeri nonstandard sono maggiori dei numeri standard. La struttura definita precedentemente mediante i poli-

nomi non è un modello di OI. Infatti OI dimostra che $(\forall x)(\exists y)(y^2 \leq x \wedge x \leq (y+1)^2)$. Nel modello in questione, scelta come x l'indeterminata, non esiste nessuna y che soddisfi questa formula. Costruire un modello nonstandard computabile di OI è infatti molto più difficile. Il terzo capitolo capitolo di questa tesi è interamente dedicato alla costruzione di un modello nonstandard computabile di OI.

Salendo ancora la scala della complessità troviamo la teoria $I\Delta_0$. Questa teoria invece non ammette modelli nonstandard computabili. Il secondo capitolo di questa tesi è dedicato al raggiungimento di questo risultato.

1.2 Teoria della computabilità

Una disciplina matematica affine alla logica che viene trattata in questa tesi è lo studio di metodi decisionali e delle funzioni ricorsive. L'importanza di questo settore per tutta la matematica è stato sottolineato da Hilbert, che riteneva che questa disciplina fosse il compito più importante per quella branca della matematica per la quale lui ha suggerito il termine di "metamatematica". Il fatto che questo termine si riferisce oggi alla logica matematica è indicativo di quanto queste due discipline siano indiscindibili. Un metodo (o procedura) decisionale deve essere come una ricetta, deve indicare cosa bisogna fare passo dopo passo in modo tale che nessuna intelligenza sia richiesta per eseguirlo; e il metodo decisionale può essere eseguito da chiunque fintanto che egli sia in grado di leggere le istruzioni e eseguire le direttive [TM51, Introduction]. Un problema che possa essere risolto mediante uno di questi metodi decisionali viene detto computabile, o ricorsivo. Si ritiene (tesi di Church-Turing) che tali problemi possano essere risolti da un qualunque calcolatore. È stata data una definizione formale dei problemi computabili (che si ritiene comprendere tutti i problemi risolvibili dagli essere umani mediante algoritmi). Dato che l'input di un algoritmo è generalmente rappresentato sotto forma di un numero intero, per studiare la calcolabilità e la complessità di un problema qualunque è sufficiente ricondurci allo studio del problema della determinazione di insiemi di numeri naturali (o $n-$uple di numeri naturali).

Insiemi e funzioni ricorsive

Dato $A \subset \mathbb{N}$ un insieme *sufficientemente* semplice potremmo scrivere un metodo di verifica basato su operazioni elementari (es: confronto fra due numeri, determinazione del successore di un numero) per determinare tutti e soli gli elementi di A. Ad esempio potrebbe esistere un metodo che, preso $n \in \mathbb{N}$, sia in grado di stabili mediante un numero finito di passi se $n \in A$ o se $n \notin A$. In questo caso diciamo che l'insieme A e la sua funzione caratteristica sono *ricorsivi totali*, che sono casi speciali di una classe più ampia di funzioni dette *ricorsive generali*. In altri casi, invece, potremmo ottenere una procedura ricorsiva generale non totale. In questo caso, dato un qualunque $n \in A$, questa procedura permette correttamente di concludere che $n \in A$, tuttavia, esiste $n \in \mathbb{N} \setminus A$, che non può essere processato correttamente dalla procedura. Nel senso

che, continuando ciecamente a eseguire i passi seguendo le direttive della procedura, questa non raggiungerebbe mai uno stato di terminazione e continuerebbe all'infinito la sua esecuzione, impedendoci così di raggiungere la conclusione che $n \notin A$; infatti, non potremmo mai essere sicuri che la procedura sia vicina alla terminazione e che non dia come risultato $n \in A$.

Dato che possiamo identificare un'insieme di numeri naturali con la sua funzione caratteristica, è sufficiente studiare solo queste ultime.

Definizione 1.3. L'insieme delle funzioni *primitive ricorsive* è il più piccolo insieme di funzioni da $\mathbb{N}^k$ a $\mathbb{N}$ che soddisfa le seguenti:

- La funzione da $\mathbb{N}$ a $\mathbb{N}$ costante 0 è primitiva ricorsiva
- La funzione "successore" da $\mathbb{N}$ a $\mathbb{N}$ che associa $n+1$ a n è primitiva ricorsiva
- La funzione di proiezione sulla i-esima coordinata è primitiva ricorsiva.
- Sia f una funzione a k variabili e siano $f_1, \ldots, f_k$ funzioni a h variabili. Se f, $f_1, \ldots,$ f_k sono primitive ricorsive allora anche $f \circ (f_1, \ldots, f_k)$ lo è.
- Siano g, h funzioni rispettivamente da $\mathbb{N}^n$ e $\mathbb{N}^{n+1}$ a $\mathbb{N}$. Ovviamente è unica la funzione f da $\mathbb{N}^{n+1}$ a $\mathbb{N}$ che soddisfa $f(n_1, \ldots, n_k, 0) = h(n_1, \ldots, n_k)$ e $f(n_1, \ldots, n_k, n+1) = g(n_1, \ldots, n_k, f(n_1, \ldots, n_k, n))$. Se g e h sono ricorsive primitive allora anche f lo è.

Data una funzione primitiva ricorsiva, le condizioni presenti nella precedente definizione garantiscono l'esistenza di un algoritmo per calcolare tale funzione. La quarta condizione è la più complessa, dal punto di informatico è quella che permette di ripetere più volte un ciclo di istruzioni, tuttavia non c'è pericolo di non terminazione in quanto il numero di ripetizioni è determinato prima dell'inizio dell'esecuzione del ciclo. Non tutte le funzioni ricorsive sempre terminanti sono abbastanza semplici da essere primitive ricorsive, infatti esistono programmi contenti cicli di istruzioni per i quali, sebbene terminino sempre, non è determinabile a priori dell'esecuzione il numero di ripetizioni.

Istruzioni più complesse possono essere anche non terminanti, dunque dobbiamo esprimere formalmente la possibilità che un programma non termini mai l'esecuzione, usiamo a tale scopo il simbolo $\perp$. Consideriamo dunque $\mathbb{N}_\perp := \mathbb{N} \cup \{\perp\}$. Definiamo ora le funzioni ricorsive generali.

Definizione 1.4. Le funzioni *ricorsive generali*, o semplicemente funzioni ricorsive, sono funzioni da $\mathbb{N}_\perp^n$ a $\mathbb{N}$ per un qualche $n \in \mathbb{N}$. Ogni funzione ricorsiva f soddisfa l'identità $f(N) = \perp$ se $\perp$ è il valore di una qualunque delle coordinate di $N \in \mathbb{N}_\perp^n$. Rimane dunque da definire il comportamento di tali funzioni sui numeri naturali (e n-tuple). L'insieme delle funzioni ricorsive è il più piccolo insieme di funzioni da $\mathbb{N}_\perp^k$ a $\mathbb{N}_\perp$ che, oltre a quanto appena detto, soddisfa le seguenti condizioni:

- La funzione con $\mathbb{N}_\perp$ come dominio che su $\mathbb{N}$ è costantemente 0 è ricorsiva generale.
- La funzione "successore" con $\mathbb{N}_\perp$ come dominio che associa $n+1$ a n è ricorsiva generale.
- La funzione di proiezione sulla i-esima coordinata è ricorsiva generale.
- Sia f una funzione a k variabili e siano $f_1, \ldots, f_k$ funzioni a h variabili. Se f, $f_1, \ldots,$ f_k sono ricorsive generali allora anche $f \circ (f_1, \ldots, f_k)$ lo è.
- Siano g, h funzioni rispettivamente da $\mathbb{N}_\perp^k$ e $\mathbb{N}_\perp^{k+1}$ a $\mathbb{N}_\perp$. Ovviamente è unica la funzione f da $\mathbb{N}_\perp^{k+1}$ a $\mathbb{N}_\perp$ che soddisfa $f(n_1, \ldots, n_k, 0) = h(n_1, \ldots, n_k)$ e $f(n_1, \ldots, n_k, n+1) = g(n_1, \ldots, n_k, f(n_1, \ldots, n_k, n))$. Se g e h sono ricorsive generali allora anche f lo è.
- Sia f una funzione a $k+1$ variabili. Sia g una funzione a k variabili definita come segue:
  - $g(n_1, ..., n_k) = \perp$ se per ogni n che soddisfa $f(n_1, \ldots, n_k, n) = 0$ esiste $m \leq n$ che soddisfa $f(n_1, \ldots, n_k, m) = \perp$.
  - $g(n_1, \ldots, n_k) = n$ se n è il più piccolo numero naturale che soddisfa $f(n_1, \ldots, n_k, n) = 0$ e $\forall m \leq n\, f(n_1, \ldots, n_k, m) \neq \perp$.

  Una g così definita è unica e se f è ricorsiva generale anche g lo è.

Analogamente al caso delle primitive ricorsive, a ogni funzione ricorsiva generale possiamo associare un programma avente come operazioni elementari quelle descritte nelle condizioni soprascritte. Tale programma può ricevere in ogni argomento dell'input solo numeri naturali e non termina l'esecuzione ("va in loop") quando la funzione associata restituisce $\perp$. L'unica possibilità di non terminazione è data dall'operazione descritta dall'ultima condizione, questa descrive *l'operatore di minimalizzazione*, ovvero un operatore che cerca per tentativi un valore particolare e va in loop se questa ricerca non ha mai fine. Le funzioni che non restituiscono $\perp$ (quando non lo ricevono in input) si dicono *ricorsive totali*, mentre le altre sono *ricorsive parziali*. Data f ricorsiva si chiama *dominio di* f l'insieme dei valori $N \in \mathbb{N}^k$ per cui $f(N) \in \mathbb{N}$, cioè i valori ammissibili per cui f non si impalla.

Definizione 1.5. Sia $f : \mathbb{N} \to \mathbb{N}$ una funzione ricorsiva generale. Diciamo che l'insieme dei valori che annullano f è *semidecidibile*, se f è anche totale, allora diciamo che tale insieme è *decidibile*.

Osserviamo che se un insieme X e il suo complementare sono semidecidibili, allora sono anche decidibili. Infatti, ogni numero naturale appartiene a X o al suo complementare; quindi, eseguendo contemporaneamente la procedura ricorsiva generale che determina gli elementi di X e quella che determina gli elementi di $\mathbb{N} \setminus X$, per ogni numero n sono sicuro di portare a terminazione almeno una delle due procedure in tempo finito. In questo modo ho realizzato una procedura ricorsiva totale per determinare gli

elementi di X.

Osserviamo anche che un insieme X è semidecidibile se e solo se enumerabile mediante una funzione ricorsiva totale. Infatti eseguendo la procedura generale che determina X, un po' per volta su tutti i numeri, e elencando via via i numeri per la quale questa termina, ottengo la funzione cercata. Viceversa, per rispondere alla domanda "$n \in X$?", sarà sufficiente eseguire funzione ricorsiva che enumera X, e terminare l'esecuzione, dando risposta affermativa, se e quando verrà elencato il numero n.

Inoltre, se X è decidibile e infinito, allora può essere enumerato per mezzo di una funzione totale non decrescente. Infatti posso enumerare gli elementi semplicemente eseguendo la procedura a partire da 0 e continuando ogni volte col numero successivo; viceversa, per sapere se $n \in X$ sarà sufficiente aspettare che funzione ricorsiva crescente che enumera X elenchi n oppure lo superi.

Potrà essere più comodo in futuro definire una funzione ricorsiva dandone semplicemente le istruzioni che permettono di computarla. Tali istruzioni possono richiedere di memorizzare una quantità arbitraria ma finita e prefissata di variabili, potrebbero richiedere di elaborare tali variabili tramite le operazioni aritmetiche o tramite altre funzioni ricorsive, potrebbero richiedere di determinare il valore di verità di una uguaglianza o di un confronto fra espressioni aritmetiche e potrebbero contenere cicli di tipo *for* o *while*. Dimostrare che si possono eseguire tutti questi tipi di istruzioni non è difficile una volta esplicitato il legame fra funzioni ricorsive e macchine di Turing.

Macchine di Turing

Come accennato prima, una data funzione ricorsiva generale può essere calcolata da un calcolatore, cioè una macchina (un computer). Formalmente è stato necessario introdurre un'astrazione rigorosa per descrivere matematicamente i calcolatori: le *macchine di Turing*. Dare una descrizione scrupolosa di tali macchine è al di là degli scopi di questo testo, è tuttavia utile richiamare alcune nozioni. Una macchina di Turing prende in input una quantità prestabilita di numeri naturali, li elabora seguendo delle istruzioni precise e, se le istruzioni terminano, restituisce come output un numero naturale. Ovviamente una macchina di Turing rappresenta la funzione che associa a un input il suo output. Ad esempio la macchina M, presi in input i numeri $n_1, \ldots, n_k$, restituisce il numero $M(n_1, \ldots, n_k)$. Nonostante ogni macchina di Turing sia progettata per prendere in input una quantità prestabilita di dati numerici essa non dà errore se ne riceve in numero sbagliato, infatti le istruzioni che esegue una macchina di Turing sono eseguibili su qualunque input. È un fatto che le funzioni rappresentate da una macchina di Turing siano ricorsive generali e che ogni funzione ricorsiva sia rappresentata da una macchina di Turing. Le macchine di Turing possono essere descritte da un *codice*, il quale specifica le istruzioni da seguire passo passo per elaborare i dati. Indichiamo con $\lceil M \rceil$ il codice di M. Inoltre, presa una funzione ricorsiva f, dato che è rappresentabile da una macchina di Turing M, anche a f possiamo associare il codice $\lceil f \rceil = \lceil M \rceil$. È

interessante notare che tali codici sono rappresentabili tramite numeri naturali (anzi, formalmente sono letteralmente numeri naturali) e dunque possono essere dati come input a altre macchine di Turing o funzioni ricorsive; per altro, secondo le convenzioni usuali, ogni numero naturale rappresenta il codice di una qualche macchina di Turing.

Un primo uso dei codici permette di preinserire alcuni input numerici in un programma prima della sua esecuzione. Ovvero esiste una macchina di Turing che prende in input un codice $\lceil M \rceil$ e un numero n e restituisce $S_k(\lceil M \rceil, n)$, il codice della macchina di Turing che associa a $n_2, \ldots, n_k$ il numero $M(n, n_2, \ldots, n_k)$.

Non tutte le macchine di Turing possono svolgere qualunque problema: nella la maggior parte dei casi esse possono svolgere solo un problema specifico; tuttavia si può costruire una *macchina di Turing universale*, ovvero un calcolatore che prende in input un codice e una quantità prestabilita di dati numerici e elabora tali dati implementando il codice. Indichiamo con U_n la macchina universale riceve in ingresso n input numerici più il codice di una macchina. Ad esempio, per ogni codice $\lceil M \rceil$ e dato numerico n si ha la seguente identità: $U_1(\lceil M \rceil, n) = M(n)$.

1.3 Legami fra computabilità e aritmetica

In questa sezione verranno mostrati i legami fra i vari concetti introdotti fin qui. Fissiamo il modello $\mathbb{N}$. Presentiamo adesso alcuni fatti di più o meno facile verifica.

Si verifica facilmente che tutti gli insiemi Δ_0 sono primitivi ricorsivi. Da questo si deduce altrettanto facilmente che gli insiemi Σ_1 sono semidecidibili ma non necessariamente decidibili. Inoltre si può dimostrare che tutti gli insiemi semidecidibili sono Σ_1.

Non abbiamo ancora dimostrate l'esistenza di insiemi semidecidibili che non siano decidibili, lo faremo ora. Chiamiamo H_0 l'insieme dei codici di macchine di Turing a 0 input che terminano. Tale insieme si chiama insieme della fermata, ed è ovviamente semidecidibile; una procedura per determinare se un dato programma si arresta o va in loop consiste nell'eseguire un programma e dare risposta affermativa se e quando tale programma si arresta. Il problema di tale procedura è che in presenza di un programma che va in loop anch'essa va in loop. Si può dimostrare che questo insieme non è decidibile, ovvero non esiste nessuna funzione ricorsiva totale che valga 0 su tutti e soli gli elementi dell'insieme della fermata.

Teorema 1.6 (Il problema della fermata)**.** L'insieme della fermata non è decidibile.

Dimostrazione. Supponiamo per assurdo che esista una funzione f ricorsiva totale soddisfi la seguente condizione:

$f(\alpha) = 0 \iff$ "α, interpretato come codice di un programma a zero input, termina".

Questa condizione ha senso perché il numero di input che riceve un dato programma non è scritto nel codice per come questo è definito usualmente, e tutti i numeri possono essere interpretati come codici di programmi che non ricevono input. Si consideri adesso la seguente funzione ricorsiva generale *neg*: questa funzione da come risultato 0 se riceve in input un valore diverso da 0, altrimenti va in loop. Componendo le due funzioni otteniamo $h = neg \circ f$. Si cerchi ora di calcolare $h(s_1(\lceil h \rceil, \lceil h \rceil))$. Se $f(s_1(\lceil h \rceil, \lceil h \rceil))$ fosse 0 significherebbe che h non andrebbe in loop, tuttavia ricevuto 0, *neg* va in loop e dunque anche h. Viceversa se $f(s_1(\lceil h \rceil, \lceil h \rceil))$ fosse diverso da 0 allora h dovrebbe andare in loop, ma ricevuto un valore diverso da 0 *neg* restituisce immediatamente 0, pertanto h non va in loop. Dato che supponendo l'esistenza di una funzione ricorsiva totale che determini l'insieme della fermata abbiamo ottenuto un assurdo tale funzione non esiste e l'insieme della fermata non è decidibile. □

Definizione 1.7. Due insiemi A, $B \subset \mathbb{N}$ semidecidibili si dicono *inseparabili* se non esiste un insieme decidibile $C \subset \mathbb{N}$ tale che $A \subset C$ e $B \cap C = \emptyset$.

Esistono vari insiemi inseparabili. Consideriamo, ad esempio, una codifica delle formule aritmetiche per mezzo di numeri naturali, diciamo che il numero n corrisponde alla formula φ_n. Consideriamo gli insiemi $A = \{$codifiche delle conseguenze logiche di Q$\}$ e $B = \{$codifiche delle negazioni delle conseguenze logiche di Q$\}$. Questi due insiemi sono semidecidibili, infatti per dimostrare in Q una formula dimostrabile è sufficiente elencare tutti i teoremi in Q fintanto che non si incontra la dimostrazione cercata. Tuttavia sono inseparabili, infatti supponendo che non lo siano è possibili costruire una teoria aritmetica ricorsiva, coerente e completa, contravvenendo così al teorema di incompletezza di Gödel. Supponiamo infatti per assurdo che esista un insieme decidibile $C \subset \mathbb{N}$ tale che $A \subset C$ e $B \cap C = \emptyset$. A meno di identificare le formule con le loro codifiche possiamo assumere che A, B, C siano insieme di formule. È un fatto che in Q si possa codificare in modo ricorsivo il concetto di dimostrazione e quindi il concetto di coerenza. Ovvero, considerata una teoria T ricorsiva, ad esempio finita, e una formula φ, si possa ottenere ricorsivamente una formula $A(T, \varphi)$ tale che $Q \vdash A(T, \varphi) \iff$ "$T \cup \{\varphi\}$ è coerente". Si costruisca dunque ricorsivamente la seguente teoria $T_0 = Q$, $T_{n+1} = T_n\{\neg\varphi_n\}$ se $A(T_n, \varphi_n) \notin C$, $T_{n+1} = T_n \cup \{\varphi_n\}$ altrimenti. Poniamo poi la teoria $T = \bigcup T_n$. La teoria così costruita è ricorsiva, infatti abbiamo appena esibito un metodo per ricavarla. È anche completa, infatti ogni per ogni formula φ_n si ha che $\varphi_n \in T_n \subset T$ o che $\neg\varphi_n \in T_n \subset T$. Rimane da dimostrare la coerenza. Ogni teoria T_n è coerente, infatti $T_0 = Q$ è coerente, e se T_n è coerente allora lo è anche T_{n+1} poiché se $T_n \cup \{\varphi\}$ non è coerente allora per il principio del terzo escluso $T_n \cup \{\neg\varphi\}$ deve essere coerente. Allora anche T è coerente, infatti ogni dimostrazione

del falso, o del principio di non contraddizione, deve contenere un numero finito di passaggi logici, quindi di assiomi, pertanto, se fossero dimostrabili in T, lo sarebbero anche in T_n per n abbastanza grande.

Teorema 1.8. Esistono insiemi inseparabili.

Dimostrazione. Esibiamo una coppia (A, B) di insiemi inseparabili: sia $A \subset H_0$ l'insieme dei codici delle macchine di Turing a zero input, terminanti, che danno come risultato 0; sia $B \subset H_0$ l'insieme dei codici delle macchine di Turing a zero input, terminanti, che danno come risultato 1. A e B sono semidecidibili e disgiunti. Supponiamo per assurdo che esista C decidibile tale che $B \subset C \subset \mathbb{N} \setminus A$. Esiste dunque una macchina di Turing M che *decide* C, ovvero che rappresenta la funzione che fa 0 sui valori di C e 1 altrove. Consideriamo ora la funzione f che associa n a $M(s_1(n, n))$, anche f è ricorsiva totale e su ogni input dà come risultato o 0 o 1. La contraddizione si presenta interrogandoci sul valore di $f(\ulcorner f \urcorner)$: se infatti tale valore è 0 allora $s_1(\ulcorner f \urcorner, \ulcorner f \urcorner) \in C$ per definizione di M, quindi $s_1(\ulcorner f \urcorner, \ulcorner f \urcorner) \notin A$, ma allora eseguendo il codice $s_1(\ulcorner f \urcorner, \ulcorner f \urcorner)$ non possiamo ottenere 0 per definizione di A, cioè $f(\ulcorner f \urcorner) \neq 0$; con lo stesso ragionamento concludiamo che tale valore non può essere nemmeno 1. □

Introduciamo adesso la definizione formale dei modelli ricorsivi, che saranno i principali oggetti di studio di questa tesi.

Come la parola suggerisce, un modello ricorsivo, o computabile, è una struttura che deve essere descrivibile in modo esplicito, ovvero dobbiamo poterne elencare gli elementi e deve esistere una procedura per calcolarne le funzioni e le relazioni. Nel caso di un modello aritmetico dobbiamo poter enumerare i suoi elementi e poterne calcolare somma, prodotto, successore, e dobbiamo avere anche una procedura per decidere se un dato elemento è minore di un altro, o se due elementi sono uguali (nel senso che ogni elemento potrebbe comparire più volta nell'enumerazione, noi dobbiamo essere in grado di individuare quanto questo accade).

Definizione 1.9. Sia $(M, 0_M, S, +, *, \leq, =)$ una $L-$struttura. M si dice ricorsivo se vale che $M \subset \mathbb{N}$ è un insieme decidibile e sia le funzioni $+$, $*$, $S : M \to M$ sia le relazioni $\leq$, $=\subset \mathbb{N}^2$ sono ricorsive. Se richiediamo che solo una delle operazioni sia ricorsiva, allora permettiamo all'altra di non esserlo, tuttavia continuiamo ad imporre che la funzione successore e le relazioni $\leq$, $=$ siano ricorsive.

Osservazione 1.10. Questa definizione di modello ricorsivo si adatta a qualunque linguaggio, ad esempio si può parlare di campo ordinato ricorsivo.

Capitolo 2

Open Induction e teorema di Tennenbaum

In questo capitolo descriviamo i modelli nonstandard dell'aritmetica e sviluppiamo alcuni strumenti di base che ci serviranno per dimostrare il teorema di Tennenbaum. In particolare dimostriamo alcune proprietà aritmetiche e una versione indebolita del principio del minimo valido per $I\Delta_0$. Diamo come referenza generale per questo capitolo il libro Metamathematics of First-Order Arithmetic [HP98], tuttavia avvertiamo il lettore sul fatto che nel libro l'assioma Q7 è dato in modo leggermente diverso.

2.1 Aritmetica di Q, di OI e principio di overspill

Dimostriamo qui alcune proprietà aritmetiche valide in qualunque modello dell'aritmetica di Robinson (Q), dopodiché ci sposteremo nella teoria Open Induction (OI) nella quale dimostreremo alcune proprietà più complesse che si riveleranno utili nelle sezioni successive di questo capitolo e nel capitolo seguente. Come riferimento bibliografico per approfondire questi argomenti indichiamo la prima sezione del primo capitolo del libro Metamathematics of First-Order Arithmetic [HP98]. L'ultimo argomento trattato in questa sezione è il principio di overspill, uno strumento utile che permette di trovare numeri nonstandard che soddisfano determinate proprietà.

Proprietà aritmetiche di Q

Ricordiamo gli assiomi di Q:

(Q1) $$S(x) \neq 0$$

(Q2) $$S(x) = S(y) \to x = y$$

(Q3) $$x + 0 = x$$

(Q4) $$x + S(y) = S(x + y)$$

(Q5) $$x * 0 = 0$$

(Q6) $$x * S(y) = x * y + x$$

(Q7) $$x \leq y \leftrightarrow (\exists z)(x + z = y)$$

(Q8) $$x \neq 0 \to (\exists y)(S(y) = x)$$

Lemma 2.1. Per ogni n, $m \in \mathbb{N}$ si ha che Q dimostra le seguenti formule:

(1) $$\overline{n} + \overline{m} = \overline{n + m},$$

(2) $$\overline{n} * \overline{m} = \overline{n * m},$$

(3) $$\overline{n} \neq \overline{m} \text{ se } n \neq m,$$

(4) $$x + y = 0 \to x = 0 \wedge y = 0$$

(5) $$x * y = 0 \to x = 0 \vee y = 0$$

(6) $$x \leq \overline{n} \leftrightarrow x = 0 \vee x = \overline{1} \vee \cdots \vee x = \overline{n}.$$

Dimostrazione. Dimostriamo (1) per induzione su m. Per $m = 0$ si ha Q$\vdash \overline{n} + 0 = \overline{n}$ che discende da (Q3). Assumendo ora $Q \vdash \overline{n} + \overline{m} = \overline{n + m}$, usando (Q4) segue che Q dimostra che $\overline{n} + \overline{m + 1} = \overline{n} + S(\overline{m}) = S(\overline{n + m}) = \overline{n + m + 1}$.

Le formule (2) e (3) si dimostrano in modo analogo.

Dimostriamo (4). Se y non fosse 0 allora per Q8 avrebbe un predecessore y', da Q4 seguirebbe $S(x + y') = 0$ contravvenendo all'assioma Q1. Dato che $y = 0$ per Q3 otteniamo che $x = 0$.

Dimostriamo (5). Se y è diveso da 0 allora per Q8 avrebbe un predecessore y' e da Q6 segue $x * y' + x = 0$. Per quanto appena dimostrato al punto precedente si ha $x * y' = x = 0$, in particolare $x = 0$.

Dimostriamo (6). L'implicazione $\leftarrow$ si può facilmente dimostrare usando (1), dunque dimostriamo per induzione su n l'altra implicazione. Il passo base segue immediatamente dal punto (4) appena dimostrato. Supponiamo la formula vera per n e consideriamo $n+1$. Sappiamo per ipotesi che esiste y tale che $x+y = \overline{n+1}$. Se $y = 0$, allora per Q3 si ha $x = \overline{n+1}$, altrimenti, per Q8 si ha $y = y' + 1$, dunque per Q4 $S(x + y') = \overline{n+1}$. Si conclude usando Q2 e l'ipotesi induttiva. □

I fatti precedenti dimostrano che la verità di una formula chiusa di classe Δ_0 si preserva in Q, più precisamente, vale la seguente affermazione.

Osservazione 2.2. Presa una formula φ, se questa è chiusa e di classe Δ_0, allora vale il seguente risultato:

$$\mathbb{N} \vDash \varphi \iff \mathrm{Q} \vdash \varphi.$$

Dimostrazione. Infatti, usando la 2.1(4), possiamo sostituire i quantificatori e ottenere una formula proposizionale sulle formule atomiche di L, il cui valore di verità si conserva in Q in virtù di 2.1(1) e 2.1(2). Ad esempio $(\forall x \leq \overline{n})(\psi(x))$ è equivalente a $\bigwedge_{m=0}^{n} \psi(\overline{m})$, mentre $(\exists x \leq \overline{n})(\psi(x))$ è equivalente a $\bigvee_{m=0}^{n} \psi(\overline{m})$. □

Vale in realtà un fatto ancora più forte: si conserva il valore di verità delle formule Σ_1.

Lemma 2.3. Presa una formula φ, se questa è chiusa e di classe Σ_1, allora vale il seguente risultato:

$$\mathbb{N} \vDash \varphi \iff \mathrm{Q} \vdash \varphi.$$

Dimostrazione. Prendiamo $\varphi(x)$ di classe Δ_0 e dimostriamo che $Q \vdash (\exists x)(\varphi(x)) \iff \mathbb{N} \vDash (\exists x)(\varphi(x))$. Ovviamente si ha $Q \vdash (\exists x)(\varphi(x)) \implies \mathbb{N} \vDash (\exists x)(\varphi(x))$ per il teorema di correttezza, infatti $\mathbb{N}$ è modello di Q. Per quanto riguarda il viceversa basta considerare la seguente catena di implicazioni:

$$\begin{gathered}
\mathbb{N} \vDash (\exists x)(\varphi(x)) \\
\exists n \in \mathbb{N} \text{ tale che } \mathbb{N} \vDash \varphi(n) \\
\exists n \in \mathbb{N} \text{ tale che } \mathbb{N} \vDash \varphi(\overline{n}) \\
\exists n \in \mathbb{N} \text{ tale che } \mathrm{Q} \vdash \varphi(\overline{n})^{1} \\
\mathrm{Q} \vdash (\exists x)(\varphi(x))
\end{gathered}$$

□

Si riveleranno molto utili le proprietà di dominio ordinato, con le quali dimostreremo l'esistenza e l'unicità del quoziente e del resto della divisone euclidea, tutte proprietà essenziali per le dimostrazioni successive. Tuttavia la teoria Q non è abbastanza forte da permetterci di dimostrarle, ci serviranno infatti gli assiomi di induzione.

[1] poiché $\varphi(\overline{n})$ è una formula chiusa di classe Δ_0

Aritmetica di OI

Teorema 2.4. OI dimostra le seguenti formule:

$$x + y = y + x, \tag{1}$$
$$x + (y + z) = (x + y) + z, \tag{2}$$
$$x * y = y * x, \tag{3}$$
$$x * (y + z) = x * y + x * z, \tag{4}$$
$$x * (y * z) = (x * y) * z, \tag{5}$$
$$x + z = y + z \to x = y, \tag{6}$$
$$x \leq y \vee y \leq x, \tag{7}$$
$$x \leq y \wedge y \leq x \to x = y, \tag{8}$$
$$x \leq y \wedge y \leq z \to x \leq z, \tag{9}$$
$$x \leq y \leftrightarrow x + z \leq y + z, \tag{10}$$
$$z \neq 0 \wedge x * z = y * z \to x = y, \tag{11}$$
$$z \neq 0 \to (x \leq y \leftrightarrow x * z \leq y * z). \tag{12}$$

Dimostrazione. Dato che le formule enunciate non sono quantificate useremo gli assiomi di induzione dentro a OI. La prima dimostrazione sarà più dettagliata, dopo verranno omessi i dettagli. La cosa importante è essere sicuri di usare un istanza dello schema di induzione per una formula la cui complessità appartiene alla classe per cui stiamo assumendo valga l'induzione; nel nostro caso la classe delle formule aperte.

(1) Dimostriamo prima $(\forall x)(0 + x = x)$. Usiamo l'induzione sulla formula $\varphi(x) \equiv 0 + x = x$. $\varphi(0)$ segue da Q8. Per dimostrare $(\forall x)(\varphi(x) \to \varphi(S(x)))$ assumiamo $0 + x = x$ e eseguiamo i seguenti conti usando Q4, in questo modo otteniamo che $0 + S(x) = S(0 + x) = S(x)$. Adesso dimostriamo $\varphi(y) \equiv S(x) + y = S(x + y)$. Usiamo l'induzione su y. $\varphi(0)$ segue da Q8. Per dimostrare $(\forall y)(\varphi(y) \to \varphi(S(y)))$ assumiamo $S(x) + y = S(x + y)$ e svolgiamo i seguenti conti $S(x) + S(y) = S(S(x) + y) = S(S(x + y)) = S(x + S(y))$. Dimostriamo infine (1) per induzione su x, il passo base l'abbiamo già svolto. Assumiamo ora $x + y = y + x$ e usando quanto appena dimostrato contiamo come segue: $S(x) + y = S(x + y) = S(y + x) = y + S(x)$.

(2) Si dimostra per induzione su z.

(3) Si segue lo stesso schema della dimostrazione di (1): dimostrare per induzione su x le formule $0 * x = 0$, $S(y) * x = y * x + y$ e $x * y = y * x$.

(4)-(6) Si dimostrano per induzione su z.

(7) Si dimostra per induzione su x.

(8)-(10) Si dimostrano usando i punti precedenti.

(11) Dimostriamo la contronominale, $x \neq y \to x * z \neq y * z \vee z = 0$. Per (7) possiamo assumere senza perdità di generalità che $x \leq y$. Usando l'induzione su z dimostriamo l'asserzione più forte

$$x < y \to x * z < y * z \vee z = 0. \tag{i}$$

dove ovviamente $x < y \equiv x \leq y \wedge x \neq y$. Osserivamo che $x < y$ è equivalente a $(\exists u)(u \neq 0 \wedge x + u = y)$. Non c'è niente da dimostrare per $z = 0$, dunque assumiamo (i) vera e consideriamo $S(z)$. Prendiamo $v \neq 0$ tale che $y * z = x * z + v$ e svolgiamo i seguenti calcoli:

$$y * S(z) = y * z + y = x * z + v + x + u = x * S(z) + (u + v).$$

(12) Assumiamo $z \neq 0$. L'implicazione $x \leq y \to x * z \leq y * z$ è facile, dunque dimostriamo l'altra, o meglio ne dimostriamo la contronominale. Per (8) otteniamo che $\neg(x \leq y)$ è equivalente a $y < x$. Ora usando (i) della dimostrazione di (11) otteniamo $\neg(x \leq y) \to \neg(x * z \leq y * z)$. □

Osservazione 2.5. Per quanto detto fin qui, OI dimostra che $\leq$ è un ordine totale e che l'addizione e la moltiplicazione per un elemento diverso da 0 sono strettamente crescenti, e dalla proprietà commutative segue che ogni numero è maggiore di 0. Inoltre $\leq$ è discreto e $S(x)$ è il più piccolo elemento maggiore di x. Quest'ultima osservazione segue dal fatto non esiste $0 < x < 1$, altrimenti, chiamato y il predecessore di x, si ha $x = 1 * x = 1 * (S(y)) = y + 1 > 1 > x$, che è un assurdo. Inoltre le proprietà associative delle operazioni rendono superflue le parentesi nelle scritture del tipo $a + (b + c)$, noi quindi le ometteremo. Si dimostra facilmente in OI anche che $x * \overline{1} = x$ e che per ogni $n \in \mathbb{N}$ si ha $x * \overline{n} = \underbrace{x + x + \cdots + x}_{n \text{ volte}}$.

Inoltre in virtù di (6), possiamo definire la differenza e divisone (per un numero diverso da zero):

Definizione 2.6.

$$x = y - z \equiv x + z = y \vee (y < z \wedge x = 0),$$
$$x = y/z = yz^{-1} \equiv (\exists u)(uz = y) \wedge xz = y \wedge z \neq 0.$$

Osservazione 2.7. Abbiamo dato la definizione di un termine, in generale, presa la notazione per nuovo termine $\mathfrak{t}(X)$, con $x = \mathfrak{t}(X) \equiv \varphi(x, X)$ intendiamo dire che per ogni formula $\psi(x)$ si ha $\psi(\mathfrak{t}(X)) \equiv (\exists x)(\varphi(x, X) \wedge \psi(x))$.

Osserviamo che per poter dividere, è necessario che il dividendo sia multiplo del divisore, e che questo sia diverso da 0.

Si possono dimostrare alcune immediate proprietà della sottrazione e della divisione

Lemma 2.8. OI dimostra le seguenti formule:

(1) $$(x - y)z = xz - yz,$$

(2) $$x|zx \pm y \to x|y,$$

(3) $$x|z - yx \to x|z,$$

(4) $$(x \pm y)/z = x/z \pm y/k.$$

Dimostrazione. (1) È conseguenza immediata della proprietà distributiva della somma e dell'unicità della sottrazione: se $u + y = x$, allora $xz = (u + y)z = uz + yz \implies (x - y)z = uz = xz - yz$, se invece $x < y$ allora $xz < yz$ e entrambi i membri sono nulli.

(2) Se $cx = zx + y$, allora $y = (c - z)x$, nel caso del meno si applicano le definizioni e ci si riconduce al caso del $+$.

(4)-(5)Immediate □

Lemma 2.9. In OI si può dimostrare il lemma della divisione con resto: $y \neq 0 \to (\exists! u \leq x)(\exists! v \leq y)(x = uy + v)$.

Dimostrazione. Sia $\varphi(u)$ la formula $y * u \leq x$. Si ha che $\varphi(0)$ e $\neg\varphi(x + 1)$ sono dimostrabili, dunque per induzione sulle formule non quantificate esiste u tale che $y * u \leq x$ e $x < y * (u + \overline{1})$. Dato che $\leq$ è totale e la moltiplicazione per un numero diverso da 0 è crescente, u è univocamente determinato, e inoltre $u \leq x$. Sia $v = x - yu$, anche v è unicamente determinato per 2.4(6). Si dimostra pure che $v < y$ altrimenti si avrebbe $y * (u + 1) \leq y * u + v = x$ che contraddice la costruzione di x; questo termina la dimostrazione. □

L'ultimo risultato, valido per OI, che esponiamo, concerne la codifica per le coppie di numeri. Per fare ciò abbiamo prima bisogno di introdurre il concetto di pari e dispari.

Definizione 2.10. x è pari: $even(x) \equiv \overline{2}|x$;
x è dispari: $\neg even(x)$.

È facile dimostrare che somma o prodotto di pari è pari, per dimostrare le altre regole sulla parità della somma e del e prodotto è utile mostrare che i numeri dispari sono della forma $\overline{2}y + \overline{1}$, dopodiché segue tutto facilmente.

Lemma 2.11. OI dimostra $even(x) \vee even(x + \overline{1})$.

Dimostrazione. 0 è pari. Assumiamo $x \neq 0$. Consideriamo la formula $\overline{2}y \leq x$ e denotiamola con $\varphi(y)$. Dato che OI verifica $\neg\varphi(x)$, dato che $\varphi(y)$ è senza quantificatori, OI dimostra esiste z minimo elemento che soddisfa $\varphi(z)$, inoltre $z \neq 0$ perché $x \neq 0$ dunque $z = u + \overline{1}$ è successore. Poiché $\overline{2}u \leq x < \overline{2}(u + \overline{1})$, per le proprietà dimostrate in OI, segue che $x = \overline{2}u \vee x + \overline{1} = \overline{2}(u + \overline{1})$ che è la tesi. □

Lemma 2.12. OI dimostra $\neg even(x) \to (\exists y)(x = \overline{2}y + \overline{1})$.

Dimostrazione. Se x non è pari allora lo è $x + \overline{1}$ per quanto appena dimostrato. Sia y' la metà di $x + \overline{1}$. Dato che $x + \overline{1}$ è dispari, è diverso da zero e quindi anche y' deve essere diverso da zero, perciò (Q8) y' ha un predecessore che chiamiamo y. Per le regole di cancellazione e le altre proprietà aritmetiche otteniamo $x + \overline{1} = \overline{2}(y + \overline{1}) = \overline{2}y + \overline{2} = \overline{2}y + \overline{1} + \overline{1} \implies x = \overline{2}y + \overline{1}$. □

È utile tenere ben presente questo risultato per tutta la sezione successiva, poiché useremo spesso le regole sulla parità per somme e prodotti senza dare i dettagli.

Diamo ora la definizione di coppia e verifichiamo che è ben posta.

Definizione 2.13. $z = (x, y) \equiv \overline{2}z = (x + y + \overline{1})(x + y) + \overline{2}x$.

Osservazione 2.14. È chiaro che per ogni (x, y) esiste unico z che soddisfa $z = (x, y)$.

Lemma 2.15. OI dimostra che $(\forall z)(\exists! x, y)(z = (x, y))$.

Dimostrazione. L'idea della dimostrazione consiste nel determinare univocamente prima $u = x + y$ e poi x e y. Prendiamo uno z qualunque e consideriamo la formula $\varphi(u) \equiv u(u + \overline{1})) \leq z$. Come sempre, usiamo il principio del minimo e consideriamo u che soddisfa $\varphi(u) \wedge \neg\varphi(u + \overline{1})$, tale valore esiste perché $\neg\varphi(u)$ è soddisfatta da $u = z$ ma non da $u = 0$, dunque il minimo $u + 1$ che soddisfa $\neg\varphi(u + 1)$ ha un precedente che verifica $\varphi(u)$. Sia x tale che verifica $\overline{2}x = \overline{2}z - u(u + \overline{1})$, che esiste per le regole sulla parità. Osserviamo che tali valori u e x sono unici perché moltiplicare per $\overline{2}$ è una funzione strettamente crescente. Deve verificarsi che $x \leq u$, altrimenti avremmo $\overline{2}u < \overline{2}x$ quindi $\overline{2}u < \overline{2}z - u(u + \overline{1})$, da cui $u^2 + \overline{3}u < \overline{2}z$, e dato che $u^2 + \overline{3}u$ è pari, si ha $(u + \overline{1})(u + \overline{2}) = u^2 + \overline{3}u + 2 \leq \overline{2}z$, una contraddizione. Allora definiamo $y = u - x$ e si verifica che $z = (x, y)$. Se $z = (x', y')$ allora, chiamato $u' = x' + y'$ si ha che $\varphi(u') \wedge \neg\varphi(u' + 1)$, dunque per l'unicità di u, x e y segue $x = x'$ e $y = y'$. □

Principio di overspill

Definizione 2.16. Dato un modello M di OI, diciamo che un suo sottoinsieme non vuoto C è un *taglio (cut)* se è chiuso per la funzione successore e se è un segmento iniziale, cioè se vale $(a \in C \to S(a) \in C) \wedge (a \in C \wedge b < a \to b \in C)$. Diciamo che C è un taglio proprio se è un sottoinsieme proprio di M. Si parla di *taglio definito (defined cut)* se C è definito da una formula.

Il prossimo risultato, molto importante per dimostrare il teorema di Tennenbaum, è utile e notevole abbastanza da meritare un nome: *overspill*.

Teorema 2.17 (Overspill)**.** Sia $\varphi(x)$ di classe Δ_0, sia M un modello nonstandard di $I\Delta_0$ e sia C un taglio proprio di M. Se $C \subset \varphi(M)$ allora esiste $b \in M$ maggiorante di C tale che $M \vDash \varphi(b)$.

Osservazione 2.18. Nelle ipotesi del teorema si ha che esiste $b \in M$ maggiorante di C tale che $M \vDash (\forall x \leq b)(\varphi(x))$, ciò segue applicando il teorema alla formula $\psi(y) \equiv (\forall x \leq y)(\varphi(x))$, che è ancora di classe Δ_0.

Osservazione 2.19. Sia $\varphi(x)$ una formula di classe Δ_0 che non abbia variabili libere all'infuori di x, sia M un modello nonstandard di $I\Delta_0$. Se $\mathbb{N}$ soddisfa $\varphi(n)$ per ogni $n \in \mathbb{N}$ allora esiste $b \in M$ non standard tale per cui M soddisfa $(\forall x \leq b)(\varphi(x))$. Infatti, chiamato C il taglio di M isomorfo a $\mathbb{N}$, si ha che per ogni $a \in C$ esiste un numero naturale n tale che $M \vDash a = \bar{n}$. Poiché la formula $\varphi(\bar{n})$ in Q è chiusa ed è soddisfatta da $\mathbb{N}$, deve essere soddisfatta anche da Q e dunque anche da M che ne è un modello, dunque possiamo applicare il teorema di overspill.

Dimostrazione di 2.17. Assumiamo per assurdo che nessun maggiorante di M soddisfi $\varphi(x)$ e procediamo a dimostrare che M soddisfa $(\forall y)(\psi(y))$, dato che C è proprio raggiungiamo così un assurdo. Dimostriamo quanto detto sfruttando gli assiomi di induzione in x di $\varphi(x)$.

Per ipotesi M soddisfa $\varphi(0)$ (C è non vuoto).

Prendiamo un generico $a \in M$ e assumiamo l'ipotesi induttiva per $x = a$: se a appartiene a C allora anche $S(a)$ appartiene a C da cui si ottiene $M \vDash \varphi(S(a))$ e in particolare vale $M \vDash \varphi(a) \to \varphi(S(a))$. Se invece a è un maggiorante di C allora anche $S(a)$ lo è e per l'assunzione fatta si ha $\neg M \vDash \varphi(a)$ e in particolare $M \vDash \varphi(a) \to \varphi(S(a))$. Dato che a è generico abbiamo ottenuto $M \vDash (\forall y)(\varphi(y) \to \varphi(S(y)))$.

Unendo quanto detto abbiamo $M \vDash \varphi(0) \wedge (\forall y)(\varphi(y) \to \varphi(S(y)))$ da cui otteniamo la contraddizione cercata usando gli assiomi di induzione. □

Osservazione 2.20 (φ ammette parametri). Si osserva che teorema è valido anche per formule con parametri.

Osservazione 2.21 (Principio del minimo). Sempre sotto le ipotesi per cui M è modello nonstandard di $I\Delta_0$, data $\varphi(x)$ di classe Δ_0, consideriamo $X := \varphi(M)$. Dal teorema di overspill discende che se X non è vuoto allora ammette minimo. Per mostrarlo consideriamo il segmento iniziale C costituito da tutti gli $a \in M$ che soddisfano la formula di classe Δ_0 seguente: $(\forall x \leq a)\neg\varphi(x)$. Se C non è un taglio allora ammette massimo, il cui successore è il minimo di X. Se invece C fosse un taglio allora non può essere proprio, cioè $C = M$, altrimenti per overspill otterremo una contraddizione, dunque in questo caso X deve essere vuoto.
Viceversa, se per una classe di formule chiuse per negazione vale il principio del minimo allora per quelle formule vale anche il principio di induzione. Supponiamo valga il principio del minimo per $\neg\varphi(x)$, supponiamo valgano le premesse della formula di induzione per $\varphi(x)$ e dimostriamo che $\varphi(x)$ valga per ogni x. Supponiamo per assurdo che non valga $(\forall x)(\varphi(x))$, allora $\neg\varphi[M]$ non è vuoto e ammette minimo $a \in M$ diverso da 0 perché per il passo base $\varphi(0)$ è soddisfatto. Allora a ha un predecessore b che verifica $\varphi(b) \wedge \neg\varphi(S(b))$, assurdo.

Osservazione 2.22. Il teorema di overspill e il principio del minimo si possono applicare anche a OI, ad esempio se M è un modello di OI e φ non è quantificata allora $\varphi[M]$ ammette minimo. La dimostrazione è esattamente la stessa.

2.2 Elevamento a potenza in $I\Delta_0$

In questa sezione mostriamo alcune costruzioni basilari che si possono eseguire in $I\Delta_0$, in particolare svilupperemo la teoria delle liste e daremo una definizione di elevamento a potenza [HP98, Pagine 295-303]. Per dimostrare il teorema di Tennenbaum nella generalità raggiunta da McAloon, serve avere una relazione ternaria che goda delle proprietà di cui gode l'elevamento a potenza in $\mathbb{N}$. Per ottenerla, potremmo aggiungere al linguaggio la relazione $x^y = z$, e aggiungere i relativi assiomi, i quali garantirebbero

quanto vogliamo; tuttavia, al fine di non indebolire le ipotesi del teorema di Tennenbaum, vorremmo essere in grado di definire tale relazione usando il linguaggio e gli assiomi di $I\Delta_0$. Inoltre, poiché possiamo usare l'induzione solo sulle formule di classe Δ_0, è conveniente definire l'elevamento a potenza usando una formula di tale classe. In generale $I\Delta_0$ non può ottenere che l'elevamento a potenza sia totale (ovvero che sia definito su tutti i valori). Tuttavia per molti risultati è sufficiente definire una relazione parziale purché si possano fare le potenze di numeri standard, così che per overspill si possano fare potenze anche di alcuni valori nonstandard sufficientemenți piccoli. Per raggiungere questo scopo dobbiamo sviluppare prima un po' di teoria delle liste. Iniziamo con un risultato che permette di "ingrandire" la classe delle formule sulle quali abbiamo a disposizione l'induzione.

Per la definizione data nel capitolo 0, permettiamo solo variabili come limiti ai quantificatori. Sia f il simbolo per una funzione unaria. Espandiamo il nostro linguaggio L aggiungendo f e che denotiamo con $\Delta_0^f(f)$ l'insieme delle formule limitate in cui ammettiamo come limiti ai quantificatori qualunque termine del linguaggio espanso $L(f)$. Consideriamo le due seguenti teorie:

$$I\Delta_0^f(f) + f \text{ è crescente},$$
$$I\Delta_0(f) + f \text{ è crescente}.$$

Nel primo caso estendiamo lo schema di induzione alle formule $\Delta_0^f(f)$, nel secondo permettiamo l'induzione solo per le formule limitate di $L(f)$ in cui ammettiamo come limiti ai quantificatori solamente variabili.

Lemma 2.23. [HP98, pagina 271] Le teorie $T_1 := I\Delta_0^f(f) + "f \text{ è crescente}"$, e $T_2 := I\Delta_0(f) + "f \text{ è crescente}"$ sono equivalenti.

Dimostrazione. È sufficiente che T_2 dimostri che valga il principio del minimo per ogni formula $\Delta_0^f(f)$.
Dimostriamo dapprima che per ogni formula $\varphi(X) \in \Delta_0^f(f)$ esiste $\varphi_0(X, y) \in \Delta_0(f)$ e un $L(f)$-termine $t(X)$ tale che

$$(\diamondsuit) \qquad T_2 \vdash (\forall y \geq t(X))(\varphi(X) \leftrightarrow \varphi_0(X, y)),$$

dove $X = x_1, \ldots, x_n$ con $y \neq x_i$. Lo dimostriamo per induzione sulla complessità della formula φ. Se φ è atomica non c'è niente da dimostrare. Assumiamo ora che $(\diamondsuit)$ valga per $\varphi(X_1)$, $\varphi_0(X_1, y_1)$, $t(X_1)$ e per $\psi(X_2)$, $\psi(X_2, y_2)$, $s(X_2)$ e svolgiamo i passi induttivi. A meno di cambiare il nome alle variabili y e ingrandire X possiamo assumere che $X_1 = X_2 = X$ e $y_1 = y_2 = y$. Per ogni $L(f)$-termine $r(X)$ e per ogni $j \in \mathbb{N}$, si verifica che vale

$$T_2 \vdash (\forall y \geq t(X))(\neg\varphi(X) \leftrightarrow \neg\varphi_0(X, y)),$$
$$T_2 \vdash (\forall y \geq t(X) + s(X))(\varphi(X) \wedge \psi(X) \leftrightarrow \varphi_0(X, y) \wedge \psi_0(X, y)),$$
$$T_2 \vdash (\forall y \geq t(X) + r(X))((\forall x_j \leq r(X))(\varphi(X)) \leftrightarrow (\forall x_j \leq y)(x_j \leq r(X) \rightarrow \varphi(X, y))).$$

Osserviamo che, dato che "f è crescente " $\in T_i$, dato che $+$ e $*$ sono monotone in OI e quindi in T_i, ogni $L(f)$-termine è crescente in ogni variabile, ciò è facilmente verificabile per induzione sulla complessità dei termini. Completiamo ora la dimostrazione del lemma, prendiamo $\varphi(X)$, $\varphi_0(X, y)$, $t(X)$ per cui valga $(\diamondsuit)$ e verifichiamo che T_2 dimostra il principio del minimo su x_1 per $\varphi(X)$. Supponiamo esista $X = x_1, \ldots, x_n$ che verifica $\varphi(X)$ allora, ponendo $y = t(X)$, deve seguire $\varphi_0(X, y)$. Sia ora x_1' il minimo x_1 che verifica $\varphi(X, y)$, che esiste perché T_2 contiene l'induzione per φ_0. Chiamiamo $X' = x_1', \ldots, x_n$. Dato che $t(X') \leq t(X)$ anche $\varphi(X')$ è soddisfatta, verifichiamo che x_1' è minimo anche per φ. Se per assurdo esistesse $x_1'' < x_1$ che, chiamato $X'' = x_1'', \ldots, x_n$, verificasse $\varphi(X'')$ allora si avrebbe $\varphi_0(X'', y')$ per ogni $y' \geq t(X'')$ e quindi anche $\varphi_0(X'', y)$ dato che $y = t(X) \geq t(X'')$ per monotonia di t, il che è assurdo per la scelta di x_1'. □

Teoria delle liste in $I\Delta_0$

Affrontiamo ora il problema delle liste. Per definire una lista di numeri ci serviremo della sua scrittura in base 2. Una lista è il dato di due numeri: il primo, in scrittura binaria, rappresenta la concatenazione di tutti gli elementi della lista (scritti in binario); il secondo, scritto in binario, sarà la codifica dei marcatori, rappresentati da degli uni, che determinano l'inizio e la fine di ciascuno dei numeri codificati. Ad esempio, per codificare la lista $(2, 3, 5)$ consideriamo da prima le scritture binarie dei suoi elementi: (10, 11, 101); dopo di ché determiniamo i numeri che rappresentano la lista:

$$10111101,$$
$$10101001.$$

Chiaramente anche la scrittura 0010 rappresenta 2 in binario, come la scrittura 00011 rappresenta 3, quindi, dato che una lista è prima di tutto una lista di stringhe di zeri e uni, anche la seguente coppia andrebbe bene per rappresentare $(2, 3, 5)$:

$$100011101,$$
$$100010001001.$$

Chiaramente i due zeri all'inizio della scrittura binaria del primo numero non li ho scritti in quanto inutili nel determinare il valore del numero stesso.

Il primo passo dunque è quello di definire mediante una formula Δ_0 la proprietà di essere una potenza di 2.

Definizione 2.24.

$$y \text{ è primo: } prime(y) \equiv 1 < y \wedge (\forall w \leq y)(w|y \to w = 1 \vee w = y)$$
$$x \text{ è una potenza di due: } pow(x) \equiv (\forall y \leq x)(prime(y) \wedge (y|x \to y) = \overline{2}) \wedge x \leq \overline{1}.$$

La teoria $I\Delta_0$ dimostra la seguente proprietà: $prime(x) \to (x|yz \to x|y \vee x|z)$. La dimostrazione del teorema fondamentale dell'aritmetica viene attribuita a Euclide, sebbene quest'ultimo abbia dimostrato solo la formula appena enunciata. Tale formula è infatti l'ingrediente fondamentale per dimostrare il teorema, almeno in $\mathbb{N}$ dove vale l'induzione al second'ordine. Tuttavia in un modello arbitrario di Δ_0 non vale necessariamente il teorema fondamentale dell'aritmetica, infatti, non è possibile dimostrare l'atomicità di un modello generico. Per altro, questa non è nemmeno una proprietà esprimibile al prim'ordine, infatti in ogni modello nonstandard elementarmente equivalenti a $\mathbb{N}$ non vale l'atomicità.

Lemma 2.25. La teoria $I\Delta_0$ dimostra che $prime(x) \to (\forall y, z \leq x)(x|yz \to x|y \vee x|z)$.

Dimostrazione. Supponiamo per assurdo che la tesi sia falsa, e prendiamo il più piccolo numero x che falsifica $prime(x) \to (\forall y, z \leq x)(x|yz \to x|y \vee x|z)$. Tale x deve soddisfare $prime(x)$. Prendiamo allora i più piccoli y, z che falsificano $(x|yz \to x|y \vee x|z)$, deve valere che $y, z < x$. Sia $xw = yz$. Se fosse $w = 1$, allora, poiché vale $prime(x)$, segue facilmente che $x|y \vee x|z$, e otterremmo un assurdo per come abbiamo scelto x, $y\, z$. Prendiamo w' il più piccolo divisore di w diverso da 1. Deve accadere che $w' \leq w < x$, altrimenti per monotonia della moltiplicazione, avremmo $yz < x^2 \leq xw$. Inoltre, per come abbiamo scelto w', si verifica facilmente che vale $prime(w')$. Perciò per ipotesi induttiva w' divide uno dei due fattori, diciamo senza perdita di generalità che divide $x = x'w'$. Chiamando $w'w'' = w$, deduciamo che $xw'' = x'y$, da cui troviamo una contraddizione per la minimalità di y, z. Dunque è stato assurdo supporre che esista x che falsifichi $prime(x) \to (\forall y, z \leq x)(x|yz \to x|y \vee x|z)$. □

Teorema 2.26. La teoria $I\Delta_0$ dimostra che $prime(x) \to (x|yz \to x|y \vee x|z)$.

Dimostrazione. Per divisione euclidea otteniamo $y = q_y x + y'$ e $z = q_z x + z'$. Se uno fra y', z' è zero, otteniamo la tesi. Invece, se per assurdo né y' né z' fossero 0, allora otterremmo che $prime(x) \to (x|yz \to x|y' \vee x|z')$ sarebbe falso; ma questo sarebbe assurdo poiché contraddirebbe il lemma precedente, infatti $y', z' < x$ in quanto sono resti della divisione euclidea. □

Usando questo teorema non è difficile dimostrare il seguente lemma.

Lemma 2.27. $I\Delta_0$ dimostra le seguenti formule:

(1) $$Pow(1),$$

(2) $$1 < x \wedge Pow(x) \leftrightarrow (\exists y \leq x)(x = \overline{2}y \wedge Pow(y)),$$

(3) $$Pow(x) \wedge Pow(y) \to Pow(xy) \wedge (x|y \vee y|x),$$

(4) $$Pow(x) \wedge Pow(y) \wedge (\overline{2}u + \overline{1})x = (\overline{2}v + \overline{1})y \to x = y,$$

(5) $$Pow(x) \wedge Pow(y) \wedge xz = y \to Pow(z),$$

(6) $$0 < x \to (\exists y)(x \leq y \leq \overline{2}x \wedge Pow(y)).$$

Questo lemma ci permette di definire:

Definizione 2.28. La più piccola potenza di 2 maggiore di x:

$$lpw(x) = y \quad \equiv \quad x \leq y \leq \overline{2}x + \overline{1} \wedge Pow(2) \wedge (\forall t \leq y)(x \leq t \wedge Pow(t) \rightarrow t = y).$$

Lemma 2.29. $I\Delta_0$ dimostra le seguenti formule:

(1) $$lpw(0) = 1,$$

(2) $$0 < x \rightarrow lpw(x) \leq \overline{2}x.$$

Adesso siamo pronti di dare la definizione di lista.

Definizione 2.30. Il valore x è la codifica di una lista ("sequence" in inglese):
$Seq(x) \equiv (\exists u, v \leq x)(x = (u, v) \wedge \neg\overline{2}|v \wedge lpw(u) \leq v)$

Non siamo al momento in grado di verificare quale sia l'i-esimo elemento di una lista, ma possiamo vedere se un dato elemento ci appartiene.

Definizione 2.31. $x \in (u, v) \equiv (\exists y, y' \leq v)(\exists u_1, v_1 < y)(\exists u_2, v_2 < v)(Pow(y) \wedge Pow(y') \wedge y' \geq \overline{2} \wedge x < y' \wedge u = u_2 y' y + xy + u_1 \wedge v = v_2 \overline{2} y' y + y' y + y + v_1)$

Ad esempio, supponiamo di volerci chiedere se $x = 100101 \in (u, v)$, ciò avviene se si verifica la seguente condizione:

$$u = * \cdots * 100101 * \cdots *$$
$$v = 1 * \cdots * 1000001 * \cdots *$$

Cerchiamo di esprimere questa condizione in termini aritmetici usando le quantità che compaiono nella definizione appena data:

$$u = \underbrace{\clubsuit \ldots \clubsuit}_{u_2} 100101 \underbrace{\spadesuit \ldots \spadesuit}_{u_1}$$
$$v = \underbrace{1\diamondsuit \ldots \diamondsuit}_{v_2} 1000001 \underbrace{\heartsuit \ldots \heartsuit}_{v_1}$$
$$y' = 1000000$$
$$y = 10 \ \ldots \ 0$$
$$y'y = 10000000 \ \ldots \ 0$$

Con questa notazione abbiamo:

$$\begin{aligned} u &= \clubsuit \ldots \clubsuit 100101 \spadesuit \ldots \spadesuit \\ u_2 y' y &= \clubsuit \ldots \clubsuit 0000000 \ \ldots 0 \\ xy &= 1001010 \ \ldots 0 \\ u_1 &= \spadesuit \ldots \spadesuit \\ u &= u_2 y' y + xy + u_1 \end{aligned}$$

$$\begin{aligned} v &= 1 \diamondsuit \ldots \diamondsuit 1000001 \heartsuit \ldots \heartsuit \\ v_2 \overline{2} y' y &= 1 \diamondsuit \ldots \diamondsuit 00000000 \ \ldots 0 \\ y' y + y &= 10000010 \ \ldots 0 \\ v_1 &= \heartsuit \ldots \heartsuit \\ v &= v_2 \overline{2} y' y + y' y + y + v_1 \end{aligned}$$

L'esplicazione appena fornita funziona anche al contrario, cioè dati y, y', u_1', u_2, v_1, v_2 che verificano quanto richiesto nella definizione, ripercorrendo al contrario quanto appena detto si può verificare che i numeri u, v rappresentano una lista in cui compare x.

Osservazione 2.32. Chiaramente è possibile esprimersi su una lista riferendosi ad essa usando un'unica variabile invece che usandone due combinate assieme con la definizione di coppia, in quel caso dobbiamo adattare la definizione: $x \in z \equiv (\exists u, v \leq z)(z = (u, v) \wedge x \in (u, v))$.
Chiaramente diamo anche la seguente definizione $x \notin t \equiv \neg(x \in t)$.

Per poter usare efficacemente le liste dobbiamo mostrare che la lista vuota è codificabile e che data una lista possiamo creare una nuova lista aggiungendo un dato elemento a quella vecchia.

Lemma 2.33. $I\Delta_0$ dimostra che

(1) $$(\forall x)(x \notin (0, \overline{1}))$$

(2) $$(\forall p, z)(Seq(p) \rightarrow (\exists q \leq \overline{9} p (z + \overline{1})^2)(Seq(q) \wedge (\forall x)(x \in q \leftrightarrow x \in p \vee x = z)))$$

Data la quantità di variabili coinvolte in questo lemma ci permettiamo di usare qualunque lettera per indicare le variabili contraddicendo momentaneamente le convenzioni stabilite all'inizio, per altro non sono coinvolti modelli specifici dunque non corriamo rischi di confusione.

Dimostrazione. (1) è ovvio. Dimostriamo (2). Assumiamo $Seq(p)$. Sia $p = (u, v)$ e sia $k = max\{\overline{2}, lpw(z)\}$. Definiamo subito q:

$$\begin{aligned} u' &= uk + z \\ v' &= vk + 1 \\ q &= (u', v') \end{aligned}$$

Sui numeri standard la definizione funziona, infatti v termina con un uno per definizione di $Seq(p)$:

$$\begin{aligned} z &= \clubsuit \ldots \clubsuit \\ k &= 10 \ \ldots \ 0 \\ u' = uk + z &= \underbrace{\spadesuit \ldots \spadesuit}_{u} \clubsuit \ldots \clubsuit \\ v' = vk + 1 &= \underbrace{\diamondsuit \ldots \diamondsuit}_{v} 10 \ \ldots \ 1 \end{aligned}$$

Dobbiamo dimostrarlo in $I\Delta_0$. Innanzi tutto verifichiamo che q rispetti le limitazioni imposte e che sia una lista.

Supponiamo $u \neq 0$. Si ha

$$\begin{aligned} u' \leq \overline{2}u(z+1) + z \leq \overline{3}u(z+1) \\ v' \leq \overline{2}v(z+1) + 1 \leq \overline{3}v(z+1) \end{aligned}$$

Dunque

$$\begin{aligned} \overline{2}q = \overline{2}(u', v') = (u' + v' + 1)(u' + v') + \overline{2}u' = \\ = (u' + v')^2 + (u' + v') + \overline{2}u' = \\ \leq \overline{9}(z+\overline{1})^2(u+v)^2 + \overline{3}(z+\overline{1})(u+v) + \overline{6}(z+\overline{1})u = \\ \leq \overline{9}(z+\overline{1})^2(u+v)^2 + \overline{9}(z+\overline{1})^2(u+v)(z+\overline{1}) + \overline{9}(z+\overline{1})^2 * \overline{2}u = \\ = \overline{9}(z+\overline{1})^2((u+v)^2 + (u+v) + \overline{2}u) = \\ = \overline{9}(z+\overline{1})^2(u, v) = \overline{9}(z+\overline{1})^2 p \end{aligned}$$

Se $u = 0$ allora $k \leq \overline{2}z + \overline{1}$, $p = (v+1)v$ e quindi, ricordando che $v \leq 1$,

$$\begin{aligned} \overline{2}q = \overline{2}(u', v') = (u' + v' + 1)(u' + v') + \overline{2}u' = \\ \leq (z + (\overline{2}z + \overline{1})v + \overline{2})(z + (\overline{2}z + \overline{1})v + \overline{1}) + \overline{2}z = \\ = \overline{4}z^2v^2 + \overline{4}z^2v + \overline{4}zv^2 + z^2 + \overline{8}zv + v^2 + \overline{5}z + \overline{3}v + \overline{2} = \\ \leq \overline{4}z^2v^2 + \overline{4}z^2v + \overline{4}zv^2 + z^2v + \overline{8}zv + v^2 + \overline{5}zv + \overline{3}v + \overline{2}v = \\ \leq \overline{9}(z+\overline{1})^2(v+1)v = \overline{9}(z+\overline{1})p. \end{aligned}$$

Abbiamo provato che q è il doppio più piccolo del suo limite. Vediamo che è una lista. v' è ovviamente dispari, rimane da provare $lpw(u') \leq v'$. Ricordiamo che $u < lpw(u)$, $z < lpw(z) = k$ e che $lpw(u) \leq v$ per l'assunzione $Seq(p)$. Dunque si ha

$$\begin{aligned} u' < uk + k \leq lpw(u)k \\ lpw(u') \leq lpw(u)k' < v' \end{aligned} \tag{1}$$

Dove in (1) abbiamo usato che prodotto di potenze di due è potenza di due.

Per mostrare che $x \in q$ è sufficiente porre $y = 1$, $y' = k$, $v_1 = u_1 = 0$, dopodiché la verifica segue immediatamente.

Supponiamo ora che $x \in p$ e dimostriamo che $x \in q$. Siano y, y', u_1, u_2, v_1, v_2 i testimoni di $x \in p$.

$$u' = u_2 y' yk + xyk + u_1 k + z$$
$$v' = v_2 \overline{2} y' yk + xyk + v_1 k + 1$$

Dunque i testimoni di $x \in q$ sono

$$yk \quad y' \quad u_1 k + z \quad u_2 \quad v_1 k + \overline{1} \quad v_2$$

È necessario dimostrare

$$u_1 k + z < yk$$
$$v_1 k + 1 < yk$$

Queste disuguaglianze seguono da

$$u_1 k + z < (u_1 + 1)k \leq yk$$
$$v_1 k + 1 < (v_1 + 1)k \leq yk$$

Assumiamo adesso che $x \in q$, vogliamo dimostrare che $x \in p$ o che $x = z$. Siano y, y', u_1, u_2, v_1, v_2 i testimoni di $x \in q$. Si ha dunque

$$v' = vk + 1 = \overline{2} y' y v_2 + y + v_1$$
$$u' = uk + z = y' y u_2 + xy + u_1$$

Esaminiamo prima il caso $v_1' = 0$, ci aspettiamo che $x = z$. Dato che v' è dispari deve esserlo anche y, e poiché vale $Pow(y)$ per ipotesi, per 2.27(2), deve valere anche $y = 1$. Per questo ci aspettiamo $x = z$, perché "$log_2(y)$" rappresenta il numero di cifre a sinistra di "x". Dunque si ha

$$vk = v' - 1 = \overline{2} v_2 y' + y' = (\overline{2} v_2 + 1) y',$$

e poiché v è dispari, si deve avere $k = y'$ per 2.27(4). Inoltre si ha $u_1 = 0$, poiché vale $u_1 < y = 1$, e da questo si ha

$$uk + z = u' = u_2 y' + xy + u_1 = u_2 k + x.$$

Dato che $x < y = k$ e $z < k$ si ha $x = z$ per unicità del resto.

Affrontiamo ora il caso $0 < v_1$, ci aspettiamo $x \in p$ poiché in questo caso varrà $1 < y$. Vale che

$$vk = v' - 1 = (v_2 \overline{2} y' + y' + 1) y + v_1 - 1$$

Se per assurdo avessimo $y|k$, sostituendo qua sopra otterremmo $y|v_1-1$, il che contraddice l'ipotesi di $x \in q$ per cui $v_1 < y$. Dato che $y \not| k$, poiché sia k sia y sono potenze di due, allora si ha $k|y$ per 2.27(3). Dunque otteniamo che $k|v_1 - 1$ perciò

$$v = v_2\overline{2}y'(y/k) + y'(y/k) + y/k + (v_1 - 1)/k. \tag{1}$$

Analogamente abbiamo

$$uk = u_2\overline{2}y'y + xy + u_1 - z$$

Ora, se per assurdo avessimo $u_1 < z$ seguirebbe

$$uk = (u_2\overline{2}y' + x)y - (z - u_1)$$

e poiché $k|y$ seguirebbe $k|z-u_1$ ma $z-u_1 \leq z < k$. Allora $k|u_1-z$ e possiamo scrivere

$$u = u_2\overline{2}y'(y/k) + x(y/k) + (u_1 - z)/k. \tag{2}$$

Da (1) e (2) si ricavano i testimoni di $x \in p$; le condizioni sulle limitazioni dei testimoni seguono immediatamente dalle stesse condizioni che abbiamo per ipotesi sui testimoni di $x \in q$, e per finire y/k è una potenza di due per 2.27(5). □

Relazione di elevamento a potenza

Il nostro scopo è definire $Exp(x, y, z)$ mediante una formula Δ_0 e dimostrare che in $I\Delta_0$ valgono le formule seguenti:

$$Exp(x, 0, z) \leftrightarrow z = \overline{1}, \tag{C1}$$

$$Exp(x, y + 1, z) \leftrightarrow (\exists v)(Exp(x, y, v) \wedge z = xv). \tag{C2}$$

Prima di iniziare la costruzione della formula vediamo che C1 e C2 implicano alcune proprietà.

Lemma 2.34. Se Exp rispetta C1 e C2, allora $I\Delta_0$ dimostra le seguenti formule:

$$Exp(\overline{m}, \overline{n}, \overline{k}) \iff m^n = k \quad \forall m, n, k \in \mathbb{N}, \tag{1}$$

$$Exp(x, y, u) \wedge Exp(x, y, v) \to u = v, \tag{2}$$

$$Exp(x, y, z) \wedge y' \leq y \to (\exists z' \leq z)(Exp(x, y', z')). \tag{3}$$

Dimostrazione. (1) C1 e C2 corrispondono alla definizione ricorsiva di elevamento a potenza in $\mathbb{N}$, dunque, in qualunque modello, restringendo Exp al segmento standard, per il teorema di ricorsione numerabile otteniamo lo stesso grafico dell'elevamento a potenza standard.

(2) La formula da dimostrare è equivalente a $(\forall u, v \leq z)(Exp(x, y, u) \wedge Exp(x, y, v) \to u = v)$. Per quest'ultima formula possiamo portare avanti una facile induzione su y.

(3) Simile al caso precedente □

L'idea più immediata per definire $Exp(x, y, z)$ prevede di costruire una lista che contenga tutte le prime y potenze di x così da testimoniare che "$x^y = z$", il problema è che tale lista cresce in modo non polinomiale rispetto a x, y, z, quindi troppo velocemente per essere definita da una formula $I\Delta_0$. Per ovviare al problema dovremmo costruire una lista simile ma più corta, per fare questo definiamo la formula $Exseq$.

Definizione 2.35.

$$\begin{aligned} Exseq(x, w) \equiv\ & Seq(w) \\ & \wedge (\overline{1}, 0) \in w \\ & \wedge (\forall y, z \leq w)[(z, y) \in w \to ((z, y) = (\overline{1}, 0) \\ & \qquad \vee (0 < y \wedge (\exists u, v \leq w)(y = 2v \wedge z = u^2 \wedge (u, v) \in w) \\ & \qquad \vee (0 < y \wedge (\exists u, v \leq w)(y = 2v + \overline{1} \wedge z = u^2 * x \wedge (u, v) \in w)))]. \end{aligned}$$

Lemma 2.36. $I\Delta_0$ dimostra che

$$\overline{2} \leq x \wedge Exseq(x, s) \wedge (z, y) \in s \to (z, y) \leq \overline{4}z^2.$$

Dimostrazione. Una facile induzione su y dimostra che $y < z$ e $\overline{1} \leq z$. Dopo di che un facile conto mostra

$$(z, y) \leq (z, z) \leq \overline{4}z^2.$$

□

Affinché la definizione di esponenziale sia Δ_0, è necessario che i testimoni di "$x^y = z$" siano limitati polinomialmente da x, y, z (quindi da z che è il più grande), perciò è utile dimostrare che ogni elemento (z, y) di una $Exseq(x, u)$ è elemento anche di un'altra $Exseq(x, v)$ limitata polinomialmente da z.

Lemma 2.37. $I\Delta_0$ dimostra che

$$(\forall x, u)(\forall z, y \leq u)(\exists v \leq \overline{30}z^{16})((\overline{2} \leq x \wedge Exseq(x, u) \wedge (z, y) \in u) \to (Exseq(x, v) \wedge (z, y) \in v)).$$

Dimostrazione. Servirà la seguente disuguaglianza di facile dimostrazione:

$$(\star) \qquad z^{16} \geq \overline{9}(\overline{4}z^4 + 1)^2 \qquad \text{per } z \geq 2.$$

Svolgiamo ora la dimostrazione per induzione su y con x e u come parametri. Se $y = 0$ allora $z = 1$ e la lista v che contiene l'unico elemento $(\overline{1}, 0)$ verifica $v = \overline{30} \leq \overline{30}z$ e soddisfa quanto richiesto. Sia ora $y > 0$ e quindi, come si verifica con una facile induzione su y, vale $z \geq x \geq 2$. Per l'ipotesi $Exseq(x, u)$, si ricade in uno dei seguenti casi:

$$\text{(i)} \qquad z = (z')^2 \quad y = \overline{2}y',$$

$$\text{(ii)} \qquad z = (z')^2 x \quad y = \overline{2}y' + \overline{1}.$$

Per ipotesi induttiva abbiamo un qualche v' per z', y'. Per il lemma 2.33 possiamo estendere v' a v in modo tale che valga

$$v \leq \overline{9}v'((z,y)+\overline{1})^2 \leq \overline{9}(\overline{30}(z')^{16})(\overline{4}z^2+\overline{1})^2$$

Dove abbiamo usato l'ipotesi induttiva per la maggiorazione di v' e il lemma precedente per quella di (z,y).

Chiaramente v soddisfa $Exseq(x,v)$ e $(z,y) \in v$, rimangono da dimostrare le disuguaglianze. Distinguiamo i due casi e usiamo $(\star)$:

(i) $$v \leq (\overline{30}(z')^{16})\overline{9}(\overline{4}(z')^4+\overline{1})^2 \leq \overline{30}(z')^{32} = \overline{30}z^{16}$$

(ii) $$v \leq (\overline{30}(z')^{16})\overline{9}(\overline{4}(z'x)^4+\overline{1})^2 \leq \overline{30}(z')^{32}x^{16} = \overline{30}z^{16}$$

□

Ora siamo pronti per definire l'esponenziazione.

Definizione 2.38. $Exp(x,y,z) \equiv (z = 1 \wedge y = 0) \vee (x \leq \overline{1} \wedge x = z \wedge y > 0) \vee (\exists u \leq \overline{30}z^{16})(Exseq(x,u) \wedge (z,y) \in u)$

Per poter usare l'induzione abbiamo avuto bisogno di imporre che la lista u sia limitata da $\overline{30}z^{16}$, ma per il lemma appena dimostrato questa limitazione è irrilevante. Per verificare che Exp soddisfi le condizioni richieste dobbiamo prima verificare alcuni risultati intermedi.

Lemma 2.39. $I\Delta_0$ dimostra le seguenti formule:

(C3) $$Exp(x,y,z) \to Exp(x,\overline{2}y,z^2) \wedge Exp(x,\overline{2}y+\overline{1},z^2x),$$

(C4) $$Exp(x,\overline{2}y,z) \to (\exists v)(v^2 = z \wedge Exp(x,y,z)),$$

(C5) $$Exp(x,\overline{2}y+\overline{1},z) \to (\exists v)(v^2x = z \wedge Exp(x,y,z)).$$

Dimostrazione. (C3) La tesi è banale per $x \leq \overline{1}$ e $y = 0$. Supponiamo $x > \overline{1}$, $y > 0$ e $Exp(x,y,z)$. Sia u la lista di potenze di x che testimonia $Exp(x,y,z)$, consideriamo le liste u_1, u_2 ottenute aggiungendo rispettivamente $(z^2,\overline{2}y)$ e $(z^2x,\overline{2}y)$ a u usando il lemma 2.33. Le liste u_1 e u_2 verificano $Exseq(x,u_i)$ e risultano essere limitate da $\overline{30}z^{16}$, in ogni caso possiamo assumere che siano limitate in tale modo ricorrendo al lemma 2.37.

(C4)-(C5) Si dimostrano in modo analogo. Assumiamo $x > \overline{1}$, $y > 0$ e consideriamo u la lista delle potenze che testimonia $Exp(x,y',z)$ con $y' = \overline{2}y$ (o $y' = \overline{2}y+\overline{1}$, a seconda di quale punto stiamo dimostrando). Dopodiché, dato che ogni numero è esclusivamente o pari o dispari, per definizione di $Exseq(x,u)$ si deve verificare che esiste v che soddisfa $(v,y) \in u$ e $v^2 = z$ (0 $v^2x = z$), infine concludiamo per il lemma 2.37. □

Lemma 2.40. $I\Delta_0$ dimostra che $Exp(x, y + \overline{1}, z) \leftrightarrow (\exists v \leq z)(Exp(x, y, v) \wedge z = vx)$.

Osserviamo che questo lemma è equivalente a C2. Infatti, con questo lemma ripercorrendo la dimostrazione fornita si può dimostrare il lemma 1(2) con il quale si può facilmente dimostrare l'equivalenza.

Dimostrazione. Supponiamo per assurdo che esistano degli x, y, z che contraddicono la tesi, per induzione sulle Δ_0 possiamo porre y e z tali che per ogni $y' < y$ e $z' < z$ la tesi risulta vera. Dividiamo due casi:

(1) $y = \overline{2}u$ è pari. Per C3 e C5 si ha che $I\Delta_0$ dimostra che

$$Exp(x, y + \overline{1}, z) \leftrightarrow (\exists w \leq z)(w^2 x = z \wedge Exp(x, u, w)) \leftrightarrow \quad (\exists w \leq z)(w^2 x = z \wedge Exp(x, y, w^2))$$

scegliendo $v = w^2$ otteniamo l'assurdo.

(2) $y = \overline{2}u + \overline{1}$ è dispari. Similmente otteniamo

$$\begin{aligned} Exp(x, y + \overline{1}, z) \leftrightarrow & Exp(x, (\overline{2}(u + \overline{1}), z) \\ & \overset{(a)}{\leftrightarrow} (\exists w \leq z)(w^2 = z \wedge Exp(x, u + \overline{1}, w)) \\ & \overset{(b)}{\leftrightarrow} (\exists w,\, w' \leq z)(w' x = w \wedge Exp(x, u, w')) \end{aligned}$$

Dove (a) segue per ipotesi induttiva e (b) segua da C3. Scegliendo $v = w'^2 x$ otteniamo l'assurdo. □

Teorema 2.41. Le proposizioni C1 e C2 sono dimostrabili in $I\Delta_0$ per la formula Exp di definizione 2.38.

Da C1 e C2 si possono dimostrare in $I\Delta_0$ altre proprietà naturali dell'elevamento a potenza, come, ad esempio:

$$\begin{aligned} & Exp(x, y_1, z_1) \wedge Exp(x, y_2, z_2) \rightarrow Exp(x, y_1 + y_2, z_1 + z_2), \\ & Exp(x, y_1, z) \wedge Exp(z, y_2, w) \rightarrow Exp(x, y_1 y_2, w), \\ & Pow(z) \rightarrow (\exists y)(Exp(\overline{2}, y, z)). \end{aligned}$$

Per definire l'elevamento a potenza in un qualunque modello di $I\Delta_0$, per prima cosa abbiamo preso una formula in tre variabili libere che, interpretata su $\mathbb{N}$, è soddisfatta da tutte e sole le triple n, m, o legate dalla relazione $n^m = o$; infine abbiamo definito l'elevamento usando tale formula. È naturale chiedersi se scegliendo una formula diversa sia possibile ottenere definizione non equivalente a quella data, in altre parole vorremo sapere se esistono vari modi per estendere l'esponenziazione ai numeri nonstandard. Questa domanda trova una risposta negativa qualora la formula usata sia di classe Δ_0 e si imponga che una relazione di esponenziazione debba rispettare alcune condizioni minime, come, ad esempio, C1 e C2.

Teorema 2.42. Sia E un simbolo per una relazione ternaria, e sia $I\Delta_0(E)$ la teoria $I\Delta_0$ con gli assiomi di induzione estesi alle formule limitate contenenti il simbolo E e con i seguenti assiomi addizionali:

(C1') $\quad E(x, 0, z) \leftrightarrow z = 1,$

(C2') $\quad E(x, y + \overline{1}, z) \leftrightarrow (\exists v)(E(x, y, v) \wedge z = vx).$

Allora la teoria $I\Delta_0(E)$ dimostra che $E(x, y, z) \leftrightarrow Exp(x, y, z)$.

Dimostrazione. Segue dimostrando in $I\Delta_0(E)$ per induzione su y la seguente formula $(\forall z \leq u)(E(x, y, z) \leftrightarrow Exp(x, y, z))$, la quale si dimostra usando C1, C2, C1', C2'. □

Osservazione 2.43. Il teorema dimostrato è abbastanza generale. Infatti, al posto di chiedere che la formula che definisce E sia di classe Δ_0 è sufficiente che valga l'induzione sulle formule limitate di che contengono E, la quale richiesta, sebbene sia abbastanza forte, è ragionevole dato che si mira a costruire E in modo tale che sia una relazione elementare (cioè già presente nel linguaggio). Inoltre, da questo teorema consegue che qualunque formula dimostrabile a partire da Exp segue da C1 e C2, a prescindere dalla definizione effettiva che abbiamo dato per Exp.

2.3 Codifiche di insiemi e teorema di Tennenbaum

Codifiche di insiemi

L'esistenza di insiemi inseparabili, che abbiamo dato nei preliminari, è di fondamentale importanza per la dimostrazione di Tennenbaum. Infatti tale dimostrazione si basa sulla possibilità di utilizzare un eventuale modello ricorsivo nonstandard per separare due insiemi inseparabili, cioè per rendere decidibile un insieme che non lo è. Per calcolare un sottoinsieme di $\mathbb{N}$ usando un modello nonstandard M, dobbiamo introdurre il concetto di codifica di un insieme.

Supponiamo di avere un modello M e un suo sottoinsieme A. Se A è limitato (esiste $a \in M$ che è un maggiorante di A) non è detto che sia finito, come invece accade in $\mathbb{N}$, dove limitatezza e finitezza sono equivalenti; però sarebbe piacevole che alcune caratteristiche degli insiemi finiti di $\mathbb{N}$ si mantengano vere anche negli insiemi limitati in M, nello specifico vorremmo che gli insiemi limitati siano codificabili mediante un elemento di M. Per codifica di A intendiamo un elemento $c \in M$ tale per cui $a \in A \iff$ l'a-esimo primo (di M) divide c (in M). Per agevolare la lettura, preso $n \in \mathbb{N}$, indichiamo l'n-esimo numero primo con P_n. In realtà per i nostri scopi vorremmo solo codificare in M sottoinsiemi di $\mathbb{N}$, che possono essere visti come sottoinsiemi di M mediante l'unico embedding fra i due modelli; cioè più precisamente diciamo che $c \in M$ codifica $A \subset \mathbb{N}$ se vale che $n \in A \iff M \vDash \overline{P_n}|c$. Manca solo di definire i numeri primi per un modello arbitrario M, ma dato che per il nostro scopo avremo necessità di codificare solo insiemi di numeri standard basterà considerare una qualunque formula

che definisce i numeri primi standard. Ad esempio, per dire che p è l'n-esimo numero primo, potremmo dire che esiste una lista crescente di n numeri primi terminanti in p e che qualunque lista crescente di $n+1$ numeri primi non può terminare con p. Più precisamente consideriamo le seguenti formule:

$$\begin{aligned}
\pi_0'(z) \equiv & seq(z) \wedge (\forall x, y \leq z)((x,y) \in z \rightarrow prime(x) \vee x = 1) \wedge \\
& \wedge (\forall x, y, x', y' \leq z)((x,y) \in z \wedge (x',y') \in z \rightarrow (x < x' \leftrightarrow y < y')), \\
\pi_0(z) \equiv & \pi_0'(z) \wedge (\forall x, y \leq z)(\exists x', y' \leq z)(0 < y \wedge (x,y) \in z \rightarrow y' + 1 = y \wedge (x',y') \in z) \\
\pi_1(x,y,z) \equiv & \pi_0(z) \wedge (x,y) \in z, \\
\pi_2(x,y,z) \equiv & \pi_0(z) \rightarrow (\forall y' \leq y+1)((x,y') \in z \rightarrow y' \leq y), \\
\pi(x,y,w) \equiv & (\exists z \leq w)(\pi_1(x,y,z)) \wedge (\forall z \leq w)(\pi_2(x,y,w)).
\end{aligned}$$

La formula $\pi_0'(z)$ assicura che z è una lista numerata e crescente di numeri primi (z può contenere anche il numero 1); la formula $\pi_0(z)$ impedisce alla lista z di "saltare"; la formula $\pi_1(x,y,z)$ garantisce che x è primo e esistono $y-1$ numeri primi più piccoli di x (infatti lo "zeresimo numero primo che viene contato" è in realtà l'1); la formula $\pi_2(x,y,z)$ invece asserisce che z non testimonia l'esistenza di più di y numeri primi minori di x; infine, la formula $\pi(x,y,w)$ asserisce che, considerando tutti i testimoni (le liste z) più piccoli di w, si può dire che x è l'$y-$esimo primo. Ovviamente la proprietà di essere l'n-esimo numero primo (con n standard) è verificabile tramite una lista finita; per cui, se nel contesto di un dato modello attribuiamo a w un numero nonstandard a, allora la formula $\pi(x,y,a)$ assolve il suo scopo (almeno per x standard). Ovvero, per ogni b del modello considerato, per ogni $n \in \mathbb{N}$ si ha $\pi(b, \overline{n}, a) \iff b = \overline{P_n}$. È importante notare che la formula $\pi(x,y,w)$ è di classe Δ_0.

Lemma 2.44. Sia M un modello $I\Delta_0$, sia $\varphi(x)$ un formula di classe Δ_0, eventualmente con parametri. Chiamiamo $C \subset \mathbb{N}$ l'insieme che soddisfa $n \in C \iff M \vDash \varphi(\bar{n})$. Se M è nonstandard allora C è codificabile in M. Inoltre C ammette codifiche arbitrariamente piccole, purché nonstandard.

Dimostrazione. Prendiamo $a \in M$ un qualunque valore nonstandard e consideriamo le seguenti formule:

$$\begin{aligned}
\psi_0(y,z) &\equiv (\forall v \leq a)(\pi(v,y,a) \wedge v|z), \\
\psi(x) &\equiv (\exists z \leq a)(\varphi(y) \leftrightarrow \psi_0(y,z)).
\end{aligned}$$

Le formule elencate sono di classe Δ_0. Per ogni x standard, la formula $\psi_0(y,z)$ dice che l'y-esimo numero primo divide z, mentre la formula $\psi(x)$ asserisce l'esistenza di una codifica (rappresentata dalla variabile z) dei primi x valori di C. Per ogni $\bar{n}$ standard, la formula $\psi(\bar{n})$ è soddisfatta in M poiché asserisce l'esistenza di una codifica di un insieme finito di numeri standard; dunque per il teorema di overspill la formula $\psi(b)$ risulta verificata per un valore nonstandard $b \in M$. Per definizione di semantica di Tarski allora esiste $c \in M$ che verifica la condizione di essere una codifica per tutti i

valori di $\varphi[M]$ minori di b[2], in particolare per tutti i valori di C dato che b, essendo nonstandard, né è un maggiorante. Inoltre c deve essere minore di a, e per generalità di a, possiamo scegliere c arbitrariamente piccolo, purché nonstandard. □

Teorema di Tennenbaum

Richiamiamo adesso la definizione di modello ricorsivo.

Definizione 2.45. Sia $(M, 0_M, S, +, *, \leq, =)$ una $L-$struttura. M si dice ricorsivo se vale che $M \subset \mathbb{N}$ è un insieme decidibile e sia le funzioni $+$, $*$, $S : M \to M$ sia le relazioni $\leq$, $= \subset \mathbb{N}^2$ sono ricorsive. Se richiediamo che solo una delle operazioni sia ricorsiva, allora permettiamo all'altra di non esserlo, tuttavia continuiamo ad imporre che siano ricorsive la funzione successore e le relazioni $\leq$, $=$.

Osservazione 2.46. Osserviamo che se la funzione somma è ricorsiva, allora anche la funzione successore e la relazione $\leq$ lo sono. Infatti la funzione successore equivale a sommare uno, e la relazione $\leq$ può essere verificata facendo tutte le possibili somme (per entrambi gli argomenti), infatti (almeno in OI) la relazione $\leq$ è un ordine totale, quindi provando tutti le possibili somme si arriverebbe certamente a trovare la somma che verifica o falsifica l'istanza di $\leq$. Osserviamo però che non partendo dalla sola funzione prodotto ricorsiva non possiamo allo stesso modo rendere ricorsive anche la funzione successore e la relazione $\leq$.

Teorema 2.47 (Tennenbaum)**.** [HP98, Pagina 269] Sia M un modello di $I\Delta_0$. Se M è non standard allora non è ricorsivo, infatti nessuna delle operazioni $+_M$ e $*_M$ può essere computabile.

Dimostrazione. Siano A, $B \subset \mathbb{N}$ due insiemi inseparabili tali che

$$n \in A \iff \mathbb{N} \vDash (\exists x)(\varphi(x, n)),$$
$$n \in B \iff \mathbb{N} \vDash (\exists x)(\psi(x, n)),$$

con φ e ψ formule di classe Δ_0. Dato che A e B sono disgiunti $\mathbb{N}$ soddisfa $(\forall x, y)(\neg(\varphi(x, y) \wedge \psi(x, y)))$, dunque per overspill M soddisfa $(\forall x, y \leq a)(\neg(\varphi(x, y) \wedge \psi(x, y)))$ per un valore $a \in M$ nonstandard. Definiamo allora l'insieme $C \subset N$ tale che

$$n \in C \iff M \vDash (\forall x \leq a)(\varphi(x, \bar{n})).$$

Per il lemma 2.44 C ammette una codifica in M che indichiamo con c. Osserviamo che $A \subset C \subset \mathbb{N} \setminus B$. L'idea è quella di supporre per assurdo che una delle due operazioni di M sia calcolabile e dimostrare che la funzione caratteristica di C sarebbe

[2]Per poter parlare di codifica in modo coerente con quanto detto prima dovremo prima definire il concetto di numero primo per tutti i valori di M. Se poniamo come definizione di "x è l'y-esimo numero primo" la seguente formula $(\exists z \leq a)(\pi(x, y, z))$, allora si può parlare effettivamente di codifiche. Ovviamente, quando y è nonstandard, non abbiamo garanzie che questa definizione conferisca ai numeri primi le proprietà ragionevoli che ci aspettiamo, ma per i nostri fini è una definizione sufficiente, dato che ci basta concertarci sui numeri primi standard.

ricorsiva totale, il che equivale a costruire una funzione ricorsiva totale f tale che $f(n) = 0 \iff M \vDash \overline{P_n}|c$. Supponiamo che sia la funzione successore S, e dunque anche la funzione $n \mapsto \bar{n} \in M$, sia la relazione $\leq$ siano ricorsive. Osserviamo che la funzione primitiva ricorsiva $(n, m) \mapsto < n, m >:= n + (n + m + 1)(n + m)/2$ è una biezione fra $\mathbb{N}$ e $\mathbb{N}^2$.

Supponiamo che la somma sia ricorsiva. Chiaramente anche la seguente funzione è ricorsiva: $(n, b) \mapsto \underbrace{b +_M b +_M \cdots +_M b}_{n \text{ volte}} = b *_M \overline{n}$. Per chiarezza sottolineo che sia n sia b sono formalmente numeri naturali, ma nel contesto della scrittura in cui compaiono, stiamo guardando n come elemento della struttura $\mathbb{N}$ mentre b come elemento di M. Consideriamo la funzione f che preso in input n cerca b, $d \in M$ che soddisfano $b *_M \overline{P_n} +_M d = c \wedge d \leq \overline{P_n}$, e che restituisce 0 se $d = 0_M$, altrimenti 1. Dato che si possono enumerare ricorsivamente, la funzione f è ricorsiva. Inoltre per il lemma della divisione con resto b e d esistono e sono unici, dunque la funzione è totale. Dunque C è un insieme decidibile, assurdo.

Adesso supponiamo per assurdo che il prodotto $*_M$ sia ricorsivo. Fissiamo $b' \in M$ nonstandard e consideriamo $(\exists y \leq b')(Exp(2, x, y))$: per overspill su x troviamo un $b \in M$ nonstandard tale che $(\forall x \leq b)(\exists y \leq b')(Exp(2, x, y))$. Dato che le codifiche sono arbitrariamente piccole possiamo assumere che $c \leq b$, e dunque che esista il valore "2^c". Usiamo adesso una variante dello stesso argomento usato precedentemente. Costruiamo prima la funzione ricorsiva che mappa $(n, d) \mapsto \underbrace{d * d * \cdots * d}_{n \text{ volte}} = d^n$. Poi consideriamo la funzione che preso in input n cerca $d, e \in M$ che soddisfano $2^c = d^{P_n} * e \wedge e \leq d$, e che restituisce 0 se $e = 1_M$, altrimenti 1. Tale funzione è ricorsiva e per argomenti simili ai precedenti conduce alle stesse conclusioni. Infatti, presi f, g, resto e quoziente della divisione euclidea di c per P_n, dato che f, $g \leq c$, esistono unici $d = 2^f$ e $e = 2^g$, usando le proprietà delle potenze otteniamo che la procedura descritta si imbatte prima o poi in dei valori d, e che la fanno arrestare, dunque la funzione che rappresenta è ricorsiva totale. Inoltre, essendo 2^c una potenza di due, da $2^c = d *_M e$ segue che anche d, e sono potenze di due, perciò, usando l'unicità del resto e del quoziente della divisione euclidea e le proprietà della potenze, si ha che l'esito della procedura è corretto, cioè restituisce 0 se $n \in C$ e 1 altrimenti. Dunque C è un insieme decidibile, assurdo. □

Wilmers

Lavori più recenti hanno ridotto ulteriormente le ipotesi in cui continua a valere il teorema di Tennenbaum. Noi ci limiteremo ad enunciare il risultato di Wilmers, per farlo però abbiamo bisogno di introdurre una nuova classe di formule. Consideriamo l'insieme E_1 costituito dalle formule della forma $(\exists x_1 \leq y_1) \ldots (\exists x_n \leq y_n)(\varphi)$, dove φ è una formula aperta. In analogia con quanto fatto nel capitolo precedente, consideriamo il frammento dell'aritmetica IE_1 che contiene gli assiomi dell'aritmetica di Robinson

a cui vengono aggiunti gli assiomi di induzione per le formule aperte e per le formule di classe E_1. Nell'articolo Buonded existential induction [Wil85], Wilmers dimostra, usando un arogmento analogo a quello presentato in questa tesi, che non può esistere nemmeno un modello ricorsivo della teoria IE_1.

Capitolo 3

I modelli di Open Induction e un esempio computabile

Adesso il nostro scopo è quello di esibire un modello ricorsivo per la teoria OI. A questo obbiettivo è giunto Sheperdson nel 1964 con l'articolo "A Non-Standard Model for a Free Variable Fragment of Number Theory"[She64], nel quale ha caratterizzato tali modelli. Usando questa caratterizzazione è facilmente individuabile un modello ricorsivo. Per presentare il lavoro di Sheperdson conviene fare alcune riflessioni sulla natura di questi modelli e sul parallelismo fra questi e i numeri naturali. Così come dai numeri naturali possiamo costruire i numeri interi, i razionali e infine i reali, allo stesso modo a partire da un modello delle Open Induction possiamo costruire un anello e dei campi che sono delle versioni alternative di quelli già citati. Iniziamo adesso introducendo il concetto di campo reale chiuso, che serve per enunciare il risultato di Sheperdson.

3.1 Campi Reali Chiusi

Ciò che ci accompagnerà in questo studio, oltre alle operazioni algebriche, è l'ordine. Si consideri dunque il linguaggio degli anelli ordinati, che fortunatamente è lo stesso di quello dell'aritmetica, e si consideri la teoria dei campi ordinati. Ricordo che un campo ordinato è un campo dotato di una relazione d'ordine totale $\leq$ compatibile con le operazioni, cioè che soddisfa i seguenti assiomi:

$$0 \leq x \wedge 0 \leq y \rightarrow 0 \leq xy,$$
$$y \leq z \rightarrow y + x \leq z + x.$$

Da questi semplici assiomi si dimostra che si può moltiplicare entrambi i membri di una disequazione per un numero positivo (dove positivo significa maggiore di 0) senza cambiarne il valore di verità, mentre moltiplicando per un numero negativo (cioè minore di 0) dobbiamo scambiare i due membri. Si dimostra anche che per ogni x si ha

che $0 \leq x^2$ e che $0 \leq 1$.
Non tutti i campi ordinati sono elementarmente equivalenti, ad esempio in $\mathbb{R}$ ogni numero positivo ammette una radice quadrata mentre in $\mathbb{Q}$ no; quindi la teoria dei campi ordinati non è completa. Al fine di ottenere una teoria completa aggiungiamo alcuni assiomi veri in $\mathbb{R}$. Aggiungiamo in particolare l'assioma che dice che ogni numero positivo ammette una radice quadrata, e pure che ogni polinomio di grado dispari ammette una radice (serve un assioma per ogni grado dispari). Si può dimostrare, teorema di Tarski [TM51], che questa teoria ammette l'eliminazione dei quantificatori, cioè che per ogni formula φ esiste ψ senza quantificatori che soddisfa $\varphi \leftrightarrow \psi$ (in questa teoria). Dopodiché, dimostrando che ogni formula senza quantificatori è o dimostrabilmente vera o dimostrabilmente falsa, segue immediatamente che tale teoria è completa, e quindi che tutti i campi che soddisfano questi assiomi sono elementarmente equivalenti fra loro, e in particolare elementarmente equivalenti a $\mathbb{R}$. Pertanto tali campi si dicono *campi reali chiusi*, sebbene noi daremo un'altra definizione e dimostreremo solo lo stretto indispensabile per i nostri scopi.

Chiaramente un campo non tutti i campi sono ordinati; tuttavia non si esclude che possa esisterne un ordine che renda tale campo un campo ordinato. In tale caso si parla di campo *ordinabile* oppure di *campo formalmente reale*. A giustificazione di questo secondo nome vedremo che ogni campo formalmente reale è ottenibile come sottocampo di un campo reale chiuso e il suo ordine è la restrizione dell'ordine di tale campo reale chiuso. La teoria che sta alla base dei campi reali chiusi è troppo ampia per essere riportata qui interamente; pertanto daremo solo i fatti e le dimostrazioni principali e rimandiamo a [Pre84, capitoli 1-3] per approfondire la lettura sull'argomento.

Per iniziare sviluppiamo alcuni strumenti utili nello studio degli ordini sui campi e analizziamo la condizione che deve soddisfare un campo per essere ordinabile. Per costruire un ordine totale dobbiamo determinare P, l'insieme candidato dei valori non negativi, fatto questo è sufficiente porre $a \leq b$ se e solo se $b - a \in P$.

Definizione 3.1. Introduciamo il concetto di cono positivo. Dato un campo K, $P \subset K$ si dice cono positivo se soddisfa i seguenti:

$$P \cap -P = \{0\}$$
$$P \cup -P = K$$
$$\{x^2 | x \in K\} \subset K$$
$$P + P \subset P$$
$$P * P \subset P$$

Osservazione 3.2. Dato un campo K con un cono positivo P, la relazione $x \leq y \equiv y - x \in P$ è un relazione d'ordine totale che rende K un campo ordinato. Viceversa l'insieme dei valori non negativi di un campo ordinato è un cono positivo. Alla luce di questo i concetti di ordine e di cono positivo sono completamente interscambiabili (ovviamente la relazione fra ordini e coni positivi è una biezione).

Lemma 3.3. Sia K un campo, K è formalmente reale se e solo se -1 non è somma di quadrati.

Dimostrazione. Chiaramente se -1 è somma di quadrati allora K non è ordinabile, infatti se per assurdo lo fosse, allora -1 sarebbe somma di positivi, in quanto i quadrati sono sempre positivi, e quindi sarebbe positivo, il che non è possibile, infatti -1 è l'opposto di 1, che è positivo. Vediamo il viceversa.

Iniziamo con l'osservare che l'insieme delle somme dei quadrati S è un cono prepositivo, cioè un insieme che ha le seguenti proprietà:

$$-1 \notin S$$
$$\{x^2 | x \in K\} \subset K$$
$$S + S \subset S$$
$$S * S \subset S$$

Sia Σ l'insieme dei coni prepositivi di K, e sia $C \subset \Sigma$ una catena per la relazione d'ordine definite dall'inclusione $\subset$. Dato che $\bigcup_{A \in C} A$ è un maggiorante di C e che Σ è non vuoto poiché contiene S, per il lemma di Zorn si ha che esiste $P \in \Sigma$ massimale rispetto a $\subset$. Rimane da dimostrare che un massimale di Σ è un cono positivo.
Affermiamo che per ogni x si ha la seguente

$$Px \cap P + 1 = \emptyset \quad \vee \quad -Px \cap P + 1 = \emptyset$$

Sia per assurdo $px = q + 1$ e $-p'x = q' + 1$ con p, q, p', $q' \in P$. Moltiplicando membro a membro otteniamo $-pp'x^2 = 1 + q + q' + qq'$, cioè $-1 = pp'x^2 + q + q' + qq' \in P$, il che è una contraddizione perché P è un cono prepositivo.
Per dimostrare $P \cup -P = K$ prendiamo $x \in K$ e a meno di cambiare x con $-x$ assumiamo senza perdita di generalità che $Px \cap P + 1 = \emptyset$. Chiamiamo $P' = P - Px$, si verifica che $P' + P' \subset P'$ e $P' * P' \subset P'$, e che $-1 \notin P'$, altrimenti si avrebbe $Px \cap P + 1 \neq \emptyset$. Dato che si verifica $P \subset P'$, per massimalità si ha $P = P'$ e dunque $x \in P$ dato che $x \in P'$ (ricordo che $0 = 0^2 \in P$). Mostriamo ora che $J := P \cap -P$ è un ideale, visto che siamo in un campo basta dimostrare che J ha la proprietà di assorbimento. Preso $x \in J$ e $a \in K$ si ha $x, -x \in P$ e $a \in P \vee -a \in P$ per quanto appena detto ($P \cup -P = K$), dunque $ax, -ax \in P$ cioè $ax \in J$. Però J è un ideale proprio in quanto $-1 \notin P$, dunque contiene solo lo zero. □

Diamo ora un paio di fatti.

Fatto 3.4. [Pre84, Corollary 1.9]

$$S_K := \left\{ \sum_{i=1}^{n} a_i^2 \middle| a_i \in K \right\} = \bigcap_{P \text{ cono positivo su K}} P$$

Fatto 3.5. [Pre84, Theorem 1.26] Sia K un campo ordinato con P il cono positivo. Sia F una estensione di K. Se vale uno dei seguenti due casi allora P si estende a un cono positivo per F:

(1) $F = K(\alpha)$ dove α è la radice quadrata di un elemento positivo

(2) $[F : K]$ è dispari

Dunque in questi due casi F ammette un ordine che estende quello di K e perciò K non è massimamente ordinato.

Lemma 3.6. Sia K un campo. S_K è un cono positivo se e solo se K ammette un unico ordine.

Dimostrazione. $\boxed{\Longrightarrow}$ Sia, P un cono positivo, $S_K \subset P$ per 3.4. Dato che per ogni cono positivo P si ha $P \cup -P = K$ e $P \cap -P = \{0\}$, si ottiene che se due coni sono uno un sottoinsieme dell'altro allora sono lo stesso cono positivo.
$\boxed{\Longleftarrow}$ Segue immediatamente da 3.4. □

Introduciamo il concetto di *ordine massimale*, che come vedremo è equivalente alla definizione che daremo di campo reale chiuso.

Definizione 3.7. Un campo ordinato K con un ordine $\leq$ si dice massimamente ordinato se non esiste una estensione algebrica F di K ordinata il cui ordine estende $\leq$.

Prima di introdurre la definizione di campo reale chiuso dobbiamo dimostrare due lemmi sugli ordini massimali.

Lemma 3.8. Ogni elemento positivo di un campo massimamente ordinato è un quadrato perfetto. Pertanto un campo massimamente ordinato ammette un solo ordine.

Dimostrazione. Sia K un campo massimamente ordinato da un ordine il cui cono positivo è P. Se $a \in P$ allora anche $\sqrt{a} \in K$, altrimenti, per il lemma 3.5, $K(\sqrt{a})$ sarebbe un'estensione algebrica che estende l'ordine definito da P; pertanto $P \subset S_K \subset P$. La dimostrazione si conclude usando il lemma 3.6. □

Lemma 3.9. Sia K un campo ordinato. Esiste un'estensione algebrica F tale che F è un campo ordinato il cui ordine che estende quello di K e è massimamente ordinato.

Dimostrazione. Sia $\leq$ l'ordine su K e fissiamo $\overline{K}$ un'estensione algebrica di K. Consideriamo l'insieme $\mathfrak{F} := \left\{ (K', \preceq) \middle| K' \subset \overline{K} \text{ è un campo ordinato da } \text{"} \preceq \text{"} \text{ e } \preceq|_K = \leq \right\}$. Si verificano facilmente le ipotesi del lemma di Zorn; inoltre preso un elemento massimale F della famiglia $\mathfrak{F}$, si ottiene immediatamente la tesi. □

Diamo ora la definizione di campo reale chiuso

Definizione 3.10. Un campo si dice *campo reale chiuso* se è ordinabile e non ammette nessuna estensione algebrica propria formalmente reale.

Lemma 3.11. Un campo è reale chiuso se e solo se ammette un unico ordinamento ed è massimamente ordinato per questo ordinamento.

Dimostrazione. $\boxed{\implies}$ Come nella dimostrazione del lemma precedente, usando il lemma 3.5, si ha che per ogni ordinamento, ogni elemento positivo è un quadrato perfetto; dunque S_K è un cono positivo e per il lemma 3.6 l'ordinamento è unico.

$\boxed{\impliedby}$ Dato che il campo ammette un unico ordinamento ogni estensione algebrica ordinabile estende l'unico ordine ammissibile nel campo base; poiché il campo base è massimamente ordinato e nessuna estensione algebrica non banale può estendere il suo ordine, nessuna estensione algebrica non banale è ordinabile. □

Da questo segue l'esistenza dalla chiusura reale chiusa.

Definizione 3.12. Sia K un campo formalmente reale, un'estensione algebrica R si dice essere la chiusura reale di K se R è reale chiuso.

Lemma 3.13. Ogni campo formalmente reale ammetta una chiusura reale.

Dimostrazione. È conseguenza immediata dei lemmi 3.9 e 3.11. □

Teorema 3.14 (Artin-Schreier AS)**.** Sia R un campo. Le seguenti affermazioni sono equivalenti:

(1) R è reale chiuso

(2) R^2 è un cono positivo e ogni polinomio di grado dispari ha un radice in F

(3) $R(\sqrt{-1})$ è algebricamente chiuso e $R \neq R(\sqrt{-1})$

Dimostrazione. Per semplicità chiamiamo i una radice di $x^2 + 1$

(1) $\implies$ (2): È conseguenza di 3.8, 3.11 e di 3.5.

(2) $\implies$ (3): Dato che per 3.3 $-1 \notin R^2$ si ha che $R(i)$ è un estensione propria di R, rimane da dimostrare che $R(i)$ è algebricamente chiuso, il che si mostra nello stesso modo in cui si mostra che $\mathbb{C}$ è algebricamente chiuso. Sia α un elemento algebrico su $R(i)$, vogliamo dimostrare che $\alpha \in R(i)$. Consideriamo K la chiusura di Galois di $R(i, \alpha)$, e sia G il gruppo di Galois dell'estensione $K/R(i)$. Dato che K è il campo di spezzamento del polinomio minimo di α l'estensione di K su $R(i)$ ha grado finito. Il campo fissato da un $2-$Sylow di G è un estensione di grado dispari che per (2) deve essere 1, dunque G è un 2-gruppo. Supponiamo per assurdo che G non sia banale. Per i teoremi di Sylow esiste un sottogruppo di G di indice 2, dunque esiste un'estensione di grado 2 su $R(i)$. Per trovare un assurdo è sufficiente mostrare che tutti i polinomi di secondo grado a coefficienti in $R(i)$ ammettono radice, il che segue mostrando che ogni elemento di $R(i)$ ammette una radice quadrata, ma questo segue facilmente dalle ipotesi ricordando che $R^2 \cup -R^2 = R$.

(3) $\implies$ (1) Mostriamo prima di tutto che $R^2 + R^2 \subset R^2$. Dato che $R(i)$ è algebricamente chiuso, per ogni a, $b \in F$ devono esistere c, $d \in R$ tale che $a + ib = (c+id)^2$ ovvero che $a = c^2 - d^2$ e $b = 2cd$. Da questo segue che $a^2 + b^2 = (c^2 + d^2)^2 \in R^2$. Da questo otteniamo che S_R l'insieme delle somme di quadrati coincide con R^2, e dato che $i \notin F$ si ha che $-1 \notin S_K$, dunque R è formalmente reale per 3.3. L'unica estensione algebrica di F è $F(i)$ che non è formalmente reale per 3.3 in quanto $-1 = i^2$. □

Ora che i campi reali chiusi sono stati introdotti rigorosamente, possiamo dimostrare una versione leggermente più debole del teorema di Rolle, che ci servirà poi nella prossima sezione. Chiaramente, dimostrando che tutti i campi reali chiusi sono elementarmente equivalenti a $\mathbb{R}$, vale a dire dimostrando il teorema di Tarski [TM51], il Teorema di Rolle viene gratuitamente come conseguenza. Tuttavia i risultati di Sheperdson che presentiamo sono ottenibili autonomamente in modo relativamente semplice.

Lemma 3.15. Sia R un campo reale chiuso. Per ogni $f(x) \in R[x]$ valgono le seguenti affermazioni:

(1) $f(x)$ si riduce in fattori della forma $x - a$
o $(x - a)^2 + b$ per qualche a, $b \in R$ con $0 < b$

(2) Se a, $b \in R$ sono tali che $f(a)$ e $f(b)$ sono discordi,
allora esiste $c \in R$ tale che $a < c < b$ e $f(c) = 0$.
Ovvero vale il teorema degli zeri per i polinomi.

Dimostrazione. (1) Poiché $R[i]$ è algebricamente chiuso, ed è un'estensione di grado 2 su R, $f(x)$ si riduce in fattori irriducibili di primo o secondo grado in $R[X]$. Rimane da verificare che ogni polinomio di grado 2 irriducibile in $R[X]$ è della forma descritta. Usando il metodo del completamento del quadrato ogni fattore di grado due può essere scritto nella forma $(x - a)^2 + b$ per qualche a, $b \in K$. Se per assurdo b non fosse positivo allora $x = \sqrt{-b} + a$ sarebbe una radice, dunque il fattore non potrebbe essere irriducibile, allora b deve essere positivo.

(2) Segue immediatamente dalla scomposizione in fattori dei polinomi. Infatti i fattori $(x - a)^2 + b$ con b positivo hanno segno costante non nullo; dunque, dividendo per tali fattori, ci riconduciamo al caso in cui $f(x)$ sia interamente fattorizzabile. Per la stessa ragione, possiamo dividere per ogni potenza pari di fattori di primo grado (infatti questi non si annullano né in a né in b poiché in quei punti $f(x)$ non è nullo per ipotesi). Otteniamo così un polinomio interamente fattorizzabile e libero da quadrati. Dato che $f(a)f(b) < 0$ e che il segno di $f(x)$ è il prodotto di segni dei fattori, è necessario che un numero dispari di fattori irriducibile cambi segno tra a e b; ma poiché un fattore di primo grado cambia segno se e solo se la sua radice è compresa tra a e b, si ha che un numero dispari di radici di $f(x)$ è compreso tra tali valori. Il teorema risulta quindi dimostrato dato che 0 è pari. □

Osserviamo adesso che se la funzione f è definibile al prim'ordine, allora anche la sua defivata lo è. Usiamo adesso il valore assoluto, che si può costruire facilmente usando $\leq$, per dare la definizione di limite e quindi di derivata; dopodiché dimostreremo alcuni risultati.

Definizione 3.16. Siano x, y, h delle variabili e t, s dei termini.

$$x = |y| \equiv (x = y \wedge 0 \leq y) \vee (x = -y \wedge y \leq 0)$$
$$\lim_{x \to y} t(x) = s \equiv (\forall \varepsilon > 0)(\exists \delta)(\forall h)(|h| < \delta \to |t(y+h) - s| < \varepsilon)$$
$$t'(x) = s(x) \equiv \lim_{h \to 0} \frac{t(x+h) - t(x)}{h} = s(x)$$

Le stesse dimostrazioni dei fatti principali che valgono su $\mathbb{R}$ funzionano per qualunque campo ordinato K. In particolare valgono i seguenti risultati: i polinomi sono continui; l'operazione di derivazione è K-lineare; la derivata del monomio ax^n esiste ed è anx^{n-1}. Da questo segue che tutti i polinomi ammettono una derivata e questa ha grado strettamente minore del polinomio di partenza oppure è nulla. Un altro risultato vero in $\mathbb{R}$ è che se la derivata di $p(x)$ è positiva in un valore allora $p(x)$ è localmente crescente. In particolare a noi serve sapere che se $0 < p'(a)$ con $a \in K$, allora per ogni ε sufficientemente piccolo $p(a + \varepsilon)$ è positivo. Vediamo quest'ultimo risultato a titolo di esempio per tutti i risultati citati.

Lemma 3.17. Sia $p(x) \in K[x]$ un polinomio a coefficienti nel campo K, sia $p'(x)$ la sua derivata e sia $a \in K$. Se $0 < p'(a)$ allora esiste $0 < \delta$ tale che per ogni $\varepsilon < \delta$ positivo si ha $p(a-\varepsilon) < p(a) < p(a+\varepsilon)$. Viceversa, se $p'(a) < 0$ si ha $p'(a+\varepsilon) < p(a) < p'(a-\varepsilon)$.

Dimostrazione. Senza perdita di generalità, supponiamo che $p'(a)$ sia positivo. Fissiamo δ tale per cui per ogni $|\varepsilon| < \delta$ il rapporto incrementale $\frac{p(a+\varepsilon)-p(a)}{\varepsilon}$ sia positivo; questo δ esiste per definizione di derivata e perché $0 < p'(a)$. Dato che tale rapporto è positivo, scegliendo ε positivo, otteniamo che $p(a + \varepsilon) - p(a)$ deve essere positivo, e che $p(a - \varepsilon) - p(a)$ deve essere negativo; da questo cui segue la tesi. □

Teorema 3.18 (Versione debole del Teorema di Rolle)**.** Sia R un campo reale chiuso, sia $p(x) \in R[x]$ un polinomio a coefficienti in R, sia $p'(x)$ la sua derivata e siano a, $b \in R$ tali che $a < b$. Se $p(a) = p(b) = 0$, allora esiste $c \in R$ tale che $a \leq c \leq b$ e $p'(c) = 0$.

Dimostrazione. Se $p'(a) = 0$ abbiamo finito. Assumiamo senza perdita di generalità che $p'(a) > 0$. Per il lemma 3.15 la tesi segue esibendo c tale che $a \leq c \leq b$ e $p'(c) \leq 0$. Per il teorema 3.17 esiste $\delta > 0$ tale che $0 < p(a + \delta)$ e $a + \delta < b$. Dato che il polinomio $q(x) = p(x) - \frac{1}{2}p(a + \delta)$ cambia segno fra $a + \delta$ e b, deve avere almeno una radice nell'intervallo $]a + \delta, b[$. Sia c la più grande di queste radici. Osserviamo che $q'(x) = p'(x)$. Se per assurdo $p'(c) > 0$, allora, seguendo lo stesso ragionamento di prima, esiste $\delta' > 0$ che soddisfa $q(c+\delta') > 0$ e $c+\delta' < b$, e dunque vi è un'altra radice in $]c + \delta', b[$ contro la scelta di c. Per tanto $q'(c) = p'(c) \leq 0$ e la tesi segue. □

3.2 Modelli di Open Induction

Per adesso abbiamo trovato dei campi che sono analoghi al campo dei numeri reali, tuttavia i modelli di open induction dovrebbero essere delle versioni alternative dei numeri naturali, perciò, come i numeri naturali sono un sottoinsieme dei numeri reali allo stesso modo vorremmo ricavare da un campo reale chiuso un modello delle open induction, e viceversa da un tale modello ricostruire un campo reale chiuso. Prendiamo dunque un campo reale chiuso R e cerchiamo in esso un insieme Z analogo a quello dei numeri interi. Sicuramente vogliamo un dominio ordinato discreto, poiché, come abbiamo visto, queste proprietà sono implicate dagli assiomi di OI. Un qualunque sottoinsieme di R è naturalmente ordinato restringendo l'ordine di R stesso; tuttavia la condizione di ottenere ordine discreto richiede già alcune limitazioni. Con l'espressione ordine discreto intendiamo che ogni elemento abbia un successivo, ovvero che preso un valore x esiste un valore y tale per cui $x < y$ e nessun altro valore sta fra x e y. In altre parole, per ogni x deve esistere y, che chiamiamo il successivo di x, con la proprietà essere il minimo dei valori strettamente maggiori di x. Per avere un ordine discreto basta che esista il successivo di 0: infatti, se esiste $S(0)$ il successivo di 0, per ogni valore x si verifica che il suo successivo è $x + S(0)$. Se lo 0 ammette un successivo allora tale valore deve essere 1, infatti un numero positivo minore di 1 è maggiore del suo quadrato, il quale però è ancora positivo e quindi maggiore di 0. A priori il successivo di 0 potrebbe essere maggiore di 1 se $1 \notin Z$, ma questo è impossibile, infatti 0 e 1 sono gli unici valori idempotenti per il prodotto e gli assiomi di OI dimostrano che esistono due elementi idempotenti, dunque non possiamo scartare 1. A questo punto, stando agli assiomi, l'unica interpretazione possibile per la funzione di successore deve coincidere con la funzione $x \mapsto x + 1$. Anche imposte queste condizioni ci sono più modi per ottenere un dominio ordinato discreto, dobbiamo ricordarci però che quando costruiremo M il modello di OI dovremo dimostrare che esso soddisfa l'induzione per tutte le formule aperte. A tal fine sarà utile usare il fatto che su R, gli insiemi definiti da una formula aperta sono unione finita di intervalli. In realtà è vero di qualcosa di più forte, ovvero che qualunque insieme definito al prim'ordine su R è unione finita di intervalli; questa proprietà va sotto al nome di o-minimalità della teoria dei campi reali chiusi, e segue dal Teorema di Tarski [TM51], che infatti dimostra che ogni formula è equivalente a una aperta. Per poter usare questo fatto efficacemente dobbiamo porre un'ultima condizione a Z, ovvero che sia una parte intera di K; in questo modo un'unione finita di intervalli di R, intersecandoli con Z, rimangono un'unione finita di intervalli (definiti ora su Z). Dire che Z è una parte intera di K significa che, oltre che essere un dominio discreto, Z contiene una parte intera di ogni elemento di K, cioè per ogni valore $x \in K$ esiste un valore $a \in Z$ tale che $a \leq x < a + 1$. Infine, per ottenere un modello di OI da Z sarà sufficiente considerare solamente i valori non negativi, cioè poniamo $M := \{n \in Z | 0 \leq n\}$, dopodiché verificheremo che M sia effettivamente un modello di OI. Durante questa costruzione, non ci preoccuperemo di sapere se un campo reale chiuso ammette sempre una parte intera o se questa sia unica, vederemo semplicemente, come emerge dal lavoro di Sheperdson già citato [She64], che un anello

ordinato è un modello di OI se e solo se è costituito dagli elementi non negativi della parte intera di un campo reale chiuso. L'articolo di Sheperdson presenta questo risultato appoggiandosi al teorema di Tarski, quindi in modo leggermente diverso da come è stato presentato qui, dove ci siamo ricondotti a alcune proprietà basilari dei campi reali chiusi che abbiamo dimostrato nella sezione precedente. Infine, nell'ultima sezione di questo capitolo, usando la caratterizzazione appena enunciata, costruiremo esplicitamente modello ricorsivo di OI. Il prossimo obbiettivo dunque è quello di dimostrare il seguente teorema.

Teorema 3.19 (Sheperdson)**.** Una struttura M è un modello di OI se e solo se è costituita dagli elementi non negativi di una parte intera di un campo reale chiuso.

Da un campo reale chiuso a un modello di Open Induction

Diamo la definizione di parte intera e dimostriamo adesso che gli elementi non negativi di una parte intera di un campo reale chiuso costituiscono un modello di OI.

Definizione 3.20. Sia K un campo ordinato. Un sottoanello $Z \subset K$ si dice parte intera di K se per ogni $x \in K$ esiste $a \in Z$ tale che $a \leq x < a + 1$.

Lemma 3.21. Sia R è un campo reale chiuso e sia $\varphi(x)$ una formula aperta, allora $\varphi[R]$ è unione finita di intervalli della forma $\{x|a < x < b\}$ e di singoletti.

Dimostrazione. Gli insiemi definiti dalle formule aperte formano un algebra su un insieme (ovvero R) i cui generatori sono gli insiemi definiti dalle formula atomiche. Infatti se $\varphi_1(x)$ e $\varphi_2(x)$ sono formule aperte, allora $\varphi_1 \wedge \varphi_2[R] = \varphi_1[R] \cap \varphi_2[R]$, $\varphi_1 \vee \varphi_2[R] = \varphi_1[R] \cup \varphi_2[R]$, e $\neg\varphi_1[R] = R \setminus \varphi_1[R]$. Pertanto ci siamo ricondotti a dimostrare la tesi per una formula atomica φ. Inoltre una formula del tipo $p(x) = 0$ è equivalente a $p(x) \wedge 0 \wedge 0 \leq p(x)$, perciò possiamo assumere che $\varphi(x) \equiv p(x) \leq 0$. Usando la scomposizione dei polinomi del lemma 3.15, si ottiene facilmente quanto voluto. Infatti l'insieme definito da φ è unione di alcuni intervalli aperti aventi come estremi le radici di $p(x)$. □

Osserviamo anche che unione finita di intervalli aperti e singoletti è equivalente a dire unione finita di intervalli, infatti i singoletti sono casi speciali di intervalli chiusi.

Teorema 3.22. Sia R un campo reale chiuso e sia $M \subset R$ un dominio discreto. Se M è costituito dagli elementi non negativi di una parte intera di R, allora è un modello di OI.

Dimostrazione. L'interpretazione di M come una struttura aritmetica è quella ovvia: interpretiamo le operazioni aritmetiche come le rispettive operazioni di K ristrette a M, interpretiamo lo 0 con lo $0 \in R$ e la funzione successore S come la funzione $x \mapsto x+1$ dove $1 \in R$ è l'elemento neutro della moltiplicazione in R. Gli assiomi Q1-Q8 seguono facilmente, rimane da verificare che M soddisfa gli assiomi di induzione sulle formule aperte.

Prendiamo $\varphi(x)$ una formula aperta, con parametri e con x come unica variabile libera. Se $\varphi(x)$ è sempre vera in particolare M soddisfa l'assioma di induzione per φ. Supponiamo dunque che esistano degli elementi di M che falsifichino φ e che però M soddisfi $\varphi(0)$; per dimostrare che φ soddisfi l'induzione, è necessario trovare $a \in M$ tale che $\varphi(a) \wedge \neg\varphi(a+1)$. Osserviamo che $\varphi(x)$ può essere letta come una formula di R con parametri, infatti i parametri di φ appartengono a R in quanto $M \subset R$. Inoltre preso $a \in M$ si ha che $\varphi(a)$ è vera in M se e solo se è vera in R dato che in $\varphi(x)$ non compaiono quantificatori. Per quanto sappiamo sui campi reali chiusi $\varphi[R]$ è unione finita di singoletti e di intervalli aperti (e semirette, ammettendo convenzionalmente anche $\pm\infty$ come estremi), i quali sono identificati dai loro estremi; e ovviamente anche il complementare di $\varphi[R]$ in R è della stessa forma. Consideriamo $R \setminus \varphi[K] = \bigcup_{i=1}^{n} I_i$ dove gli I_i sono intervalli di estremi $b_i \leq c_i$. Consideriamo adesso solo I_j per $j \in J$ gli intervalli che intersecano M in un insieme non vuoto. Sia I l'intervallo di estremi b e c tale che b è il minimo fra i b_j al variare di $j \in J$ (questo minimo esiste perché J è un insieme finito). In parole povere abbiamo individuato il primo (per quello che può vedere M) elemento positivo in cui cambia il valore di verità di φ. Sia $a \in M$ la parte intera di b, dunque abbiamo che $a \leq b < a+1$. Se $\varphi(a)$ è vera allora non è vera $\varphi(a+1)$ perché in caso contrario si avrebbe che $I \cap M =$, se invece $\varphi(a)$ è falsa segue necessariamente che $a = b \neq 0$, e poiché b è il minimo fra gli estremi indicizzati in J si deve avere che $\varphi(a-1)$ è vera; in ogni caso riusciamo a falsificare la premessa dell'assioma di induzione su φ che quindi risulta verificato. □

Da un modello di Open Induction a un campo reale chiuso

Dimostriamo adesso che ogni modello delle open induction è costituito dagli elementi non negativi di una parte intera di un campo reale chiuso.

Teorema 3.23. Sia M una struttura aritmetica. Se M è modello di OI allora è una parte intera di un campo reale chiuso.

Dimostrazione. Prima di tutto costruiamo un anello a partire da M aggiungendoci gli opposti. La costruzione è standard: consideriamo il prodotto cartesiano $M \times M$, lo quozientiamo per $\sim$ dove $(a,b) \sim (c,d) \iff a+d = c+b$, indichiamo con $a-b$ la classe di (a,b) e aggiungiamo le seguenti operazioni: $(a-b)+(c-d) = (a+c)-(b-d)$ e $(a-b)*(c-d) = (ac+bd)-(ad+bd)$, dove le operazioni fra elementi di M sono le operazioni di M stesso; aggiungiamo anche la relazione d'ordine per cui un elemento $a-b$ è positivo (dove identifichiamo lo zero con $0-0$) se e solo se $b < a$. Usando le varie proprietà di OI dimostrate nel capitolo 2, la struttura Z costruita in questo modo risulta essere un dominio ordinato discreto tale che la mappa da M a Z, $a \mapsto a-0$, è un immersione che preserva le operazioni e la cui immagine coincide con i valori non negativi di Z. Consideriamo adesso il campo delle frazioni $Q = frac(Z)$, che è ordinato nel modo usuale (a/b positivo $\iff$ a e b sono concordi), e la sua chiusura reale R che esiste per il lemma 3.13. Rimane da dimostrare che Z è una parte intera di R.

Sappiamo che R è un estensione algebrica di Q. Prendiamo ora un elemento $\alpha \in R$ e dimostriamo che esiste la parte intera di α in Z, cioè esiste $a \in Z$ tale che $a \leq \alpha < a+1$. Chiaramente a meno di moltiplicare per -1 possiamo assumere che α sia positiva. Sia $p(x) \in Q[x]$ il polinomio minimo di α. Osserviamo che essendo Q di caratteristica 0, si ha che $p(x)$ è separabile, ovvero non ha radice doppie. Vogliamo ottenere la tesi procedendo per induzione sul grado di $p(x)$.

Svolgiamo il passo base. Se $p(x)$ ha grado uno allora $\alpha \in R$ e si conclude per il lemma della divisone euclidea: infatti esistono a, b, q, $r \in M$ tali che $\alpha = a/b$ e $a = bq + r$ con $r < b$. In questo caso abbiamo che $q \leq \alpha < q + 1$.

Svolgiamo il passo induttivo. Cerchiamo ora dei valori b, $c \in R$ positivi che separino α dalle altre radici di $p(x)$, ovvero tali che si abbia che per ogni $\beta \in R$ valga che $p(\beta) = 0 \wedge b \leq \beta \leq c \leftrightarrow \alpha = \beta$, inoltre ci serve anche che b, c abbiano parte intera in Z. Se α non è né la prima né l'ultima radice positiva di φ allora per la versione debole del teorema di Rolle troviamo i valori cercati tra le radici della derivata, che, avendo grado minore di quello di $p(x)$, è tale che le sue radici hanno parte intere in Z per ipotesi induttiva. Se α è la prima radice positiva è sufficiente porre $b = 0$, che è parte intera di sé stesso e per trovare c usiamo Rolle. Se invece α è l'ultima radice positiva allora basterà porre $c = nM/m$ dove n è il grado di $p(x)$, M è il massimo fra 1 e i coefficienti, e m è il minimo fra 1 e il coefficiente direttore. Semplici conti mostrano che valutando $p(x)$ in un valore maggiore di c risulta che il monomio di grado massimo è in valore assoluto maggiore della somma dei valori assoluti degli altri monomi, dunque nessuna radice può essere più grande di c, che essendo razionale ha parte intera in Z come spiegato prima. Anche in questo caso per trovare b usiamo Rolle.

Siano dunque b_0, c_0 le parti intere rispettivamente di b e di c. Dato che $b \leq \alpha \leq c$, si verifica uno dei seguenti tre casi: $b_0 \leq \alpha < b_0 + 1$; $b_0 + 1 \leq \alpha < c_0$; $c_0 \leq \alpha < c_0 + 1$. Nel primo e nel terzo caso b_0 e c_0 sono rispettivamente la parte intera di α per definizione. Supponiamo dunque di essere nel secondo caso, in cui abbiamo che i numeri "interi" $b_0 + 1$ e c separano α dalle altre radici di $p(x)$. Se $p(b_0 + 1) = 0$, poiché $\alpha = b_0 + 1 \in Z$, $b_0 + 1$ è la parte intera di α e concludiamo. Supponiamo dunque che $p(b_0 + 1)$ non sia nullo, a meno di moltiplicare $p(x)$ per -1, possiamo supporre che sia positivo. Consideriamo la seguente formula con parametri: $\varphi(x) \equiv x \leq b_0 + 1 \vee 0 \leq p(x) \vee c_0 < x$[1]. Dato che $p(b_0 + 1)$ è positivo e che fra $b_0 + 1$ e c_0 intercorre esattamente una radice di $p(x)$ e che $p(x)$ è separabile, segue che $p(c_0)$ è strettamente negativo e quindi che $\varphi(c_0)$ è falso. Dato che $\varphi(0)$ è vera, poiché φ è una formula aperta, deve esistere $a \in M$ tale $\varphi(a)$ è vero e $\varphi(a + 1)$ è falso. Tuttavia i valori per cui $\varphi(x)$ si falsifica sono nell'intervallo $(\alpha, c_0]$; dunque, affinché $\varphi(a)$ sia vero e $\varphi(a + 1)$ sia falso, deve accadere che

[1] Osserviamo che tale formula è esprimibile a parametri in M usando il linguaggio dell'aritmetica, infatti la diseguaglianza $0 \leq p(x)$ è equivalente a una diseguaglianza della forma $p_1(x) \leq p_2(x)$ dove $p_1(x)$, $p_2(x) \in M[x]$

$a \leq \alpha < a+1$. Abbiamo dimostrato che la parte intera di α appartiene a Z e abbiamo concluso che M è costituito dagli elementi non negativi di una parte intera del campo reale chiuso R. □

3.3 Un esempio computabile

La costruzione di un esempio computabile di una parte intera di un campo reale chiuso non isomorfa a $\mathbb{N}$ non è immediata. Noi ci serviremo di due ingredienti. Prima di tutto introdurremo $K\langle\langle\varepsilon\rangle\rangle$, l'insieme delle serie di Puiseux a coefficienti in un campo K. Una serie di Puiseux è una serie formali $\sum_{i\geq k} a_i\varepsilon^{i/q}$ dove $i, k \in \mathbb{Z}$, $a_i \in K$ e $q \in \mathbb{N}$ e ε è un'indeterminata. Si dimostra che, se K è ordinato, $K\langle\langle\varepsilon\rangle\rangle$ è un campo ordinato che estende K. La scelta di ε come indeterminata al posto di un più neutrale X è giustificato dal fatto che ε risulterà essere un infinitesimo su K. Dimostreremo anche che $R\langle\langle\varepsilon\rangle\rangle$ è reale chiuso se R lo è. Infine è facile costruire una parte intera di $K\langle\langle\varepsilon\rangle\rangle$ e vedere che essa è computabile a patto che K lo sia. Come ultimo ingrediente dunque dobbiamo trovare un campo reale chiuso computabile. A tale scopo useremo $\mathbb{R}_{alg}$. Infatti mostreremo che per ogni campo computabile, la sua chiusura reale è computabile, e dato che $\mathbb{Q}$ è ovviamente computabile otteniamo quanto ci serve. Sfruttando il fatto che $\mathbb{R}_{alg}\langle\langle\varepsilon\rangle\rangle$ contiene un infinito (su $\mathbb{N}$), cioè ε^{-1}, costruiremo una sua parte intera che contiene dei valori non standard e che quindi non può essere isomorfa a $\mathbb{N}$.

Serie di Puiseux

Sia K un campo. Indichiamo con $K[[X]]$ l'anello delle serie formali di potenze a coefficienti in K nell'indeterminata X. Gli elementi invertibili in $K[[X]]$ sono le serie con termine noto non nullo. Dato che ogni serie non nulla è il risultato del prodotto fra una potenza di x e una serie con termine noto non nullo segue che se aggiungiamo X^{-1} all'anello otteniamo un campo i cui elementi sono della forma $\sum_{i\geq k}^{\infty} a_i x^i$ con $i, k \in \mathbb{Z}$ e $a_i \in K$. Il campo $K[[X]][X^{-1}]$ è il campo delle frazioni di $K[[X]]$ e si indica con $K((X))$. Introduciamo alcune grandezze legate ai campi di serie: sia p una serie, l'ordine di p, indicato con $o(p)$ è il grado del monomio col grado minore fra quelli con coefficiente non nullo, se p è la serie nulla poniamo $o(p) = \infty$; se la serie p non è nulla, chiamiamo coefficiente iniziale di p, e lo indichiamo con $In(p)$, il coefficiente del monomio di grado $o(p)$. Si verifica facilmente che l'ordine soddisfa le seguenti affermazioni: $o(pq) = o(p) + o(q)$ e $o(p+q) \geq min(o(p), o(q))$ con uguaglianze se $o(p) \neq o(q)$. Se K è ordinato anche $K((X))$ è ordinabile, infatti, se $\leq$ è l'ordinamento su K, allora possiamo costruire un ordine su $K((X))$ i cui elementi positivi sono le serie per cui il coefficiente iniziale è positivo.

Osserviamo adesso che fissata un indeterminata X possiamo vedere gli elementi di $K((X^k))$ come elementi di $K((X))$. Fissiamo dunque l'indeterminata ε e scriviamo il campo delle serie di Puniseux nel seguente modo: $K\langle\langle\varepsilon\rangle\rangle := \bigcup_{q\in\mathbb{Q}} K((\varepsilon^q))$. Da questa

scrittura otteniamo immediatamente che le serie di Puniseux formano un campo: infatti prese due tali serie, portando gli esponenti dell'indeterminata a minimo comune multiplo, si ha che entrambe appartengono a un $K((\varepsilon^q))$ per un opportuno q, sono quindi sommabili, moltiplicabili e ammettono un inverso. Dobbiamo adesso dimostrare che preso un campo reale chiuso R anche $R\langle\langle\varepsilon\rangle\rangle$ è reale chiuso. Per raggiungere questo risultato dobbiamo prima citare un fatto generale noto come Lemma di Hensel.

Fatto 3.24 (Lemma di Hensel)**.** [GR71, Chap. I, §5.6] Sia A un anello, e $\mathfrak{m} \lhd A$ un ideale massimale. Siano h, f, $g \in A[X]$ dei polinomi monici tali che f e g siano coprimi modulo $(\mathfrak{m})$ e valga la relazione $h \equiv fg \pmod{\mathfrak{m}}$. Allora per ogni $n \in \mathbb{N}$ esistono unici f_n, g_n tali che $f_n \equiv f \pmod{\mathfrak{m}}$, $g_n \equiv g \pmod{\mathfrak{m}}$ e $h \equiv f_n g_n \pmod{\mathfrak{m}^n}$.

In questo contesto con la scrittura $h \equiv fg \pmod{\mathfrak{m}}$ intendiamo dire che $fg - h \in \mathfrak{m}A[X]$.

Corollario 3.25. Sia $p(w, X)$ un polinomio monico in X a coefficienti in $K[[w]]$. Se $p(0, X) \in k[X]$ si fattorizza in due polinomi e coprimi allora anche $p(w, X)$ è riducibile.

Dimostrazione. Chiamiamo $f_0(X)$, $g_0(X)$ due polinomi coprimi che soddisfano $f_0(X)g_0(X) = p(0, X)$. Osservo che $p(0, X) \equiv p(w, X) \pmod{(w)}$. Siccome $(w) \lhd K[[w]]$ è massimale, siamo nelle ipotesi del lemma di Hensel ed esistono $f_k(w, X)$, $g_k(w, X)$ tali che $f_k(w, X)g_k(w, X) \equiv p(w, X) \pmod{(w)^k}$. Per unicità, f_k e f_{k+1} condividono gli stessi coefficienti dei monomi che hanno grado in w minore di k; quindi i coefficienti di f_k sono definitivamente costanti in k (lo stesso vale per g_k). Dunque, prendendo per ogni grado tali coefficienti stabilizzati, otteniamo $f(w, X)$, $g(w, X) \in K[[w]][X]$ il cui prodotto è equivalente a $p(w, X)$ modulo $(w)^k$ per ogni k; ma se due serie hanno gli stessi coefficienti ad ogni grado allora sono la stessa serie, dunque $p(w, X) = f(w, X)g(w, X)$. Inoltre, dato che $f_0(X)$ e $g_0(X)$ hanno grado (strettamente) maggiore di 0, pure f e g hanno grado positivo (in X); dunque la fattorizzazione $p(w, X) = f(w, X)g(w, X)$ non è banale. □

Teorema 3.26. [Now00, Teorema di Newton-Puiseux] Sia K un campo algebricamente chiuso di caratteristica zero. Allora $K\langle\langle\varepsilon\rangle\rangle$ è algebricamente chiuso.

Dimostrazione. È sufficiente mostrare che ogni polinomio monico

$$P(\varepsilon, X) = x^n + a_1(\varepsilon)x^{n-1} + \cdots + a_n(\varepsilon) \in K\langle\langle\varepsilon\rangle\rangle[X]$$

di grado $n > 1$ è riducibile. Facendo uso di un cambio di variabili di Tschirnhausen $x' = x - \frac{1}{n}a_1(\varepsilon)$ possiamo assumere che a_1 sia nullo. Sia $r_k = o(a_k) \in \mathbb{Q}$ per ogni a_k non nullo, e poniamo $r = min\{\frac{r_k}{k}\}$. Ovviamente $0 \leq r_k/k - r$ e abbiamo l'uguaglianza per almeno un indice k. Prendiamo un intero positivo q tale per cui ogni serie di Puiseux $a_k(\varepsilon)$ è della forma $f_k(\varepsilon^{1/q})$ con $f_k(\varepsilon) \in K[[\varepsilon]]$, e sia $r = p/q$. Dopo il cambio di variabili $\varepsilon = w^q$, $X = Yw^p$ otteniamo $P(\varepsilon, X) = w^{np}Q(w, Y)$, dove

$$Q(w, Y) = Y^n + b_2(w)Y^{n-2} + \cdots + b_n(w)$$

con $b_k(w) = a_k(w^q)w^{-kp}$. Dato che per b_k non nullo vale $o(b_k) \in \mathbb{Z}$ e

$$o(b_k(w)) = qr_k - kp = qk\left(\frac{r_k}{k} - r\right) \in \mathbb{N},$$

$Q(w, Y)$ è un polinomio a coefficienti in $K[[w]]$. Inoltre $o(b_k) = 0$ per almeno un k, dunque $b_k(0) \neq 0$ per ogni tale k. Dunque per ogni $c \in K$ vale che

$$Q(0, Y) \neq (Y - c)^n,$$

pertanto $Q(0, Y)$ è il prodotto di due polinomi coprimi. Quindi per il lemma di Hensel $Q(w, Y)$ è uguale al prodotto di due polinomi $Q_1(w, Y)$, $Q_2(w, Y) \in K[[w]][Y]$. Allora

$$P(\varepsilon, X) = \varepsilon^{nr} Q_1(\varepsilon^{1/q}, \varepsilon^r X) \cdot Q_2(\varepsilon^{1/q}, \varepsilon^r X)$$

e il teorema segue. □

Corollario 3.27. Sia R un campo reale chiuso. Allora $R\langle\langle\varepsilon\rangle\rangle$ è reale chiuso.

Dimostrazione. Infatti aggiungere $i := \sqrt{-1}$ commuta con il campo di Puniseux, vale a dire $R\langle\langle\varepsilon\rangle\rangle[i] \cong R[i]\langle\langle\varepsilon\rangle\rangle$. Per il teorema Artin-Schreier (3.14), $R[i]$ è algebricamente chiuso; dunque usando il teorema precedente dunque otteniamo che $R\langle\langle\varepsilon\rangle\rangle[i]$ è algebricamente e, sempre per Artin-Schreier, otteniamo che $R\langle\langle\varepsilon\rangle\rangle$ è reale chiuso. □

Possiamo ricavare una parte intera di $R\langle\langle\varepsilon\rangle\rangle$ dall'insieme dei polinomi in indeterminata $\varepsilon^{-1/q}$ al variare di $q \in \mathbb{N}$ e a coefficienti in R. Basta considerare i polinomi che sono nulli oppure che hanno coefficiente direttore positivo e termine noto intero (ha senso parlare di interi in un qualunque campo di caratteristica zero perché esiste un'unica immersione di $\mathbb{Z}$ in K). Osserviamo che consideriamo i polinomi nell'indeterminata $\varepsilon^{-1/q}$, infatti non vogliamo considerare potenze positive di ε poiché sarebbero infinitesimi, e ogni valore più piccolo di 1 in un modello di OI deve essere nullo. È ovvio che un insieme 'sì fatto di polinomi a coefficienti in R sia ricorsivo qualora lo sia anche il campo R.

Campo reale chiuso computabile

Per completare la costruzione di un modello ricorsivo dobbiamo esibire un campo reale chiuso computabile. A questo scopo ci serviremo dell'eliminazione di Tarski con la quale dimostreremo che la chiusura reale di un campo ordinato ricorsivo rimane ricorsiva. Fatto ciò segue immediatamente che $\mathbb{R}_{alg}$ è un campo computabile e così terminiamo la costruzione.

Nell'articolo "A decision method for elementary algebra and geometry" Tarski [TM51] presenta una procedura di decisione algebrica basata sull'algoritmo di Strum. Il teorema di Strum può essere esso stesso visto come una procedura algebrica per determinare la verità di una qualunque proposizione della forma "Esistono esattamente k radici del polinomio p nell'intervallo $]a, b[$ ". Tarski generalizza questo risultato

fornendo, come lemma per il suo risultato principale, una procedura per decidere le proposizioni della forma "Ci sono esattamente k valori che soddisfano σ", dove σ è un sistema di equazioni in x della forma $a_n x^n + \cdots + a_0 = 0$ e diseguaglianze in x della forma $a_n x^n + \cdots + a_0 > 0$. Usando questo risultato, Tarski mostra che esiste un metodo per determinare da ogni formula φ una formula $U(\varphi)$ che è equivalente a φ nella teoria dei campi reali chiusi, che non contiene quantificatori e che non contiene variabili libere eccetto quelle che compaiono libere in φ. Precisamente, sarà questo il risultato che useremo in questa tesi. Per quanto riguarda il teorema di Tarski, ovvero l'esistenza di una procedura per decidere il valore di verità delle formule chiuse della teoria dei campi reali chiusi, esso segue da quanto appena detto e dal fatto che le formule senza quantificatori e senza variabili libere sono composte di uguaglianze e diseguaglianze di espressioni a valori in $\mathbb{N}$ e quindi facilmente verificabili o falsificabili.

Definizione 3.28. Dato un campo K un campo, denotiamo con $L(K)$ il linguaggio della teoria degli anelli ordinati espanso con delle constanti che rappresentano gli elementi di K.

Teorema 3.29. [Mad70] Se K è un campo ordinato computabile, allora la sua chiusura reale R è computabile.

Dimostrazione. Sia $\alpha \in R$. Con *notazione* per α si intende una coppia (f, n), dove $f \in K[X]$ e $n \in \mathbb{N}$, tale che $x = \alpha$ sia l'unica soluzione di

$$\text{"}f(x) = 0 \wedge f \text{ ha esattamente } n \text{ radici prima di } \alpha\text{"}.$$

È ovvio che ogni elemento di α ha una notazione (dato che ogni chiusura reale è un'estensione algebrica), e che due elementi distinti non possono avere una notazione in comune. Fissiamo adesso una enumerazione $\{T_i\}$ delle notazioni, e, se T_n è la notazione di un elemento di R, denotiamo con $\langle n \rangle$ tale elemento, altrimenti poniamo $\langle n \rangle$=0. Vogliamo mostrare che le seguenti relazioni sono computabili: $\langle n \rangle = \langle m \rangle$, $\langle n \rangle = 0$, $\langle n \rangle = 1$, $\langle n \rangle + \langle m \rangle = \langle o \rangle$, $\langle n \rangle * \langle m \rangle = \langle o \rangle$ e $\langle n \rangle \leq \langle m \rangle$. Sia $T = (f, n)$ una coppia della forma di cui sopra, la proposizione "T è la notazione per x", dove x è una variabile, è esprimibile nel linguaggio $L(K)$ tramite una formula della forma "$f(x) = 0$ e f ammette esattamente n radici strettamente minori di x". Denotiamo tale formula con $A(T, x)$; è chiaro che tale formula conterrà i coefficienti del polinomio f, che sono stati accortamente aggiunti al linguaggio. Inoltre, è chiaro anche che data T la formula $A(T, x)$, o per meglio dire una sua codifica in $\mathbb{N}$, è ottenibile tramite una procedura ricorsiva. Consideriamo, ad esempio, la relazione $\langle n \rangle = \langle m \rangle$: questa è esprimibile mediante la formula $C(n, m, a_1, \ldots, a_k) \equiv (\exists x,\, y)(A(T_n, x) \wedge A(T_m, y) \wedge x = y)$, dove intendiamo che $a_i \in K$ e $C(n, m, x_i, \ldots, x_k)$ sia una $L-$formula. Per il risultato di Tarski è possibile costruire una formula aperta $B(x_1, \ldots, x_k)$ che soddisfa $(\forall\, x_1, \ldots, x_k)(B(x, y, x_1, \ldots, x_k) \leftrightarrow C(n, m, x_1 \ldots, x_k))$. Essendo una formula aperta, B contiene solo uguaglianze e diseguaglianze fra espressioni nelle variabili $x_1, \ldots x_k$. Usando l'ipotesi che K sia computabile riusciamo a computare il valore di verità della

formula $B(a_i, \ldots, a_k)$, che è lo stesso di $C(n, m, a_1, \ldots, a_k)$. Ricordiamo che il risultato di Tarski è costruttivo, nel senso che fornisce un metodo esplicito e ricorsivo per determinare la formula B a partire dalla formula C; dunque la procedura appena descritta può essere implementata da funzioni ricorsive totali (in quanto, quelle descritte, sono tutte procedure terminanti). Abbiamo dunque mostrato che la relazione su $\mathbb{N}$ data da $\langle n \rangle = \langle m \rangle$ è computabile, nello stesso modo si può mostrare che tutte le relazioni prima citate sono computabili; questo conclude la dimostrazione. □

Approfondimenti

Sia M il modello che abbiamo costruito e chiamiamo $\Omega = \varepsilon^{-1}$. In M esistono i seguenti elementi: Ω, $\Omega\sqrt{2}$, $\Omega\sqrt[3]{2}$. Questi elementi mostrano che né l'irrazionalità di $\sqrt{2}$:

$$x^2 \neq 2y^2 \vee x = 0,$$

né l'ultimo teorema di Fermat

$$x^3 + y^3 \neq z^3 \vee xyz = 0$$

sono dimostrabili in OI. Una conseguenza di questo è che il modello M non è normale, ovvero non è integralmente chiuso dato che $\sqrt{2} \in Frac(M) \setminus M$. Osseraviamo che la normalità può essere espressa al prim'ordine tramite gli assiomi N. Dove $\mathrm{N}=\{\mathrm{N}_n\}_{n\in\mathbb{N}}$, e per ogni $n \in \mathbb{N}$ N_n è il seguente assioma

$$y \neq 0 \wedge x^n + z_1 x^{n-1} y + 1 \cdots + z_n y^n = 0 \to (\exists z)(zy = x).$$

Da altra parte sappiamo che frammenti dell'aritmetica da IE_1 a PA dimostrano la normalità e non sono ricorsivi; dunque ci si potrebbe chiedere se esistono modelli normali e ricorsivi di OI. Prima di rispondere ci poniamo un'altra domanda analoga: esistono modelli ricorsivi di OI che contengono numeri primi nonstandard? L'insieme dei numeri primi non è illimitato in M, anzi M non contiene numeri primi nonstandard: ha solo numeri primi finiti [BO96, Abstract]. L'esistenza di numeri primi infiniti potrebbe suggerire la possibilità di codificare un insieme non computabile e dunque l'impossibilità di avere un modello ricorsivo, come accade per IE_1. Tuttavia Berarducci e Otero in A Recursive Nonstandard Of Normal Open Induction (1996) danno una risposta affermativa alle domande poste tramite il seguente risultato:

Teorema 3.30. [BO96, §1 theorem 1.3] Esiste un modello nonstandard ricorsivo di NOI con un insieme di primi illimitato.

Dove NOI è la teoria di Open Induction a cui si aggiungono gli assiomi di normalità.

Bibliografia

[BO96] Alessandro Berarducci and Margarita Otero, *A recursive nonstandard model of normal open induction*, The Journal of Symbolic Logic **61** (1996), no. 4, 1228–1241.

[Goo65] R. L. Goodstein, *Review of A Non-Standard Model for a Free Variable Fragment of Number Theory by j. c. shepherdson*, The Journal of Symbolic Logic **30** (1965), no. 3, 389–390, Reviewed Work: *A Non-Standard Model for a Free Variable Fragment of Number Theory*.

[GR71] Hans Grauert and Reinhold Remmert, *Analytische stellenalgebren*, Die Grundlehren der mathematischen Wissenschaften, vol. 176, Springer-Verlag, Berlin, New York, 1971, Unter Mitarbeit von O. Riemenschneider.

[HP98] Petr Hájek and Pavel Pudlák, *Metamathematics of first-order arithmetic*, Perspectives in Mathematical Logic, Springer, 1998.

[Mad70] E. W. Madison, *A note on computable real fields*, Journal of Symbolic Logic **35** (1970), no. 2, 239–241.

[Now00] Krzysztof Jan Nowak, *Some elementary proofs of puiseux's theorems*, Universitatis Iagellonicae Acta Mathematica **38** (2000), 279–282.

[Pre84] Alexander Prestel, *Lectures on formally real fields*, Lecture Notes in Mathematics, vol. 1093, Springer, 1984.

[She64] John C. Shepherdson, *A non-standard model for a free variable fragment of number theory*, Bulletin of the British Society for the History of Mathematics **29** (1964), 265–276.

[TM51] Alfred Tarski and J. C. C. McKinsey, *A decision method for elementary algebra and geometry*, University of California Press, Berkeley and Los Angeles, 1951, Prepared for Publication with the Assistance of J.C.C. McKinsey.

[Wil85] G. Wilmers, *Bounded existential induction*, The Journal of Symbolic Logic **50** (1985), 72–90.