Un'analisi costruttiva della nozione di ordinale con una applicazione al teorema di Goodstein

Alberto Conz
Tesi di Laurea
Corso di Laurea Specialistica in Informatica
Dipartimento di Matematica Pura ed Applicata
Università degli Studi di Padova
Relatore: Prof. Silvio Valentini
Controrelatore: Prof. Giovanni Sambin

18 aprile 2007

Indice

Introduzione

Con la scoperta del Primo Teorema di Incompletezza di Godel nel 1931 la comunità matematica ha conosciuto l'esistenza di proposizioni esprimibili all'interno di un sistema formale (ad es. l'aritmetica di Peano (PA)) che sono 'vere', ma non sono dimostrabili a partire dagli assiomi del sistema. Tuttavia tali proposizioni sembravano dover possedere un carattere di innaturalità: la comunità matematica riteneva infatti che le proposizioni oggetto del Teorema di Incompletezza fossero meri artefatti logici, enunciati privi di un reale significato matematico e quindi privi di interesse per la comune pratica matematica. Tale pensiero era destinato a mutare. In [KirbyParis77] viene presentato il primo enunciato sui numeri naturali indipendente da PA (vera ma non dimostrabile in PA) e successivamente in [KirbyParis82] i risultati precedenti vengono utilizzati per mostrare l'indipendenza da PA di uno dei più famosi teoremi sui naturali, il teorema di Goodstein. Il teorema di Goodstein, presentato in [Goodstein44], afferma che una particolare sequenza di naturali converge a zero. Dato un naturale di partenza p e una base m, la successione si sviluppa nel seguente modo:

- Si scrive p in forma normale di Cantor, cioè si scrive il numero come somma di potenze di m e si ripete ricorsivamente l'operazione sugli esponenti delle potenze. Ad es., supponendo $m = 2$ e $p = 9$, la forma normale di Cantor del numero p è

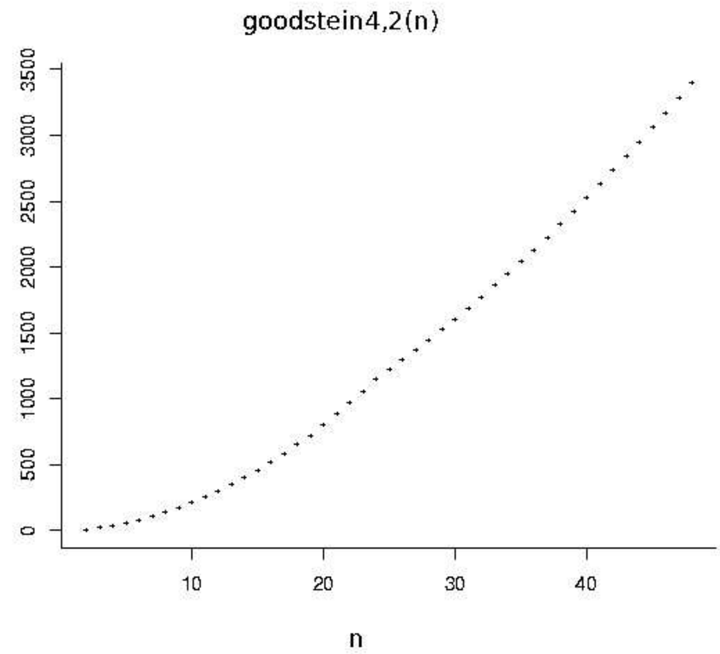
$$p = 2^3 + 2^0 = 2^{2^1+2^0} + 2^0$$

- Si sostituisce ad ogni occorrenza di m nella forma normale di Cantor di p il naturale $m + 1$ e si sottrae 1 dalla nuova somma. Il numero naturale così ottenuto è il nuovo elemento della successione. Nel caso dell'esempio precedente

$$p' = 3^{3^1+3^0} + 3^0 - 1 = 81$$

- Si ripete il procedimento descritto a partire dalla base $m+1$ e dal naturale calcolato fino a che non si raggiunge lo 0.

Il risultato mostrato dal teorema risulta sorprendente qualora si osservi il comportamento della sequenza anche a partire da numeri naturali piccoli come 4.



Si osserva infatti che la funzione nella sua fase iniziale cresce molto velocemente e nulla fa supporre che la curva ad un certo punto descresca fino a convergere a 0. La particolarità della sequenza di Goodstein si rispecchia anche negli strumenti necessari per dimostrarne la convergenza. Infatti la dimostrazione del teorema di Goodstein si fonda sull'utilizzo dei numeri ordinali. Tali numeri possono essere considerati estensioni dei numeri naturali e sono essenzialmente rappresentanti di classi di insiemi (di cardinalità finita o infinita) su cui è definito un morfismo d'ordine. La dimostrazione del teorema di Goodstein si può quindi riassumere in questo modo: Data una sequenza di Goodstein possiamo costruire una sequenza di numeri ordinali 'parallela' alla sequenza data. Tale sequenza di ordinali risulta essere una sequenza decrescente ed ogni elemento di questa sequenza è maggiore o uguale ad un qualsiasi elemento della sequenza di Goodstein. Infine, l'assioma di fondazione è equivalente al fatto che ogni sequenza decrescente di ordinali converge e quindi otterremmo una contraddizione se la sequenza di Goodstein data non convergesse.
In questo scritto il nostro scopo è cercare di analizzare costruttivamente la nozione di ordinale per poi valutare tale nozione nello sviluppo costruttivo di una dimostrazione del teorema di Goodstein. Vogliamo infatti osservare le potenzialità dimostrative degli ordinali immersi in una teoria costruttiva e quindi privati dei concetti di infinito attuale, induzione transfinita ed in generale di tutte le proprietà derivanti dagli assiomi della teoria degli insiemi rifiutati in ambito costruttivo. Articoleremo dunque lo scritto nel seguente modo:

- Nel **Capitolo 1** presenteremo la teoria assiomatica degli insiemi con l'aggiunta dell'assioma di scelta (ZFC) e definiremo all'interno di tale teoria la nozione classica di numero ordinale.

- Nel **Capitolo 2** svilupperemo estesamente la dimostrazione classica del teorema di Goodstein fornendo le dimostrazioni dei teoremi più importanti ed evidenziando l'utilizzo essenziale degli assiomi di ZFC.
- Nel **Capitolo 3** forniremo una breve introduzione a ITT, teoria che adotteremo come teoria costruttiva di riferimento nello scritto.
- Nel **Capitolo 4** proporremo un framework costruttivo per ordinali. Dimostremo le proprietà presentate dai numeri ordinali in forma normale e definiremo un ordine su di essi.
- Infine nel **Capitolo 5** inizieremo uno sviluppo costruttivo della dimostrazione del teorema di Goodstein, così evidenziando i limiti e le potenzialità del framework costruttivo presentato nel capitolo precedente.
- Nell' **Appendice A** definiremo nel formalismo di ITT il framework costruttivo per gli ordinali, mentre nell'**Appendice B** svilupperemo le dimostrazioni dei teoremi dei Capitoli 4 e 5.

Capitolo 1

Teoria degli insiemi e ordinali

Presentiamo in questo capitolo la teoria assiomatica degli insiemi di Zermelo-Fraenkel con l'inclusione dell'assioma della scelta (ZFC) e la teoria degli ordinali di Von Neumann. E' possibile trovare una buona introduzione all'argomento in [Hamilton82] e [Sierpinski] ed è inoltre disponibile in [Cantor92] una raccolta dei primi scritti di Cantor sulla teoria degli insiemi.

1.1 Cenni storici

Possiamo individuare la nascita della teoria degli insiemi nella pubblicazione nel 1874 dell'articolo *Su una proprietà della classe di tutti i numeri reali algebrici*[Cantor92]. In questo articolo Cantor mostra che l'insieme dei numeri reali algebrici è in relazione biunivoca con l'insieme dei naturali ed inoltre mostra che i numeri reali non possono essere messi in relazione biunivoca con i numeri naturali. In un successivo articolo del 1878 (*Contributo alla teoria delle molteplicità*[Cantor92]) Cantor introduce il concetto fondamentale di potenza di un insieme, concetto che porta con sè l'idea che se due insiemi possono essere messi in corrispondenza biunivoca allora hanno la stessa potenza. Nel 1883 Cantor pubblica (all'interno di un trattato più ampio pubblicato dal 1879 al 1884 sui Mathematische Annalen) una prima teoria dei numeri ordinali e cardinali. In questa prima versione i numeri ordinali sono trattati come tipi d'ordine di insiemi ben ordinati; inoltre viene data una iniziale versione dell'aritmetica dei numeri transfiniti che sarà trattata più dettagliatamente negli scritti successivi del 1895 e 1897. Negli ultimi anni dell'800 vengono scoperti i primi paradossi di questa ingenua teoria degli insiemi (paradosso di Burali-Forti) fino alla formulazione nel 1902 del paradosso di Russel. Le problematiche emerse dal paradosso di Russel portano alla prima formulazione di una teoria assiomatica degli insiemi (in cui viene incluso, e quindi esplicitato, l'uso dell'assioma di scelta) da parte di Ernst Zermelo nel 1908 e ad una definizione dei numeri ordinali all'interno di questa teoria assiomatica da parte di Von Neumann negli anni venti.

1.2 ZFC

Presentiamo ora la lista degli assiomi di ZFC fornendo per ognuno di essi una breve descrizione:

ZF1(estensionalità)

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

L'assioma di estensionalità esprime la proprietà fondamentale che dice che un insieme è determinato dai suoi elementi e quindi due insiemi sono uguali se e solo se hanno gli stessi elementi.

ZF2(insieme vuoto)

$\exists z.\forall x.x \notin z$

L'assioma dell' insieme vuoto dice che esiste un insieme senza elementi. In virtù dell'assioma di estensionalità tale insieme sarà unico e lo possiamo quindi indicare con $\emptyset$.

ZF3(coppia)

$\forall x.\forall y.\exists z.\forall w.(w \in z \leftrightarrow w = x \vee w = y)$

L'assioma della coppia dice che dati due insiemi x e y c'è un insieme z i cui elementi sono esattamente x e y.

ZF4(unione)

$\forall y.\exists z.\forall x.(x \in z \leftrightarrow \exists w.x \in w \wedge w \in y)$

L'assioma di unione dice che per ogni y esiste un insieme z i cui elementi sono esattamente gli elementi appartenenti a qualcuno degli elementi di y. Scriveremo $z = \cup_{w \in y} w$.

ZF5(insieme potenza)

$\forall u.\exists z.\forall y.(\forall x.(x \in y \rightarrow x \in u) \leftrightarrow y \in z)$

L'assioma dell'insieme potenza dice che dato un insieme esiste un altro insieme che ha come elementi tutti i sottoinsiemi dell'insieme dato.

ZF6(separazione)

$\forall u.\exists z.\forall x.(x \in z \leftrightarrow (x \in u \wedge \phi(x)))$

L'assioma di separazione dice che data una formula ϕ tutti gli elementi di un insieme u che soddisfino ϕ formano un insieme z ($\{x \in u | \phi(x)\}$).

ZF7(rimpiazzamento)

$\forall u.(\forall x \in u \exists ! z.\phi(x, z, u) \rightarrow \exists Z.\forall x \in u.\exists z \in Z.\phi(x, z, u))$

L'assioma di rimpiazzamento garantisce che se u è un insieme e c'è un modo per assegnare ad ogni insieme $x \in u$ a qualche insieme y allora l'immagine di u sotto tale assegnamento è un insieme.

ZF8(infinito)

$\exists z.\emptyset \in z \wedge \forall x.x \in z \rightarrow x \cup \{x\} \in z$

L'assioma dell'infinito dice che esiste un insieme infinito z.

ZF9(fondazione)

$\forall x(\neg(x = \emptyset) \rightarrow \exists y.(y \in x \wedge \neg\exists z.(z \in x \wedge z \in y)))$ L'assioma di fondazione dice che ogni insieme non vuoto x contiene un elemento y tale che x ey sono disgiunti. Tale assioma si rivelerà estremamente importante nel seguito di questo scritto poichè garantisce che in un insieme non vi siano sequenze discendenti infinite rispetto alla nozione di appartenenza insiemistica.

AC(scelta)

$\forall f.(\forall h \in f.\neg(h = \emptyset) \wedge \forall F \in f.\forall G \in f.(F = G \vee F \cap G = \emptyset)$
$\rightarrow \exists S.\forall F \in f.\exists! s.(s \in S \wedge s \in F))$

L'assioma di scelta dice che data una famiglia di insiemi non vuoti digiunti esiste un insieme che contiene esattamente un elemento di ciascun insieme della famiglia, cioè esiste una funzione di scelta che seleziona un elemento da ogni insieme e costruisce un nuovo insieme a partire dagli elementi scelti.

Mostriamo nel prossimo paragrafo la costruzione degli ordinali all'interno di ZFC.

1.3 Ordinali

Procediamo nella definizione degli ordinali classici a partire dalla definizione di insieme ben ordinato e dalle sue proprietà.

Definizione 1.4 *Un insieme parzialmente ordinato è un insieme M con una relazione < definita su di esso tale che:*

1. $\forall a, b, c \in M.(a < b \wedge b < c) \rightarrow a < c$

In altre parole un insieme è parzialmente ordinato se la relazione < definita su di esso è una relazione transitiva. Mostriamo ora le proprietà che un insieme parzialmente ordinato deve presentare per essere ben ordinato.

Definizione 1.5 *Un insieme ben ordinato è un insieme parzialmente ordinato M con una relazione < definita su di esso tale che ogni suo sottoinsieme non vuoto ha un elemento minimo, i.e.*

$$\forall S \subseteq M.S \neq \emptyset \rightarrow \exists a \in S.\forall s \in S(s \neq a) \rightarrow a < s$$

E' immediato verificare che se M è un insieme ben ordinato allora la relazione < definita su di esso è tricotomica, cioè vale:

$$\forall a, b \in M.a = b \vee a < b \vee b < a$$

Possiamo ora introdurre una relazione fra insiemi ben ordinati.

Definizione 1.6 *Due insiemi ben ordinati (A,$<_A$) e (B,$<_B$) si dicono isomorfi per ordine se e solo se esiste una biezione*

$$f : A \to B$$

tale che sia un morfismo d'ordine, cioè

$$\forall a_1, a_2 \in A.(a_1 <_A a_2) \leftrightarrow f(a_1) <_B f(a_2)$$

Siamo quindi nella condizione di poter dare una nozione di numero ordinale:

Definizione 1.7 *Un numero ordinale (o ordinale) è un qualsiasi elemento di una collezione di insiemi ben ordinati isomorfi per ordine.*

Dobbiamo ora fornire le basi formali per permettere un confronto fra gli ordinali. Diamo infatti la definizione di segmento iniziale di un insieme ben ordinato:

Definizione 1.8 *Un segmento iniziale di un insieme ben ordinato $(M, <)$ è un insieme $M_c = \{m \in M | m < c\}$ per qualche $c \in M$.*

La nozione di segmento iniziale ci permette di dare la seguente definizione di ordine fra ordinali:

Definizione 1.9 *Siano α e β due ordinali corrispondenti agli insiemi ben ordinati A e B rispettivamente. Abbiamo $\alpha < \beta$ se e solo se A è isomorfo per ordine ad un segmento iniziale di B.*

Facciamo a questo punto notare che ogni numero naturale n, costruito nel seguente modo

$$0 = \emptyset$$

$$n = \{0, 1, .., n - 1\},$$

risulta essere un numero ordinale associato ad una classe di insiemi ben ordinati isomorfi per ordine di cardinalità n. E' possibile inoltre dimostrare che l'insieme dei numeri naturali $\omega = \{0, 1, 2, ...\}$ è un ordinale ed in particolare è il primo ordinale transfinito (di cardinalità infinita).
Per caratterizzare i numeri ordinali è ora necessario definire su di essi un'opportuna aritmetica. Definiamo in prima istanza la somma tra due ordinali passando attraverso gli insiemi ben ordinati da loro rappresentati. Possiamo infatti definire la somma d'ordine tra due insiemi ben ordinati nel seguente modo:

Definizione 1.10 *Siano ($M, <_M$) e ($N, <_N$) due insiemi ben ordinati disgiunti. Definita la relazione d'ordine $<$ sulla loro unione come*

$$(a < b) \equiv (\ (a, b \in M \wedge a <_M b) \vee (a, b \in N \wedge a <_N b) \vee (a \in M \wedge b \in N)$$

la somma d'ordine di M e N è M+N≡(M∪N,<).

La somma fra due ordinali si definisce dunque in questo modo:

Definizione 1.11 *Siano α e β due numeri ordinali rappresentati dagli insiemi ben ordinati disgiunti A e B. La somma $\alpha+\beta$ è definita come il numero ordinale della somma d'ordine A+B.*

Definita la somma fra numeri ordinali, possiamo suddividere tali numeri in tre categorie, categorie cui faremo riferimento nel seguito dello scritto. Avremo infatti:

- L'ordinale 0 rappresentato unicamente da $\emptyset$
- Gli ordinali successori, dove α è un ordinale successore se esiste un ordinale β tale che $\alpha = \beta + 1$
- Gli ordinali limite, dove α è un ordinale limite se α è diverso da 0 e non esiste un ordinale β tale che $\alpha = \beta + 1$ o, in altre parole, β è il limite di una successione di ordinali (ad es. $\omega = \lim_{n\to\infty} n$).

In modo analogo alla somma tra ordinali definiamo il prodotto:

Definizione 1.12 *Siano $(M, <_M)$ e $(N, <_N)$ due insiemi ben ordinati disgiunti. Definita la relazione d'ordine $<$ sul loro prodotto cartesiano $M \times N$ come*

$$(a_1, b_1) < (a_2, b_2) \equiv (b_1 <_N b_2) \vee (b_1 = b_2 \wedge a_1 <_M a_2)$$

*per (a_1, b_1),$(a_2, b_2) \in M \times N$ il prodotto d'ordine di M e N è M*N$\equiv$(M$\times$N,$<$).*

Il prodotto fra due ordinali si definisce dunque in questo modo:

Definizione 1.13 *Siano α e β due numeri ordinali rappresentati dagli insiemi ben ordinati disgiunti A e B. Il prodotto $\alpha * \beta$ è definito come il numero ordinale del prodotto d'ordine A*B.*

Per completare l'esposizione dell'aritmetica dei numeri ordinali dobbiamo definire l'operazione di esponenziazione su di essi.

Definizione 1.14 *Sia α un numero ordinale. Definiamo:*

- $\alpha^0 = 1$
- *Se β è un ordinale successore*

$$\alpha^{\beta+1} = \alpha^\beta * \alpha$$

- *Se β è un ordinale limite*

$$\alpha^\beta = \lim_{\gamma<\beta} \alpha^\gamma$$

Come abbiamo visto i numeri ordinali corrispondenti ad insiemi finiti sono equivalenti ai numeri naturali. Ora, i numeri naturali portano con sè un principio di induzione e non è quindi sorprendente che anche i numeri ordinali presentino un principio di induzione. E' possibile infatti dimostrare il seguente principio di induzione transfinita:

Teorema 1.15 (Principio di induzione transfinita)
$\forall P.(\ P(0) \wedge (\forall\beta.P(\beta) \rightarrow P(\beta+1)) \wedge (\forall\alpha.\forall\gamma < \alpha.P(\gamma) \rightarrow P(\alpha))\ ) \rightarrow \forall\delta.P(\delta)$

Per concludere questa sezione enunciamo alcune proprietà dei numeri ordinali minori di ϵ_0 che utilizzeremo nel seguito dello scritto. Ricordiamo prima di tutto che ϵ_0 è l'ordinale definito ponendo

$$\epsilon_0 = \omega^{\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}}$$

dove la torre di esponenti è alta ω, o equivalentemente ϵ_0 è la più piccola soluzione dell'equazione ordinale

$$x = \omega^x.$$

Diamo ora la nozione di primalità di un ordinale:

Definizione 1.16 *Sia $\alpha > 0$ un numero ordinale minore di ϵ_0. Allora α si dice primo o(componente prima) se se solo se*

$$\forall\xi < \alpha.\xi + \alpha = \alpha$$

A partire dalla definizione è possibilire dimostrare il seguente teorema:

Teorema 1.17 *Ogni ordinale $\alpha > 0$ minore di ϵ_0 è la somma di un numero finito di componenti prime non crescenti e tale decomposizione è unica.*

Dunque ogni ordinale maggiore di 0 e minore di ϵ_0 presenta una forma univocamente determinata che lo identifica. Raffiniamo questo risultato passando attraverso un teorema che possiamo dimostrare a partire dalla nozione di componente prima.

Teorema 1.18 *Le componenti prime minori di ϵ_0 sono potenze di ω e viceversa ogni potenza di ω è una componente prima.*

Mettendo insieme i risultati dei due precedenti teoremi otteniamo il seguente teorema.

Teorema 1.19 (Forma normale) *Ogni ordinale α minore di ϵ_0 può essere rappresentato univocamente come*

$$\alpha = \omega^{\alpha_1}m_1 + \omega^{\alpha_2}m_2 + ... + \omega^{\alpha_k}m_k$$

dove k e $m_1, m_2, ..., m_k$ sono numeri naturali e $\alpha > \alpha_1 > \alpha_2 > ... > \alpha_k$.

Diremo che un ordinale α minore di ϵ_0 è in forma normale se presenta la forma sopra esposta dove gli esponenti $\alpha_1, \alpha_2, ..., \alpha_k$ sono anch'essi in forma normale. Vedremo nel prossimo capitolo una classica applicazione degli ordinali minori di ϵ_0 nella dimostrazione del teorema di Goodstein.

Capitolo 2

Dimostrazione classica del teorema di Goodstein

2.1 Cenni storici

Possiamo trovare una prima dimostrazione del teorema di Goodstein in [Goodstein44]. In tale articolo Goodstein sviluppa un dimostrazione del teorema a partire dalle pubblicazioni sulla consistenza dell'aritmetica di Gentzen, pubblicazioni in cui assume una notevole importanza il fatto che una sequenza decrescente di ordinali minori di ϵ_0 termini. Il teorema assume una notevole importanza quando in [KirbyParis82] Kirby e Paris mostrano che il Teorema di Goodstein è una delle famose proposizione 'vere', ma non dimostrabili di cui parlava il teorema di incompletezza di Godel. La proposizione di Goodstein infatti, seppur esprimibile all'interno dell'aritmetica di Peano (PA), necessita degli strumenti della teoria degli insiemi per essere dimostrata. Nel seguito del capitolo faremo riferimento alla dimostrazione del teorema fornita in [KirbyParis82].

2.2 Il teorema di Goodstein

Prima di fornire gli strumenti formali che portano alla dimostrazione del teorema, cerchiamo di enunciarne il contenuto. Il teorema afferma che una sequenza di naturali (chiamata per ovvie ragioni sequenza di Goodstein) converge a zero. Tale sequenza è parametrica su un naturale m chiamato base e un naturale p che corrisponde al primo elemento della successione. La successione si sviluppa nel seguente modo:

- Si scrive p in forma normale di Cantor, cioè si scrive il numero come somma di potenze di m e si ripete ricorsivamente l'operazione sugli esponenti delle potenze. Ad es. supponendo $m = 2$ e $p = 9$, la forma normale di Cantor del numero p è

$$p = 2^3 + 2^0 = 2^{2^1+2^0} + 2^0$$

- Si sostituisce ad ogni occorrenza di m nella forma normale di Cantor di p il naturale $m+1$ e si sottrae 1 dalla nuova somma. Il numero naturale così ottenuto è il nuovo elemento della successione. Nel caso dell'esempio precedente

$$p' = 3^{3^1+3^0} + 3^0 - 1 = 81$$

- Si ripete il procedimento descritto a partire dalla base $m+1$ e dal naturale calcolato fino a che non si raggiunge lo 0.

Il problema è dunque: 'è possibile che tale funzione ad un certo punto decresca e converga a 0?'. E' infatti immediato notare che nei suoi punti iniziali la funzione cresce molto rapidamente. Facendo riferimento all'esempio precedente, la sequenza si sviluppa nel seguente modo:

$$\{9, 81, 1023, ...\}$$

Nel prossimo paragrafo formalizzeremo i concetti espressi e daremo una dimostrazione del teorema.

2.3 Dimostrazione del teorema di Goodstein

Iniziamo la dimostrazione del teorema definendo formalmente la funzione di Goodstein. Definiamo anzitutto una funzione $f_{n,base}(x) : \omega + 1 \rightarrow \epsilon_0$ che rimpiazza ogni correnza di *base* presente in un n in forma normale di Cantor con x, ovvero con un naturale o con l'ordinale ω:

$$\begin{aligned} f_{0,base}(x) &= 0 \\ f_{n,base}(x) &= \sum_{i=0}^{k} x^{f_{\gamma_i,base}(x)} \mu_i \end{aligned}$$

dove k, γ_i, μ_i sono dati dalla rappresentazione in forma normale di $n = \sum_{i=0}^{k} base^{\gamma_i} \mu_i$. Possiamo quindi definire la funzione $step_i : \omega \rightarrow \omega$ che permette di passare dall'elemento i+1-esimo di una sequenza di Goodstein all'elemento i-esimo della sequenza seguendo il procedimento descritto nel paragrafo precedente:

$$\begin{aligned} step_i(0) &= 0 \\ step_i(n) &= f_{n,i}(i+1) - 1 \end{aligned}$$

Definita la funzione $step_i$ diamo una nozione formale di sequenza di Goodstein parametrizzata sulla base m e sul naturale di partenza p:

$$\begin{aligned} goodstein_{m,p}(0) &= p \\ goodstein_{m,p}(n+1) &= step_{n+m}(goodstein_{m,p}(n)) \end{aligned}$$

Come abbiamo precedentemente indicato, l'osservazione dello sviluppo della sequenza dall'unico punto di vista dei numeri naturali prodotti non sembra fornire sufficienti informazioni per arrivare alla dimostrazione di terminazione. Perciò cerchiamo di astrarre dai naturali che si presentano nella sequenza la particolare struttura offerta dalla loro forma normale di Cantor. E' facile tuttavia notare che le varie forme normali di Cantor si differenziano per la base di rappresentazione usata e risulta quindi necessario tentare di uniformarle 'dimenticando' tale base di rappresentazione. Possiamo fare questo sostituendo ogni possibile base con un numero maggiore di ogni possibile base naturale m di rappresentazione: ω. Cominciamo definendo la seguente funzione $< \alpha >: \omega \rightarrow \epsilon_0$ parametrica sull'ordinale α:

$$
\begin{aligned}
< 0 > (n) &= 0 \\
< \alpha + 1 > (n) &= \alpha \\
< \omega^{\delta}(\alpha + 1) > (n) &= \omega^{\delta}\alpha + \omega^{<\delta>(n)}n + < \omega^{<\delta>(n)} > (n)
\end{aligned}
$$

dove è possibile dimostrare che $\omega^{\delta}(\alpha + 1)$ è una forma univocamente determinabile di ogni ordinale limite transfinito. A partire dalla definizione della funzione $< \alpha >$ possiamo ottenere il seguente risultato:

Teorema 2.4
$\forall \alpha < \epsilon_0 . \forall n : N . \alpha > 0 \rightarrow < \alpha > (n) < \alpha$

Il teorema ci permette quindi di ottenere una sequenza decrescente di ordinali, che chiameremo Goodstein Predecessor Sequence (GPS), applicando ripetutamente la funzione $< \alpha >$:

$$< ... << \alpha_1 > (n_1) > (n_2) .... > (n_k)$$

Dobbiamo ora domandarci che rapporto vi sia tra la sequenza discendente di ordinali che abbiamo definito e la sequenza di Goodstein. Definiamo ora una funzione che ci permette di ottenere un numero in forma normale di Cantor rispetto alla base ω a partire da un numero in forma normale di Cantor rispetto ad una base i.

$$
\begin{aligned}
O_i(0) &= 0 \\
O_i(n) &= f_{n,i}(\omega)
\end{aligned}
$$

Possiamo quindi dimostrare i seguenti teoremi che mostrano la relazione sussistente fra la funzione $< \alpha >$, O_i e $step_i$:

Teorema 2.5
$\forall m \in \omega . \forall n > 1 \in \omega . \alpha = O_{n+1}(m) \rightarrow O_{n+1}(m - 1) =< \alpha > (n)$

Teorema 2.6
$\forall m \in \omega . \forall n > 1 \in \omega . < O_n(m) > (n) = O_{n+1}(step_n(m))$

Facendo riferimento alle due equivalenze portate dai precedenti teoremi, è possibile ora definire una sequenza γ di ordinali 'parallela' ad una sequenza di Goodstein fissata e quindi mostrare che la sequenza definita è equivalente alla Goodstein Predecessor Sequence. Infatti, definita in tal modo la sequenza γ

$$\begin{aligned}
\gamma_0 &= O_i(goodstein_{i,p}(0)) \\
\gamma_{n+1} &= O_{n+1+i}(goodstein_{i,p}(n+1))
\end{aligned}$$

è possibile dimostrare che tale sequenza è equivalente ad una Goodstein Predecessor Sequence:

$$\begin{aligned}
O_{n+1+i}(goodstein_{i,p}(n+1)) &= O_{n+1+i}(step_{n+i}(goodstein_{i,p}(n))) \\
&= < O_{n+i}(goodstein_{i,p}(n)) > (n+i) \\
&= << O_{n+i-1}(goodstein_{i,p}(n-1)) > (n+i-1) > (n+i) \\
&. \\
&. \\
&. \\
&= < ... << O_i(goodstein_{i,p}(0)) > (i) > (i+1) ... > (n+i) \\
&= < ... << \gamma_0 > (i) > (i+1) ... > (n+i)
\end{aligned}$$

Abbiamo dunque dimostrato che ogni sequenza di Goodstein può essere associata ad una sequenza di ordinali 'parallela' che abbiamo dimostrato essere decrescente. Per concludere la dimostrazione dobbiamo quindi dimostrare che se una sequenza di ordinali è decrescente è anche finita. Enunciamo quindi il teorema e ne forniamo una semplice dimostrazione.

Teorema 2.7
Sia Φ *una collezione di ordinali. Allora*
$\forall f : N \rightarrow \Phi . \exists i, j \in N | (i < j \wedge f(j) \geq f(i))$
Dim.
Sia f *una qualunque funzione da* N *a* Φ *e consideriamo l'insieme* $\{f(i) \in \Phi | i \in N\}$. *Per l'assioma di fondazione tale insieme non può contenere sequenze discendenti infinite rispetto alla relazione di appartenenza e quindi devono esistere due indici* $i, j \in N$ *tali che* $i < j$ *ma* $f(j) \notin f(i)$ *cioè non vale* $f(j) < f(i)$.

Infine, osservando che se per ogni k naturale avessimo $goodstein_{i,p}(k) \neq 0$ allora la sequenza di ordinali associata γ risulterebbe essere una sequenza decrescente infinita (entrando così in contraddizione con il teorema 2.7), possiamo concludere la dimostrazione del teorema di Goodstein.

Teorema 2.8
$\forall i, p \in N . \exists k \in N . goodstein_{i,p}(k) = 0$

Nel capitolo 5 analizzeremo un possibile sviluppo costruttivo di questa dimostrazione.

Capitolo 3

Teoria dei tipi di Martin-Löf

3.1 Cenni storici

A partire dai lavori di Erret Bishop sulla fondazione di una matematica costruttiva essenzialmente algoritmica [Bishop67], Per Martin-Löf dà vita, all'inizio degli anni '70, alla cosiddetta Intuitionistic Type Theory (ITT) o Martin-Löf's Type Theory (ML). Una prima versione impredicativa di ITT è infatti presentata in [Martin-Löf71] e, in seguito alla scoperta del paradosso di Girard [Girard72], la teoria viene riproposta in una veste predicativa in [Martin-Löf75]. E' possibile trovare una esposizione completa di ITT in [Martin-Lof84] ed una discussione su alcuni fondamenti filosofici della teoria in [Martin-Löf96]. Lo scopo principale di ITT è fornire un sistema formale all'interno del quale sviluppare matematica costruttiva, basandosi sul paradigma 'propositions as types' ovvero sull'idea che i tipi di un sistema formale possano rappresentare proposizioni (leggi anche specifiche di programmi) e gli oggetti di un determinato tipo possano rappresentare dimostrazioni (leggi anche programmi) di determinate proposizioni.

3.2 Proposizioni e giudizi

La distinzione tra proposizione e giudizio costituisce il nucleo fondazionale di ITT. Una proposizione è ciò che possiamo costruire a partire da variabili, costanti e operatori logici ($\perp, \rightarrow, \wedge, \vee, \forall, \exists$) e può avere una dimostrazione. All'interno del paradigma 'propositions as types', una proposizione corrisponde ad un tipo inteso come l'insieme degli elementi che corrispondono a dimostrazioni di tale proposizione. Una proposizione non ha dunque, come accade in ambito classico, un valore di verità associato, ma ha o meno una dimostrazione. L' intepretazione dei vari tipi di proposizione si può quindi riassumere nella seguente tabella:

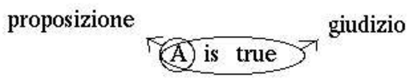
Una dimostrazione della proposizione	è data da
$\perp$	-
A $\wedge$ B	una dimostrazione di A e una dimostrazione di B
A $\vee$ B	una dimostrazione di A o una dimostrazione di B
A $\rightarrow$ B	una funzione che trasforma una qualsiasi dimostrazione di A in una dimostrazione di B
$\forall x : A.B(x)$	una funzione che da un elemento arbitrario a di A produce una dimostrazione di B(a)
$\exists x : A.B(x)$	un elemento arbitrario a di A ed una dimostrazione di B(a)

dove la prima riga della tabella dice che il falso ($\perp$) è un tipo in ITT e che tale tipo non ha dimostrazioni.
Sostituendo quindi alle proposizioni i tipi corrispondenti ed adottando come linguaggio per le dimostrazioni il λ-calcolo tipato semplice è possibile raffinare la tabella precedente nel seguente modo:

Un elemento del tipo	è dato da
$\perp$	-
A $\times$ B	$< a, b >$, dove a è una dimostrazione di A e b è una dimostrazione di B
A $\oplus$ B	inl(a) dove a è una dimostrazione di A o inr(b) dove b è una dimostrazione di B
A $\rightarrow$ B	$\lambda x.b(x)$ dove $b(a)$ è una dimostrazione di B se a è una dimostrazione di A
$\forall x : A.B(x)$	$\lambda x.b(x)$ dove $b(a)$ è una dimostrazione di B(a) se a è un elemento di A

$\exists x : A.B(x)$	$< a, b >$, dove a è un elemento di A e b è una dimostrazione di B(a)

Un giudizio è una asserzione su una proposizione (o su un tipo), ad es:



In ITT vengono utilizzate quattro forme di giudizio sulle proposizioni:

- Giudizi che asseriscono che una proposizione è un insieme od un tipo :

A : type

- Giudizi che asseriscono che due tipi sono uguali :

A=B

- Giudizi che asseriscono che un'espressione è un elemento di un tipo :

a : A

- Giudizi che asseriscono che due elementi di uno stesso tipo sono uguali:

a = b : A

Infine la distinzione fra giudizi e proposizioni è data dalla nozione di dimostrazione definita su di essi. La dimostrazione di un giudizio è data da una derivazione nello stile della deduzione naturale, mentre la dimostrazione di una proposizione è data da uno qualsiasi degli elementi del tipo corrispondente a tale proposizione. Mostreremo nel prossimo paragrafo la tecnica per la definizione di un tipo e dei suoi elementi costitutivi.

3.3 Tipi

Descriviamo in questo paragrafo il sistema di regole che permette la definizione di un tipo.

- Regole di Formazione. Le regole di formazione dicono come formare un nuovo tipo e quando due tipi costruiti in tal modo sono uguali. Ad es. il tipo prodotto cartesiano $(A \times B)$ corrispondente alla proposizione $(A \wedge B)$ presenta le seguenti regole di formazione:

$$\frac{A : type \quad B : type}{A \times B : type} \qquad \frac{A = C \quad B = D}{A \times B = C \times D}$$

- Regole di Introduzione. Le regole di introduzione dicono come costruire gli elementi canonici di un tipo e quando tali elementi sono uguali. Facendo riferimento al tipo $(A \times B)$, le regole di introduzione sono le seguenti:

$$\frac{a : A \quad b : B}{< a, b >: A \times B} \qquad \frac{a = c : A \quad b = d : B}{< a, b >=< c, d >: A \times B}$$

- Regole di Eliminazione. Le regole di eliminazione dicono come definire funzioni sugli elementi di un tipo e quando tali funzioni sono equivalenti. Facendo riferimento al tipo $(A \times B)$, le regole di eliminazione sono le seguenti:

$$\frac{c : A \times B \quad d : A \to B \to C}{split(c, d) : C} \qquad \frac{c = e : A \times B \quad d = d' : A \to B \to C}{split(c, d) = split(e, d') : C}$$

- Regole di Equivalenza. Le regole mostrano come stabilire una nozione di equivalenza fra i termini prodotti dalla regola di eliminazione di un tipo e gli altri termini del linguaggio. Facendo riferimento al tipo $(A \times B)$, la regola di equivalenza è la seguente:

$$\frac{a : A \quad b : B \quad d : A \to B \to C}{split(< a, b >, d) = d(a)(b) : C}$$

- Regole di Riduzione. Le regole di riduzione rendono esplicito il processo computazionale implicito nelle regole precedenti. Facendo riferimento al tipo $(A \times B)$, le regole di riduzione sono le seguenti:

$$\frac{a \Rightarrow g_a \quad b \Rightarrow g_b}{< a, b >\Rightarrow< g_a, g_b >} \qquad \frac{c \Rightarrow< a, b > \quad d(a)(b) \Rightarrow g}{split(c, d) \Rightarrow g}$$

E' immediato notare che il sistema necessita di alcuni tipi 'primitivi', ovvero di tipi che non corrispondano alle proposizioni comunemente intese, ma siano semplicementi insiemi di oggetti con determinate proprietà. Tramite le regole appena esposte è infatti possibile definire tipi diversi da $A \times B$, come ad es. il tipo induttivo dei naturali N. Tale tipo presenta due regole per costruire gli oggetti:

$$\frac{}{0 : N} \qquad \frac{n : N}{s(n) : N}$$

E' associata a tali regole la seguente regola di eliminazione ed è possibile mostrare che, per ogni tipo induttivamente generato, la regola di eliminazione corrisponde al principio di induzione sugli oggetti di quel tipo:

$$\frac{c : N \quad d : \gamma \quad e : N \to (\ \gamma \to \gamma\ )}{Natrec(c, d, e) : \gamma}$$

Infatti l'elemento d insieme alla funzione e che prende un naturale x ed una dimostrazione di $\gamma(x)$ e restituisce una dimostrazione di $\gamma(s(x))$, rappresenta direttamente una versione costruttiva del principio di induzione classico. Più in generale è possibile mostrare [Dybjer91] che le regole di eliminazione sono univocamente deducibili dalle regole di introduzione e questo giustificherà le regole di eliminazione che stabiliremo per i nuovi tipi presentati nello scritto. Forniremo infatti nell' Appendice A uno sviluppo in ITT del framework per gli ordinali che presenteremo nel prossimo capitolo.

Capitolo 4

Un Framework costruttivo per gli ordinali

Come abbiamo visto nel capitolo 1 ogni ordinale $\alpha < \epsilon_0$ può essere rappresentato univocamente come

$$\alpha = \omega^{\alpha_1} m_1 + \omega^{\alpha_2} m_2 + ... + \omega^{\alpha_k} m_k$$

dove k e $m_1, m_2, ..., m_k$ sono numeri naturali e $\alpha > \alpha_1 > \alpha_2 > ... > \alpha_k$. Da questa particolare rappresentazione di un ordinale (che d'ora in poi chiameremo forma normale) nasce l'idea di una definizione induttiva degli ordinali di Von Neumann minori di ϵ_0. Possiamo infatti pensare ogni ordinale minore di ϵ_0 come una tripla $< n, \gamma, \delta >$ dove n è il coefficiente naturale del primo elemento della sommatoria, γ è l'esponente del primo elemento della sommatoria rappresentato in forma normale e δ è l'ordinale corrispondente alla sommatoria privata del primo elemento, rappresentato in forma normale. Nel caso in cui avessimo

$$\alpha = \omega^{\alpha_1} m_1 + \omega^{\alpha_2} m_2 + ... + \omega^{\alpha_k} m_k,$$

otterremmo $n = m_1$,$\gamma = NF(\alpha_1)$ e $\delta = NF(\omega^{\alpha_2} m_2 + ... + \omega^{\alpha_k} m_k)$ dove con NF indichiamo la funzione di conversione in forma normale. Facendo riferimento allo schema di definizione induttiva presentato nel capitolo 3 diamo ora una veste formale alla nostra idea per la rappresentazione di un ordinale minore di ϵ_0. E' ovvio che una buona definizione induttiva necessiti di un caso base o meglio di un'entità da cui partire per la costruzione di tutti gli ordinali. Definiamo perciò l'ordinale zero:

$$\frac{}{0_{O^{<\epsilon_0}} : O^{<\epsilon_0}}$$

Ottenuto l'ordinale 0 possiamo costruire tutti gli ordinali sfruttando l'idea precedentemente esposta:

$$\frac{n : N \quad \alpha : O^{<\epsilon_0} \quad \beta : O^{<\epsilon_0}}{< n, \alpha, \beta >: O^{<\epsilon_0}}$$

Se volessimo ad esempio costruire l'ordinale $\omega^3 2 + \omega^1$, dovremmo procedere nel seguente modo:

1. Generiamo l'ordinale $0_{O<\epsilon_0}$ utilizzando l'assioma corripondente.
2. Applichiamo la regola di costruzione con $\alpha = \beta = 0_{O<\epsilon_0}$ e $n = 3$ per ottenere l'ordinale 3 in forma normale: $< 3, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >$.
3. Applichiamo la regola di costruzione con $\alpha = \beta = 0_{O<\epsilon_0}$ e $n = 1$ per ottenere l'ordinale 1 in forma normale: $< 1, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >$.
4. Applichiamo la regola di costruzione con $\alpha =< 1, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >$, $\beta = 0_{O<\epsilon_0}$ e $n = 1$ per ottenere l'ordinale ω^1 in forma normale: $< 1, < 1, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >, 0_{O<\epsilon_0} >$.
5. Applichiamo la regola di costruzione con $\alpha =< 3, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >$, $\beta =< 1, < 1, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >, 0_{O<\epsilon_0} >$ e $n = 2$ per ottenere l'ordinale $\omega^3 2 + \omega^1$ in forma normale: $< 2, < 3, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >, < 1, < 1, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >, 0_{O<\epsilon_0} >>$.

E' immediato mostrare che la nostra definizione genera (potenzialmente) tutti gli ordinali minori di ϵ_0 e, purtroppo, è altresì immediato notare che la nostra definizione genera dei termini che non rispettano le proprietà della forma normale. Infatti, facendo riferimento all'esempio precedente, possiamo costruire l'ordinale $\omega^1 + \omega^3 2$ applicando la regola di costruzione ad $\alpha =< 1, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >$, $\beta =< 2, < 3, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >, 0_{O<\epsilon_0} >$ e $n = 1$ violando così l'ordine degli esponenti dei termini della sommatoria. E' inoltre possibile generare l'ordinale $< 0, 0_{O<\epsilon_0}, 0_{O<\epsilon_0} >$ che nella nostra intuizione degli ordinali minori di ϵ_0 non dovrebbe poter essere generato poichè si sovrappone all'ordinale $0_{O<\epsilon_0}$. Risulta pertanto necessaria la definizione di una funzione che permetta di trasformare un ordinale non in forma normale nell'ordinale corrispondente in forma normale, cioè di una funzione che ordini i termini della sommatoria in base all'esponente e che unisca (sommi) i termini con lo stesso esponente.
Prima di impegnarci in tale compito, vogliamo indagare le caratteristiche essenziali del nuovo tipo da noi definito e nello specifico vogliamo individuare possibili relazioni esistenti fra i numeri creati e i numeri naturali. Il lettore più attento avrà infatti notato che nella nostra definizione degli ordinali minori di ϵ_0 non compare in alcuna occasione il primo ordinale transfinito ω in totale conformità con il rifiuto costruttivo di un infinito pensato attualmente. Possiamo quindi asserire che la nostra definizione dei numeri ordinali astrae dai costituenti della sommatoria per parlare solo della forma di tale sommatoria, in altre parole della struttura in cui poniamo ω per costruire i nostri ordinali. E' possibile ravvisare una struttura simile associata ai numeri naturali? La risposta è affermativa. Infatti, come abbiamo mostrato nel capitolo 2, ogni numero naturale m ha un'unica rappresentazione in forma normale rispetto ad una base fissata n, cioè esistono $m_0, m_1, ..., m_k < n$ e $e_k > e_{k-1} > ... > e_0$ naturali ed univocamente determinati tali che

$$m = n^{e_k} m_k + n^{e_{k-1}} m_{k-1} + ... + n^{e_0} m_0$$

E' evidente la somiglianza fra la rappresentazione degli ordinali minori di ϵ_0 e la rappresentazione dei numeri naturali scritti in tale forma. Procediamo pertanto alla definizione di un nuovo insieme di oggetti, parametrico sulla base di rappresentazione m, che chiameremo insieme dei numeri di Cantor in onore al fatto che un numero naturale m che presenta la forma sopra esposta anche per gli esponenti dei termini della sommatoria si dice essere in forma normale di Cantor. Definiamo quindi il numero di Cantor 0 parametrico su m:

$$\frac{}{0_m : Cantor(m)}$$

A partire dallo 0 possiamo costruire tutti i numeri di Cantor utilizzando la seguente regola:

$$\frac{n : N \quad \alpha : Cantor(m) \quad \beta : Cantor(m)}{< n, \alpha, \beta >_m : Cantor(m)}$$

Si può notare che i numeri di Cantor da noi definiti presentano gli stessi problemi degli ordinali minori di ϵ_0 per ciò che riguarda le proprietà della forma normale. In aggiunta, la nostra definizione permette di violare l'ulteriore vincolo posto sui numeri, ovvero il vincolo che ogni coefficiente naturale associato ad un elemento della sommatoria sia minore del parametro m. Dobbiamo perciò definire anche in questo caso una funzione che porti in forma normale (di Cantor) ogni numero. Questo compito risulta tuttavia meno gravoso poichè i nostri numeri di Cantor sono essenzialmente numeri naturali e diviene pertanto possibile definire le funzioni su di essi tramite funzioni sugli stessi numeri naturali. Mostreremo nel seguito che le funzioni operanti sui numeri di Cantor possono costituire la base per la maggior parte delle funzioni definibili sugli ordinali da noi creati. Procediamo ora nella definizione di alcune funzioni necessarie per stabilire la relazione sussistente fra numeri naturali e numeri di Cantor. Per prima cosa mostriamo come si possa tradurre un numero di Cantor in un numero naturale tramite la funzione $cantor_m 2n$:

$$\begin{aligned} cantor_m 2n(0_m) &= 0 \\ cantor_m 2n(< n', \alpha, \beta >_m) &= n' * m^{cantor_m 2n(\alpha)} + cantor_m 2n(\beta) \end{aligned}$$

Definiamo ora simultaneamente[1] tre funzioni che ci permettono di tradurre i numeri naturali in numeri di Cantor in forma normale. La funzione $n2cantor_m$ mappa i numeri naturali in numeri di Cantor appoggiandosi alla funzione inc_m.

$$\begin{aligned} n2cantor_m(0) &= 0_m \\ n2cantor_m(s(k)) &= inc_m(n2cantor_m(k)) \end{aligned}$$

La funzione inc_m incrementa di una unità un qualsiasi numero di Cantor (facendo riferimento al valore del numero di Cantor rispetto alla sua traduzione nei

[1] Tale definzione per 'ricorsione simultanea' non è immediatamente traducibile in ITT. E' tuttavia possibile tradurre tale 'ricorsione simultanea' in uno schema di ricorsione semplice.

naturali):

$$\begin{array}{rcl} inc_m(0_m) & = & <1, 0_m, 0_m>_m \\ inc_m(<n', \alpha, \beta>_m) & = & if\ not\ nf_m(x) = x\ then\ <1, 0_m, <n', \alpha, \beta>_m>_m \\ & & else\ if\ \alpha = snd(inc_m(\beta))\ then \\ & & \quad\quad if\ n' < m-1\ then\ <n'+1, \alpha, 0_m>_m \\ & & \quad\quad else\ <1, inc_m(\alpha), 0_m>_m \\ & & \quad else\ <n', \alpha, inc_m(\beta)>_m \end{array}$$

dove snd è la funzione che restituisce il secondo elemento della tripla corrispondente ad un numero di Cantor ($snd(0_m) = 0_m$). La funzione di forma normale nf_m permette di applicare con diverso esito la funzione inc_m se il numero di Cantor è o non è in forma normale. Diciamo infatti che un termine γ è in forma normale se $nf_m(\gamma) = \gamma$.

$$nf_m(<n', \alpha, \beta>_m) \quad = \quad n2cantor_m(cantor_m2n(<n', \alpha, \beta>_m))$$

Per dimostrare che la funzione di forma normale sopra definita rispetta tutte i vincoli imposti su un numero in forma normale di Cantor, è in prima istanza necessario dimostrare che le funzioni $nat2cantor_m, cantor_m2n$ si comportano 'bene' ovvero che le operazioni s ed inc_m sono equivalenti rispetto alle due funzioni. E' infatti possibile dimostrare i seguenti teoremi.

Teorema 4.1
$\forall m : N.\forall n : N.inc_m(n2cantor_m(n)) = n2Cantor_m(s(n))$.

Teorema 4.2
$\forall m : N.\forall x : Cantor(m).cantor_m2n(inc_m(x)) = s(cantor_m2n(x))$.

Immediato corollario dei due teoremi è il fatto che la relazione fra numeri naturali e numeri di Cantor sia una relazione biettiva rispetto alla nozione di equivalenza fra numeri naturali.

Corollario 4.3 $\forall m : N.\forall n : N.cantor_m2n(n2cantor_m(n)) = n$

Si può inoltre osservare che sussiste una relazione biettiva fra numeri naturali e numeri di Cantor rispetto alla nozione di equivalenza fra numeri Cantor restringendo l'insieme dei numeri di Cantor ai numeri in forma normale. Questo deriva dal fatto che, per definizione di nf_m, un termine γ è in forma normale se $n2cantor_m(cantor_m2n(\gamma)) = \gamma$. In più facciamo notare che ogni numero di Cantor ottenuto tramite l'applicazione di $n2cantor_m$ ad un numero naturale k è in forma normale. Infatti, applicando il Corollario 4.3, otteniamo $nf_m(n2cantor_m(k)) = n2cantor_m(cantor_m2n(n2cantor_m(k))) = n2cantor_m(n)$. Procediamo dunque alla dimostrazione delle proprietà dei numeri di Cantor in forma normale, tenendo presente il fatto appena mostrato che, in ultima analisi, ci dice che dimostrare una proposizione su $n2cantor_m(k)$ equivale a dimostrare una proposizione analoga sui numeri di Cantor in forma normale. Possiamo infatti dimostrare i seguenti teoremi per induzione su n

Teorema 4.4
$\forall n : N.\forall m : N.(n! = 0 \ \wedge \ snd(n2cantor_m(n))! = 0) \rightarrow snd(n2cantor_m(n)) > snd(trd(n2cantor_m(n)))$

Teorema 4.5
$\forall n : N.\forall m : N.(n! = 0 \ \wedge \ snd(n2cantor_m(n)) = 0) \rightarrow trd(n2cantor_m(n)) = 0$

Teorema 4.6
$\forall n : N.\forall m : N.fst(n2cantor_m(n)) < m$

dove la funzione di confronto $<$ tra numeri di Cantor è la seguente

$$\begin{array}{rcl} 0_m \ < \ 0_m & = & false \\ 0_m \ < \ (< n', \alpha, \beta >_m) & = & true \\ (< n', \alpha, \beta >_m) \ < \ 0_m & = & false \\ (< n', \alpha, \beta >_m) \ < \ (< n'', \gamma, \delta >_m) & = & if\ \alpha \ < \ \gamma\ then\ true \\ & & else\ if\ \alpha = \gamma\ then \\ & & \quad\quad if\ n' < n''\ then\ true \\ & & \quad\quad else\ if\ n' = n''\ then\ \beta \ < \ \delta \\ & & \quad\quad\quad else\ false \\ & & \quad else\ false \end{array}$$

e fst e trd sono le funzioni che restituiscono rispettivamente il primo ed il secondo elemento di una tripla corrispondente ad un numero di Cantor. Il primo teorema dice che un numero di Cantor generato da $n2cantor_m$ rispetta l'ordine degli esponenti dei termini della sommatoria, mentre il secondo teorema garantisce che per un numero di Cantor generato da $n2cantor_m$ avente la forma $< n', 0_m, \beta >$, vale $\beta = 0_m$. L'ultimo teorema asserisce che i coefficienti naturali di ogni termine della sommatoria, corrispondente ad un numero di Cantor generato da $n2cantor_m$, sono minori della base di rappresentazione m. Questi teoremi hanno delle immediate conseguenze sulle proprietà dei numeri di Cantor in forma normale. E' infatti immediato dimostrare i seguenti corollari, sfruttando l'interessante fatto che abbiamo precedentemente osservato.

Corollario 4.7
$\forall m : N.\forall x : Cantor(m).(nf_m(x) = x \ \wedge \ x! = 0 \ \wedge \ snd(x)! = 0) \rightarrow \ snd(x) > snd(trd(x))$

Corollario 4.8
$\forall m : N.\forall x : Cantor(m).(nf_m(x) = x \ \wedge \ x! = 0 \ \wedge \ snd(x) = 0) \rightarrow \ trd(x) = 0$

Corollario 4.9
$\forall m : N.\forall x : Cantor(m).(nf_m(x) = x) \rightarrow \ fst(x) < m$

Abbiamo dunque mostrato che i numeri di Cantor da noi definiti soddisfano le proprietà richieste. Mostriamo ora come sia possibile dare una nozione di forma normale per gli ordinali minori di ϵ_0 a partire dalla nozione data per i numeri di Cantor. Cominciamo definendo una funzione di traduzione da numeri di Cantor (con base generica di rappresentazione m) a ordinali minori di ϵ_0.

$$\begin{aligned} cantor_m2ord(0_m) &= 0_{O^{<\epsilon_0}} \\ cantor_m2ord(< n', \alpha, \beta >_m) &= < n', cantor_m2ord(\alpha), cantor_m2ord(\beta) > \end{aligned}$$

Come si può notare, la funzione di traduzione trasporta da un tipo all'altro la struttura degli oggetti e risulta pertanto naturale definire in modo analogo la funzione di traduzione da ordinali minori di ϵ_0 a numeri di Cantor.

$$\begin{aligned} ord2cantor_m(0_{O^{<\epsilon_0}}) &= 0_m \\ ord2cantor_m(< n', \alpha, \beta >) &= < n', ord2cantor_m(\alpha), ord2cantor_m(\beta) >_m \end{aligned}$$

Definite in tal modo le funzioni di traduzione, possiamo dimostrare i seguenti teoremi.

Teorema 4.10
$\forall m : N.\forall x : Cantor(m).ord2cantor_m(cantor_m2ord(x)) = x$

Teorema 4.11
$\forall m : N.\forall x : O^{<\epsilon_0}.cantor_m2ord(ord2cantor_m(x))) = x$

Ora, prima di indicare una nozione formale di forma normale di un ordinale minore di ϵ_0, esponiamo l'idea alla base di tale nozione. Appurato infatti, tramite i precedenti teoremi, che l'applicazione consecutiva di $ord2cantor_m$ e $cantor_m2ord$ in qualsiasi ordine porta alla funzione identità, sembra ragionevole calcolare la forma normale di un ordinale tramite la funzione già definita sui numeri di Cantor e le funzioni di traduzione sopra definite. Rimane tuttavia aperta una questione: quale base di rappresentazione m utilizzare per le funzioni $ord2cantor_m$ e $cantor_m2ord$? Il calcolo di un m minimo per cui per un ordinale γ in forma normale valga $cantor_n2ord(nf_m(ord2cantor_n(\gamma)))$ potrebbe risultare piuttosto complesso. Vogliamo infatti trovare un m abbastanza grande per evitare cambi di base dovuti all'aumentare del coefficiente naturale di un termine della sommatoria quando passiamo dall'ordinale (che ovviamente non richiede cambi di base poichè $\forall n : N.n < \omega$) al numero di Cantor di traduzione. Possiamo dunque definire una funzione di calcolo molto più semplice rilassando il problema. Garantiamo pertanto la bontà dell'm calcolato sommando tutti i coefficienti naturali presenti nella struttura dell'ordinale ed osservando che questo nuovo coefficiente sarà certamente maggiore di qualunque coefficiente prodotto dall'unione dei termini delle sommatorie corrispondenti all'ordinale o ai suoi esponenti.

$$\begin{aligned} base(0_{O^{<\epsilon_0}}) &= 2 \\ base(< n', \alpha, \beta >) &= n' + base(\alpha) + base(\beta) \end{aligned}$$

In generale, per preservare la generalità della definizione, diremo che un termine γ per cui valga $cantor_n 2ord(nf_m(ord2cantor_n(\gamma)))$ è in forma m-normale. Definiamo perciò in tal modo la funzione di forma m-normale.

$$\begin{array}{rcl} nf(0_{O^{<\epsilon_0}})(m) & = & 0_{O^{<\epsilon_0}} \\ nf(< n', \alpha, \beta >)(m) & = & cantor_m 2ord(nf_m(ord2cantor_m(< n', \alpha, \beta >))) \end{array}$$

Dimostriamo ora le proprietà degli ordinali in forma m-normale sfruttando i risultati analoghi mostrati per i numeri di Cantor.

Teorema 4.12
$\forall m : N.\forall x : O^{<\epsilon_0}.(nf(x)(m) = x \ \wedge \ x! = 0_{O^{<\epsilon_0}} \ \wedge \ snd(x)! = 0_{O^{<\epsilon_0}}) \rightarrow snd(x) > snd(trd(x))$

Teorema 4.13
$\forall m : N.\forall x : O^{<\epsilon_0}.(nf_m(x) = x \ \wedge \ x! = 0_{O^{<\epsilon_0}} \ \wedge \ snd(x) = 0_{O^{<\epsilon_0}}) \rightarrow \ trd(x) = 0_{O^{<\epsilon_0}}$

Nei precedenti teoremi la funzione di confronto $<$ tra ordinali minori di ϵ_0 è la seguente

$$\begin{array}{rcl} 0_{O^{<\epsilon_0}} \ < \ 0_{O^{<\epsilon_0}} & = & false \\ 0_{O^{<\epsilon_0}} \ < \ (< n', \alpha, \beta >) & = & true \\ (< n', \alpha, \beta >) \ < \ 0_{O^{<\epsilon_0}} & = & false \\ (< n', \alpha, \beta >) \ < \ (< n'', \gamma, \delta >) & = & if \ \alpha \ < \ \gamma \ then \ true \\ & & else \ if \ \alpha = \gamma \ then \\ & & \quad if \ n' < n'' \ then \ true \\ & & \quad else \ if \ n' = n'' \ then \ \beta \ < \ \delta \\ & & \quad \quad else \ false \\ & & \quad else \ false \end{array}$$

e snd e trd sono funzioni che restituiscono rispettivamente il secondo ed il terzo elemento di una tripla corrispondente ad un ordinale.
Con questi ultimi risultati riteniamo chiara l'individuazione degli oggetti del nostro nuovo sistema formale. Infatti una definizione degli operatori di somma e prodotto sugli ordinali risulta piuttosto banale e al di là degli scopi di questa presentazione. Spendiamo invece alcune ultime parole sul principio di induzione portato da questi nuovi ordinali costruttivi. Ricordiamo dal capitolo 1 che per ogni ordinale e per ogni proposizione definita su di essi vale il seguente principio di induzione transfinita:

$$\forall P.(\ P(0) \wedge (\forall \beta.P(\beta) \rightarrow P(\beta+1)) \wedge (\forall \alpha.\forall \gamma < \alpha.P(\gamma) \rightarrow P(\alpha)) \ ) \rightarrow \forall \delta.P(\delta)$$

E' facile osservare, facendo riferimento al capitolo 3, che la forma di induzione dei nostri ordinali è molto più debole e si presenta nel seguente modo:

$$\forall P.(\ P(0) \wedge \forall \alpha.(P(snd(\alpha)) \wedge P(trd(\alpha)) \rightarrow P(\alpha) \ ) \rightarrow \forall \gamma.P(\gamma)$$

Mostreremo nel prossimo capitolo alcuni risultati relativi ai nostri ordinali ed al Teorema di Goodstein.

Capitolo 5

E' possibile una dimostrazione costruttiva del Teorema di Goodstein?

Ricordiamo brevemente i passi principali della dimostrazione classica del teorema di Goodstein, presentata nel capitolo 2, prima di tentare una dimostrazione costruttiva dello stesso.

1. Per prima cosa si definisce la Goodstein predecessor sequence $< \alpha > (n)$, dove α è un ordinale minore di ϵ_0 e n un numero naturale, e si dimostra che $\forall \alpha > 0. < \alpha > (n) < \alpha$. Quindi a partire da un ordinale α si può costruire una sequenza di ordinali descrescente applicando ad ogni passo la Goodstein predecessor sequence.

2. Si dimostra che la sequenza descrescente di ordinali è 'parallela' alla successione di Goodstein, ovvero che per ogni i l'elemento i-esimo della sequenza decrescente di ordinali corrisponde all'elemento i-esimo della successione di Goodstein dove ad ogni m+i (m è la base di partenza) abbiamo sostituito ω.

3. Poichè, per l'assioma di fondazione, ogni sequenza decrescente di ordinali è finita e, come abbiamo dimostrato nel punto precedente, la nostra sequenza di ordinali è parallela alla sequenza di Goodstein, avremmo una contraddizione se la sequenza di Goodstein non terminasse.

Cercheremo nel seguito del capitolo di fornire una versione costruttiva dei passi enumerati, mostrando i problemi epistemologico-ontologici che emergono nel portare in ambito costruttivo il terzo passo della dimostrazione. In primo luogo definiamo la successione di Goodstein definita sul numero naturale p a partire dalla base m

$$goodstein(m)(p)(0) \quad = \quad n2cantor_m(p)$$

$$goodstein(m)(p)(s(k)) = pr_{m+s(k)}(cantor_{m+k}2cantor_{m+s(k)}(goodstein(m)(p)(k)))$$

dove le funzioni pr_m e $cantor_m 2cantor_k$ sono definite nel seguente modo:

$$pr_m(x) = n2cantor_m(pred(cantor_m 2n(x)))$$

$$\begin{aligned} cantor_m 2cantor_k(0_m) &= 0_k \\ cantor_m 2cantor_k(< n', \alpha, \beta >_m) &= < n', cantor_m 2cantor_k(\alpha), cantor_m 2cantor_k(\beta) >_k \end{aligned}$$

Successivamente definiamo la funzione Goodstein Predecessor (GP) e costruiamo grazie ad essa una Goodstein Ordinal Sequence (GOS).

$$GP(x)(n) = cantor_{s(n)}2ord(pr_{s(n)}(ord2cantor_{s(n)}(x)))$$

$$\begin{aligned} GOS(m)(p)(0) &= cantor_m 2ord(goodstein(m)(p)(0)) \\ GOS(m)(p)(s(k)) &= GP(GOS(m)(p)(k))(k+m) \end{aligned}$$

dove la definizione delle funzioni $cantor_m 2ord$ e $ord2cantor_m$ è la seguente:

$$\begin{aligned} cantor_m 2ord(0_m) &= 0_{O^{<\epsilon_0}} \\ cantor_m 2ord(< n', \alpha, \beta >_m) &= < n', cantor_m 2ord(\alpha), cantor_m 2ord(\beta) > \end{aligned}$$

$$\begin{aligned} ord2cantor_m(0_{O^{<\epsilon_0}}) &= 0_m \\ ord2cantor_m(< n', \alpha, \beta >) &= < n', ord2cantor_m(\alpha), ord2cantor_m(\beta) >_m \end{aligned}$$

Possiamo quindi procedere enunciando la proprietà più importante di GP attraverso alcuni lemmi la cui dimostrazione sarà presentata nell' Appendice B.

Teorema 5.1
$\forall x : O^{<\epsilon_0}.\forall n : N.(nf(x)(s(n)) = x \ \wedge \ x! = 0_{O^{<\epsilon_0}}) \rightarrow \ GP(x)(n) < x$

Il teorema garantisce infatti che l'applicazione di GP ad un ordinale in forma $s(n)$-normale genera un ordinale minore di quello dato. Dimostrato dunque che ogni ordinale generato da $GOS(m)(p)(k)$ è in forma $s(k)+m$ normale, possiamo ottenere come semplice corollario il fatto che si può costruire una sequenza di ordinali descrescente applicando ad ogni passo la Goodstein predecessor sequence.

Teorema 5.2
$\forall m : N.\forall p : N.\forall k : N.nf(GOS(m)(p)(k))(s(k)+m) = GOS(m)(p)(k)$

Corollario 5.3
$\forall m : N.\forall p : N.\forall k.(GOS(m)(p)(k)! = 0_{O^{<\epsilon_0}}) \rightarrow GOS(m)(p)(s(k)) < GOS(m)(p)(k)$

Mostriamo ora il parallelismo sussistente fra la Goodstein Ordinal Sequence e la sequenza di Goodstein. E' infatti immediato dimostrare, a partire dalle definizioni delle due sequenze, il seguente teorema:

Teorema 5.4
$\forall m : N.\forall p : N.\forall k.GOS(m)(p)(k) = cantor_{m+k}2ord(goodstein(m)(p)(k))$

Possiamo dunque affermare che la traduzione negli ordinali del k-esimo elemento della sequenza di Goodstein è equivalente al k-esimo elemento della GOS quando facciamo partire le due successioni dalla base naturale m e dal naturale p.
Rimane invece aperto il problema del buon ordine dei nostri ordinali. In altre parole per concludere la dimostrazione in ambito costruttivo necessitiamo di una dimostrazione costruttiva della non esistenza di sequenze decrescenti infinite di ordinali.
Pur non avendo un risultato che indichi il limite di ITT nel non poter mostrare il buon ordine degli ordinali minori di ϵ_0, forniamo di seguito alcune argomentazioni a favore della non dimostrabilità del buon ordine in $O^{<\epsilon_0}$, confidando nel fatto che in futuri lavori si possa arrivare ad una trattazione formale delle idee esposte.
Vogliamo dunque enucleare le caratteristiche che differenziano ZFC e ITT per ciò che concerne la dimostrabilità del buon ordine degli ordinali minori di ϵ_0 e quindi proporre alcuni indirizzi di ricerca che potrebbero portare a risultati più deboli del buon ordine su ϵ_0, ma forse utili per gettare maggior luce sul problema. E' infatti immediato notare che tutti gli oggetti di ZFC portano con sè le proprietà date dall'assioma di fondazione, proprietà che necessariamente portano alla non esistenza di sequenze discendenti infinite. D'altra parte in ITT non è presente l' assioma di fondazione o un assioma che permetta senza mediazioni la dimostrazione della non esistenza di sequenze discendenti infinite.
Nello specifico degli ordinali da noi proposti, la definizione di $<$ sembra portare con sè alcune peculiarità di ZFC come l'utilizzo dell'infinito attuale, la definizione dell'ordine a partire dalla relazione di appartenenza e l'induzione transfinita, peculiarità che non possono trovare una controparte in una teoria costruttiva finitista. Infatti, sebbene sia possibile ridurre l'ordine di un numero finito di ordinali all'ordine dei naturali tramite una opportuna traduzione nei numeri di Cantor parametrici ad m e quindi nei naturali (dove m è un naturale maggiore di ogni coefficiente naturale presente negli ordinali), non sembra lecita una estensione della tecnica per ciò che riguarda un numero (potenzialmente) infinito di ordinali. E' necessario infatti, in tal caso, trovare un numero naturale maggiore di ogni possibile coefficiente di un ordinale e, purtroppo, è evidente che tale numero deve essere ω ovvero la prima manifestazione dell'infinito attuale.
Possiamo tuttavia pensare dimostrabili alcune congetture su ordinali più piccoli degli ordinali minori di ϵ_0. Pensiamo infatti all'insieme $O^{<\omega 2}$, ovvero all'insieme di tutti gli ordinali minori di $\omega 2$. In tal caso le regole di formazione potrebbero essere le seguenti (con una opportuna nozione di forma normale):

$$\frac{}{0_{O^{<\omega 2}} : O^{<\omega 2}}$$

$$\frac{n : Bool \quad m : N}{< n, < 1, 0_{O^{<\omega 2}}, 0_{O^{<\omega 2}} >, < m, 0_{O^{<\omega 2}}, 0_{O^{<\omega 2}} >>: O^{<\omega 2}}$$

Sembra più facile in questo nuovo framework pensare ad una dimostrazione della non esistenza di sequenze discendenti infinite. L'idea alla base della dimostrazione dovrebbe essere la seguente: 'Se l'ordinale γ è minore dell'ordinale δ allora o il primo coefficiente booleano di δ è passato da true a false (ed è potenzialmente aumentato il secondo coefficiente) o il primo coefficiente naturale di δ e γ era lo stesso ed è dimuito il secondo coefficiente. L'aumento del secondo coefficente può avvenire una sola volta e solo quando passiamo da true a false nel primo coefficiente.' In [Valentini] si dimostra che ogni sequenza discendente di naturali è finita e quindi possiamo mostrare che prima o poi arriveremo all'ordinale

$$< false, < 1, 0_{O^{<\omega 2}}, 0_{O^{<\omega 2}} >, < 0, 0_{O^{<\omega 2}}, 0_{O^{<\omega 2}} >>= 0_{O^{<\omega 2}}$$

E' naturale pensare che lo stesso meccanismo possa funzionare anche per $\omega 3, \omega 4, ...$ e una rappresentazione simile a quella per $O^{<\omega 2}$ è possibile anche per gli ordinali minori di $\omega^2, \omega^3 ....$ Ad esempio l'insieme degli ordinali minori di ω^2 si genera tramite le seguenti regole:

$$\frac{}{0_{O^{<\omega^2}} : O^{<\omega^2}}$$

$$\frac{n : N \quad m : N}{< n, < 1, 0_{O^{<\omega 2}}, 0_{O^{<\omega 2}} >, < m, 0_{O^{<\omega 2}}, 0_{O^{<\omega 2}} >>: O^{<\omega 2}}$$

In questo caso è possibile applicare l'idea sopra descritta sostituendo i finiti passaggi da true a false con gli altrettanto finiti passaggi da un naturale n a 0. Sarà dunque ω^ω il limite della nostra teoria? In [Simpson88] si mostra che in una particolare teoria costruttiva (RCA_0) non è possibile dimostrare il buon ordine di ω^ω ed in generale è possibile trovare in letteratura numerosi risultati che stabiliscono limiti alle teorie costruttive rispetto ai numeri ordinali. Possiamo quindi affermare che uno sviluppo delle idee qui esposte potrà chiarire alcuni aspetti di ITT e fornire una base di confronto con altre teorie costruttive.

Conclusioni

Abbiamo quindi presentato un framework costruttivo per gli ordinali minori di ϵ_0 dimostrando le proprietà essenziali per operare con essi. Abbiamo inoltre valutato il nostro framework nel tentativo di una dimostrazione costruttiva del Teorema di Goodstein. I risultati mostrati indicano che i nostri ordinali riproducono alcune delle peculiarità degli ordinali classici anche se, come ci si poteva aspettare, falliscono laddove avrebbero dovuto mostrare proprietà legate al substrato non costruttivo della teoria degli insiemi. Nel Capitolo 5 abbiamo infatti mostrato come sia possibile fornire una versione costruttiva della dimostrazione classica del Teorema di Goodstein arrestandosi tuttavia all'ultimo passo della dimostrazione in cui è necessario far riferimento all'assioma non costruttivo di fondazione. Due sono quindi le vie che possiamo indicare per proseguire il lavoro qui cominciato. In primo luogo, come abbiamo già indicato alla fine del Capitolo 5, uno studio dei limiti di ITT per ciò che riguarda le dimostrazioni di buon ordine sembra poter fornire utili informazioni sul framework da noi creato e sulla teoria stessa. In seconda ed ultima istanza un confronto dei nuovi ordinali costruttivi con nozioni simili già presenti in letteratura ([Taylor96][Hancock00][Martin-Lof84]) potrebbe aiutarci a raffinare, e quindi migliorare, le idee esposte in questo scritto.

Appendice A

Ordinali in ITT

A.1 Naturali

Formazione

$$\frac{}{N : type} \qquad \frac{}{N = N}$$

Introduzione

$$\frac{}{0 : N} \qquad \frac{n : N}{s(n) : N}$$

$$\frac{}{0 = 0 : N} \qquad \frac{n = m : N}{s(n) = s(m) : N}$$

Eliminazione

$$\frac{c : N \quad d : \gamma \quad e : N \rightarrow (\ \gamma \rightarrow \gamma\ )}{Natrec(c, d, e) : \gamma}$$

$$\frac{c = c' : N \quad d = d' : \gamma \quad e = e' : N \rightarrow (\ \gamma \rightarrow \gamma\ )}{Natrec(c, d, e) = Natrec(c', d', e') : \gamma}$$

Equivalenza

$$\frac{d : \gamma \quad e : N \to (\ \gamma \to \gamma\ )}{Natrec(0, d, e) = d : \gamma}$$

$$\frac{c : N \quad d : \gamma \quad e : N \to (\ \gamma \to \gamma\ )}{Natrec(s(c), d, e) = e(c)(Natrec(c, d, e)) : \gamma}$$

Riduzione

$$\frac{}{0 \Rightarrow 0} \qquad \frac{c \Rightarrow g}{s(c) \Rightarrow s(g)}$$

$$\frac{c \Rightarrow 0 \quad d \Rightarrow g}{Natrec(c, d, e) \Rightarrow g} \qquad \frac{c \Rightarrow s(n) \qquad e(n)(Natrec(n, d, e) \Rightarrow g}{Natrec(c, d, e) \Rightarrow g}$$

A.1.1 Operazioni sui Naturali

Test zero

$$iszero_N \equiv \lambda x.Natrec(x, true, \lambda z.\lambda w.false)$$

Somma

$$x + y \equiv \lambda x.\lambda y.Natrec(x, y, \lambda z.\lambda w.s(w))$$

Prodotto

$$x * y \equiv \lambda x.\lambda y.Natrec(y, 0, \lambda z.\lambda w.x + w)$$

Esponente

$$x^y \equiv \lambda x.\lambda y.Natrec(y, s(0), \lambda z.\lambda w.x * w)$$

Predecessore

$$pred \equiv \lambda x.Natrec(x, 0, \lambda z.\lambda w.z)$$

Minore

$$le \equiv x < y \equiv \lambda x.Natrec(x, \lambda y.not\ iszero_N(y), \lambda z.\lambda w.\lambda y.w(pred(y)))$$

A.2 Numeri di Cantor

Formazione

$$\frac{n : N}{Cantor(n) : type} \qquad \frac{n = m : N}{Cantor(n) = Cantor(m)}$$

Introduzione

$$\frac{}{0_m : Cantor(m)} \qquad \frac{n : N \quad \alpha : Cantor(m) \quad \beta : Cantor(m)}{< n, \alpha, \beta >: Cantor(m)}$$

$$\frac{}{0_m = 0_m : Cantor(m)} \qquad \frac{n = n' : N \quad \alpha = \gamma : Cantor(m) \quad \beta = \delta : Cantor(m)}{< n, \alpha, \beta >=< n', \gamma, \delta >: Cantor(m)}$$

Eliminazione

$$\frac{c : Cantor(m) \quad d : \gamma \quad e : N \rightarrow (Cantor(m) \rightarrow (Cantor(m) \rightarrow (\gamma \rightarrow (\gamma \rightarrow \gamma))))}{CRec(c, d, e) : \gamma}$$

$$\frac{c = c' : Cantor(m) \quad d = d' : \gamma \quad e = e' : N \rightarrow (Cantor(m) \rightarrow (Cantor(m) \rightarrow (\gamma \rightarrow (\gamma \rightarrow \gamma))))}{CRec(c, d, e) = CRec(c', d', e') : \gamma}$$

Equivalenza

$$\frac{d : \gamma \quad e : N \rightarrow (Cantor(m) \rightarrow (Cantor(m) \rightarrow (\gamma \rightarrow (\gamma \rightarrow \gamma))))}{CRec(0, d, e) = d : \gamma}$$

$$\frac{n : N \quad \delta : Cantor(m) \quad \epsilon : Cantor(m) \quad d : \gamma \quad e : N \rightarrow (Cantor(m) \rightarrow (Cantor(m) \rightarrow (\gamma \rightarrow (\gamma \rightarrow \gamma))))}{CRec(< n, \delta, \epsilon >, d, e) = e(n)(\delta)(\epsilon)(CRec(\delta, d, e))(CRec(\epsilon, d, e)) : \gamma}$$

Riduzione

$$\frac{}{0_m \Rightarrow 0_m} \qquad \frac{n \Rightarrow g_n \quad \alpha \Rightarrow g_\alpha \quad \beta \Rightarrow g_\beta}{< n, \alpha, \beta > \Rightarrow < g_n, g_\alpha, g_\beta >}$$

$$\frac{c \Rightarrow 0 \quad d \Rightarrow g_d}{CRec(c, d, e) \Rightarrow g_d} \qquad \frac{c \Rightarrow < n, \alpha, \beta > \quad e(n)(\alpha)(\beta)(CRec(\alpha, d, e))(CRec(\beta, d, e)) \Rightarrow g}{CRec(c, d, e) \Rightarrow g}$$

A.2.1 Operazioni sui Numeri di Cantor

Incremento

$$inc_m \equiv \lambda x.CRec(x, < s(0), 0_m, 0_m >, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.if\ (not\ nf_m(x) = x)\ then\ < s(0), 0, x >_m\ else$$
$$if\ u = snd(w)\ then$$
$$if\ t < pred(m)\ then\ < s(t), u, 0_m >_m$$
$$else\ < s(0), z, 0_m >_m$$
$$else\ < t, u, w >_m)$$

Proiezioni

$fst_m \equiv \lambda x.CRec(x, 0, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.t)$

$snd_m \equiv \lambda x.CRec(x, 0_m, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.u)$

$trd_m \equiv \lambda x.CRec(x, 0_m, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.v)$

Test zero

$iszero_m \equiv \lambda x.CRec(x, true, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.false)$

Equivalenza

$$eq_m \equiv x =_m y \equiv \lambda x.CRec(x, \lambda y.iszero(y), \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.\lambda y.if\ iszero(y)\ then\ false$$
$$else\ (t = fst(y))\ and\ z(snd(y))\ and\ w(trd(y))\ )$$

Minore

$le_m \equiv \lambda x.CRec(x, \lambda y.notiszero(y), \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.\lambda y.if\ iszero(y)\ then\ false$
$else\ if\ z(snd(y))\ then\ true$
$else\ if\ u =_m snd(y)\ then$
$if\ t < fst(y)\ then\ true$
$else\ if\ t = fst(y)\ then\ w(trd(y))$
$else\ false$
$else\ false\ )$

Traduzione

$cantor_m 2n \equiv \lambda x.CRec(x, 0, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.t * m^z + w)$
$n2cantor_m \equiv \lambda x.Natrec(x, 0_m, \lambda z.\lambda w.inc_m(w))$
$cantor_m 2cantor_n \equiv \lambda x.CRec(x, 0_n, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w. < t, z, w >_n)$

Forma normale
$nf_m \equiv \lambda x.n2cantor_m(cantor_m2n(x))$

Predecessore
$pr_m \equiv \lambda x.n2cantor_m(pred(cantor_m2n(x)))$

Sequenza di Goodstein
$goodstein \equiv \lambda m.\lambda p.\lambda n.Natrec(n, n2cantor_m(p), \lambda z.\lambda w.pr_{m+s(n)}(cantor_{m+n}2cantor_{m+s(n)}(w)))$

A.3 Ordinali minori di ϵ_0

Formazione

$$\frac{}{O^{<\epsilon_0} : type} \qquad \frac{}{O^{<\epsilon_0} = O^{<\epsilon_0}}$$

Introduzione

$$\frac{}{0_{O^{<\epsilon_0}} : O^{<\epsilon_0}} \qquad \frac{n : N \quad \alpha : O^{<\epsilon_0} \quad \beta : O^{<\epsilon_0}}{< n, \alpha, \beta >: O^{<\epsilon_0}}$$

$$\frac{}{0_m = 0_m : O^{<\epsilon_0}} \qquad \frac{n = n' : N \quad \alpha = \gamma : O^{<\epsilon_0} \quad \beta = \delta : O^{<\epsilon_0}}{< n, \alpha, \beta >=< n', \gamma, \delta >: O^{<\epsilon_0}}$$

Eliminazione

$$\frac{c : O^{<\epsilon_0} \quad d : \gamma \quad e : N \to (O^{<\epsilon_0} \to (O^{<\epsilon_0} \to (\gamma \to (\gamma \to \gamma))))}{ORec(c, d, e) : \gamma}$$

$$\frac{c = c' : O^{<\epsilon_0} \quad d = d' : \gamma \quad e = e' : N \to (O^{<\epsilon_0} \to (O^{<\epsilon_0} \to (\gamma \to (\gamma \to \gamma))))}{ORec(c, d, e) = ORec(c', d', e') : \gamma}$$

Equivalenza

$$\frac{d : \gamma \quad e : N \to (O^{<\epsilon_0} \to (O^{<\epsilon_0} \to (\gamma \to (\gamma \to \gamma))))}{ORec(0, d, e) = d : \gamma}$$

$$\frac{n : N \quad \delta : O^{<\epsilon_0} \quad \epsilon : O^{<\epsilon_0} \quad d : \gamma \quad e : N \to (O^{<\epsilon_0} \to (O^{<\epsilon_0} \to (\gamma \to (\gamma \to \gamma))))}{ORec(< n, \delta, \epsilon >, d, e) = e(n)(\delta)(\epsilon)(ORec(\delta, d, e))(ORec(\epsilon, d, e)) : \gamma}$$

Riduzione

$$\frac{}{0_m \Rightarrow 0_m} \qquad \frac{n \Rightarrow g_n \quad \alpha \Rightarrow g_\alpha \quad \beta \Rightarrow g_\beta}{< n, \alpha, \beta > \Rightarrow < g_n, g_\alpha, g_\beta >}$$

$$\frac{c \Rightarrow 0 \quad d \Rightarrow g_d}{ORec(c, d, e) \Rightarrow g_d} \qquad \frac{c \Rightarrow < n, \alpha, \beta > \quad e(n)(\alpha)(\beta)(ORec(\alpha, d, e))(ORec(\beta, d, e)) \Rightarrow g}{ORec(c, d, e) \Rightarrow g}$$

A.3.1 Operazioni sugli Ordinali minori di ϵ_0

Equivalenza

$$eq \equiv x = y \equiv \lambda x.ORec(x, \lambda y.iszero(y), \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.\lambda y.if\ iszero(y)\ then\ false$$
$$else\ (t = fst(y))\ and\ z(snd(y))\ and\ w(trd(y))\ )$$

Minore
$le \equiv \lambda x.CRec(x, \lambda y.notiszero(y), \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.\lambda y.if\ iszero(y)\ then\ false$
$else\ if\ z(snd(y))\ then\ true$
$else\ if\ u = snd(y)\ then$
$if\ t < fst(y)\ then\ true$
$else\ if\ t = fst(y)\ then\ w(trd(y))$
$else\ false$
$else\ false\ )$

Base
$base \equiv \lambda x.ORec(x, s(s(0)), \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.t + v + z)$

Test zero
$iszero \equiv \lambda x.ORec(x, true, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.false)$

Traduzione
$cantor_m 2ord \equiv \lambda x.CRec(x, 0_{O<\epsilon_0}, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w. < t, z, w >)$
$ord2cantor \equiv \lambda x.ord2cantor_{base(x)}(x)$
$ord2cantor_m \equiv \lambda x.ORec(x, 0_m, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w. < t, z, w >)$

Forma normale
$nf \equiv \lambda x.\lambda n.cantor_n 2ord(nf_n(ord2cantor_n(x)))$

Proiezioni
$fst \equiv \lambda x.ORec(x, 0, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.t)$

$snd \equiv \lambda x.ORec(x, 0, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.u)$

$trd \equiv \lambda x.ORec(x, 0, \lambda t.\lambda u.\lambda v.\lambda z.\lambda w.v)$

Goodstein Predecessor
$GP \equiv \lambda x.\lambda n.cantor_{s(n)} 2ord(pr_{s(n)}(ord2cantor_{s(n)}(x)))$

Goodstein Ordinal Sequence
$GOS \equiv \lambda m.\lambda p.\lambda n.Natrec(n, cantor_m 2ord(goodstein(m)(p)(0)), \lambda z.\lambda w.GP(w)(z+m))$

Appendice B

Dimostrazioni

B.1 Dimostrazioni del Capitolo 4

Teorema 1
$\forall m : N.\forall n : N.inc(n2cantor_m(n)) = n2Cantor_m(s(n))$.
Dim.
Se n= 0 *allora* $inc(0) = inc(0)$ *per definizione di* $n2cantor_m$.
Se n= $s(n')$ *allora per definizione di* $n2cantor_m$ $inc(n2cantor_m(n')) = inc(n2Cantor_m(n'))$.

Teorema 2
$\forall m : N.\forall x : Cantor(m).cantor_m2n(inc(x)) = s(cantor_m2n(x))$.
Dim.*Per induzione sulla struttura di x.*

Se $x = 0$ *dobbiamo dimostrare* $cantor_m2n(< s(0), 0, 0 >) = s(cantor_m2n(0))$ *che per definizione di* $cantor_m2n$ *equivale a dimostrare* $s(0) = s(0)$.

Se $x =< n', \alpha, \beta >$ *dobbiamo mostrare*

$$cantor_m2n(inc(< n', \alpha, \beta >)) = s(cantor_m2n(< n', \alpha, \beta >))$$

e per ipotesi induttiva su α *e* β *abbiamo*

$$cantor_m2n(inc(\alpha)) = s(cantor_m2n(\alpha))$$
$$cantor_m2n(inc(\beta)) = s(cantor_m2n(\beta))$$

Ragioniamo per casi sulle possibili trasformazioni operate da inc su $< n', \alpha, \beta >$:

- *not* $nf_m(x) = x$
  In tal caso applicando inc otteniamo

$$inc(< n', \alpha, \beta >) =< s(0), 0, < n', \alpha, \beta >>$$

e quindi per la definizione di $cantor_m 2n$

$$cantor_m 2n(< s(0), 0, < n', \alpha, \beta >>) = s(0) * m^0 + cantor_m 2n(< n', \alpha, \beta >) = s(cantor_m 2n(< n', \alpha, \beta >))$$

sfruttando le proprietà dei numeri naturali e dell'operatore successore definito su di essi.

- $\alpha = snd(inc(\beta))$ *e* $n' < pred(m)$
  In tal caso applicando inc otteniamo

$$inc(< n', snd(inc(\beta)), \beta >) =< s(n'), snd(inc(\beta)), 0 >$$

e dobbiamo quindi mostrare che

$$cantor_m 2n(< s(n'), snd(inc(\beta)), 0 >) =$$

$$s(cantor_m 2n(< n', snd(inc(\beta)), \beta >)).$$

Ora questo, per la definizione di $cantor_m 2n$*, equivale a mostrare*

$$s(n') * m^{cantor_m 2n(snd(inc(\beta)))} = s(n' * m^{cantor_m 2n(snd(inc(\beta)))} + cantor_m 2n(\beta))$$

che per le proprietà dei numeri naturali e dell'operatore successore definito su di essi equivale a mostrare

$$m^{cantor_m 2n(snd(inc(\beta)))} = s(cantor_m 2n(\beta)).$$

Per ipotesi induttiva ho che

$$s(cantor_m 2n(\beta)) = cantor_m 2n(inc(\beta))$$

e possiamo quindi concludere per la definizione di $cantor_m 2n$

$$cantor_m 2n(inc(\beta)) = m^{cantor_m 2n(snd(inc(\beta)))}$$

- $\alpha = snd(inc(\beta))$ *e* $n' = pred(m)$
  In tal caso

$$inc(< n', snd(inc(\beta)), \beta >) =< s(0), inc(snd(inc(\beta))), 0 >$$

e dobbiamo quindi mostrare che

$$cantor_m 2n(< s(0), inc(snd(inc(\beta))), 0 >) =$$

$$s(cantor_m 2n(< n', snd(inc(\beta)), \beta >)).$$

Per definizione di $cantor_m 2n$ questo equivale a mostrare

$$s(0) * m^{cantor_m 2n(inc(snd(inc(\beta))))} = \\ s(n' * m^{cantor_m 2n(snd(inc(\beta)))} + cantor_m 2n(\beta))$$

che per ipotesi induttiva su $\alpha = snd(inc(\beta))$ equivale a mostrare

$$s(0) * m^{s(cantor_m 2n(\alpha)} = s(n' * m^{cantor_m 2n(\alpha)} + cantor_m 2n(\beta)).$$

Ora per ipotesi induttiva su β e per le proprietà dei numeri naturali e dell'operatore successore definito su di essi

$$s(n' * m^{cantor_m 2n(\alpha)} + cantor_m 2n(\beta)) = \\ pred(m) * m^{cantor_m 2n(\alpha)} + m^{cantor_m 2n(\alpha)}$$

e per le proprietà delle potenze sui naturali possiamo mostrare

$$pred(m) * m^{cantor_m 2n(\alpha)} + m^{cantor_m 2n(\alpha)} = s(0) * m^{s(cantor_m 2n(\alpha)}.$$

- *(caso di default) Nel caso in cui nessuna delle condizioni precedenti dovesse verificarsi otteniamo*

  $$inc(< n', \alpha, \beta >) =< n', \alpha, inc(\beta) >$$

  e dobbiamo quindi mostrare che

  $$cantor_m 2n(< n', \alpha, inc(\beta >)) = s(cantor_m 2n(< n', \alpha, \beta)).$$

  Per la definizione di $cantor_m 2n$ questo equivale a mostrare

  $$n' * m^{cantor_m 2n(\alpha)} + cantor_m 2n(inc(\beta)) = \\ s(n' * m^{cantor_m 2n(\alpha)} + cantor_m 2n(\beta))$$

  che per le proprietà dei numeri naturali e dell'operatore successore definito su di essi equivale a mostrare

  $$n' * m^{cantor_m 2n(\alpha)} + cantor_m 2n(inc(\beta)) = \\ n' * m^{cantor_m 2n(\alpha)} + s(cantor_m 2n(\beta)).$$

  Possiamo quindi concludere sfruttando l'ipotesi induttiva su β.

Corollario 3
$\forall m : N.\forall n : N cantor_m 2n(n2cantor_m(n)) = n$
Dim. *Per induzione su n.*

Se $n = 0$ allora per definizione di $cantor_m 2n$ e $n2cantor_m$ otteniamo

$$cantor_m2n(n2cantor_m(0)) = cantor_m2n(0_m) = 0.$$

Supponendo $n = k$ abbiamo per ipotesi induttiva

$$cantor_m2n(n2cantor_m(k)) = k$$

e dobbiamo dimostrare

$$cantor_m2n(n2cantor_m(s(k))) = s(k).$$

Ora, a partire dall'ipotesi induttiva, otteniamo

$$s(cantor_m2n(n2cantor_m(k))) = s(k)$$

e possiamo quindi concludere poichè

$$s(cantor_m2n(n2cantor_m(k))) = cantor_m2n(inc(n2cantor_m(k))) = \\ cantor_m2n(n2cantor_m(s(k)))$$

per i teoremi 1 e 2.

Teorema 4
$\forall n : N.\forall m : N.(n! = 0 \ \wedge \ snd(n2cantor_m(n))! = 0) \rightarrow \ snd(n2cantor_m(n)) > snd(trd(n2cantor_m(n)))$
Dim.\ *Per induzione su n.*
Per ipotesi induttiva abbiamo che

$$(k! = 0 \ \wedge \ snd(n2cantor_m(k))! = 0) \rightarrow$$

$$snd(n2cantor_m(k)) > snd(trd(n2cantor_m(k)))$$

e per ipotesi abbiamo

$$s(k)! = 0 \ \wedge \ snd(n2cantor_m(s(k)))! = 0.$$

Se $s(k) = s(0)$ la dimostrazione è immediata.
Se $s(k)! = s(0)$, per la decidibilità dell'uguaglianza, è possibile mostrare per assurdo che l'ipotesi implica

$$k! = 0 \ \wedge \ snd(n2cantor_m(k))! = 0$$

e quindi abbiamo

$$snd(n2cantor_m(k)) > snd(trd(n2cantor_m(k))).$$

Dobbiamo quindi mostrare

$$snd(n2cantor_m(s(k))) > snd(trd(n2cantor_m(s(k))))$$

che equivale per il Teorema 1 a mostrare

$$snd(inc(n2cantor_m(k))) > snd(trd(inc(n2cantor_m(k)))).$$

Ragioniamo quindi sulle possibili trasformazioni operate da inc su $n2cantor_m(k)$*:*

- $snd(n2cantor_m(k)) = snd(inc(trd(n2cantor_m(k)))$ *e* $fst(n2cantor_m(k)) < pred(m)$
  In tal caso applicando inc otteniamo

  $$inc(< fst(n2cantor_m(k)), snd(n2cantor_m(k)), trd(n2cantor_m(k)) >) =$$

  $$< s(fst(n2cantor_m(k))), snd(n2cantor_m(k)), 0 >.$$

  Dobbiamo quindi mostrare che $snd(inc(n2cantor_m(k))) > 0$*. Ora, poichè per ipotesi*

  $$snd(inc(n2cantor_m(k))) = snd(n2cantor_m(k))$$

  e poichè

  $$snd(n2cantor_m(k)) > snd(trd(n2cantor_m(k)))$$

  implica $snd(n2cantor_m(k)) > 0$*, possiamo concludere.*

- $snd(n2cantor_m(k)) = snd(inc(trd(n2cantor_m(k)))$ *e* $fst(n2cantor_m(k)) = pred(m)$
  In tal caso applicando inc otteniamo

  $$inc(< fst(n2cantor_m(k)), snd(n2cantor_m(k)), trd(n2cantor_m(k)) >) =$$

  $$< s(0), inc(snd(n2cantor_m(k))), 0 >.$$

  Dobbiamo quindi mostrare che $snd(inc(n2cantor_m(k))) > 0$ *cioè* $inc(snd(n2cantor_m(k))) > 0$ *che vale per la definizione di inc.*

- *(caso di default) Nel caso in cui nessuna delle condizioni precedenti dovesse verificarsi otteniamo*

  $$inc(< fst(n2cantor_m(k)), snd(n2cantor_m(k)), trd(n2cantor_m(k)) >) =$$

  $$< fst(n2cantor_m(k)), snd(n2cantor_m(k)), inc(trd(n2cantor_m(k))) >.$$

  Dobbiamo quindi mostrare che

  $$snd(inc(n2cantor_m(k))) > snd(inc(trd(n2cantor_m(k)))).$$

  Ora, per il primo ed il terzo caso di applicazione di inc a $trd(n2cantor_m(k))$ *abbiamo che*

$$snd(inc(trd(n2cantor_m(k)))) = snd(trd(n2cantor_m(k)))$$

e quindi vale

$$snd(inc(n2cantor_m(k))) > snd(inc(trd(n2cantor_m(k))))$$

poichè $snd(n2cantor_m(k)) > snd(trd(n2cantor_m(k)))$.
Nel secondo caso di applicazione di inc a $trd(n2cantor_m(k))$ *abbiamo*

$$snd(inc(trd(n2cantor_m(k)))) = inc(snd(trd(n2cantor_m(k))))$$

e, poichè è possibile dimostrare che se

$$snd(n2cantor_m(k)) > snd(trd(n2cantor_m(k)))$$

allora vale

$$snd(n2cantor_m(k)) >= inc(snd(trd(n2cantor_m(k)))),$$

possiamo concludere.

Teorema 5
$\forall n : N.\forall m : N.(n! = 0 \ \wedge \ snd(n2cantor_m(n)) = 0) \rightarrow \ trd(n2cantor_m(n)) = 0$
Dim. *Per induzione su n.*
Per ipotesi induttiva abbiamo che

$$(k! = 0 \ \wedge \ snd(n2cantor_m(k)) = 0) \rightarrow \ trd(n2cantor_m(k)) = 0$$

e per ipotesi abbiamo

$$s(k)! = 0 \ \wedge \ snd(n2cantor_m(s(k))) = 0.$$

Se $s(k) = s(0)$ *la dimostrazione è immediata.*
Se $s(k)! = s(0)$, *per la decidibilità dell'uguaglianza, è possibile mostrare per assurdo che l'ipotesi implica*

$$k! = 0 \ \wedge \ snd(n2cantor_m(k)) = 0$$

e quindi abbiamo

$$trd(n2cantor_m(k)) = 0.$$

Dobbiamo quindi mostrare

$$trd(n2cantor_m(s(k))) = 0$$

che equivale per il Teorema 1 a mostrare

$$trd(inc(n2cantor_m(k))) = 0.$$

Ora, poichè

$$snd(n2cantor_m(k)) = snd(inc(trd(n2cantor_m(k))),$$

$$fst(n2cantor_m(k)) < pred(m)$$

è l'unico caso delle possibili trasformazioni operate da inc su $n2cantor_m(k)$ *che si possa verificare (gli altri portano ad una contraddizione), applicando inc otteniamo*

$$inc(< fst(n2cantor_m(k)), 0, 0 >) =< s(fst(n2cantor_m(k))), 0, 0 >$$

e possiamo concludere.

Teorema 6
$\forall n : N.\forall m : N.fst(n2cantor_m(n)) < m$
Dim. *Per induzione su n.*
Se $n = 0$ *abbiamo che* $fst(0) = 0$ *e* $0 < m$.
Per ipotesi induttiva abbiamo che

$$fst(n2cantor_m(k)) < m$$

Dobbiamo quindi mostrare

$$fst(n2cantor_m(s(k))) < m$$

che equivale per il Teorema 1 a mostrare

$$fst(inc(n2cantor_m(k))) < m.$$

Ragioniamo quindi sulle possibili trasformazioni operate da inc su $n2cantor_m(k)$*:*

- $snd(n2cantor_m(k)) = snd(inc(trd(n2cantor_m(k)))$ *e* $fst(n2cantor_m(k)) < pred(m)$
  In tal caso applicando inc otteniamo

  $$inc(< fst(n2cantor_m(k)), snd(n2cantor_m(k)), trd(n2cantor_m(k)) >) =$$

  $$< s(fst(n2cantor_m(k))), snd(n2cantor_m(k)), 0 >$$

  e quindi possiamo concludere poichè $fst(n2cantor_m(k)) < pred(m)$ *implica* $s(fst(n2cantor_m(k))) <= pred(m)$.

- $snd(n2cantor_m(k)) = snd(inc(trd(n2cantor_m(k)))$ *e* $fst(n2cantor_m(k)) = pred(m)$ *In tal caso applicando inc otteniamo*

  $$inc(< fst(n2cantor_m(k)), snd(n2cantor_m(k)), trd(n2cantor_m(k)) >) =$$

  $$< s(0), inc(snd(n2cantor_m(k))), 0 >$$

  e quindi possiamo concludere.

- *(caso di default) Nel caso in cui nessuna delle condizioni precedenti dovesse verificarsi otteniamo*

  $$inc(< fst(n2cantor_m(k)), snd(n2cantor_m(k)), trd(n2cantor_m(k)) >) =$$

  $$< fst(n2cantor_m(k)), snd(n2cantor_m(k)), inc(trd(n2cantor_m(k))) >$$

  e possiamo concludere sfruttando l'ipotesi induttiva.

Corollario 7
$\forall m : N.\forall x : Cantor(m).(nf_m(x) = x \ \wedge \ x! = 0 \ \wedge \ snd(x)! = 0) \rightarrow \ snd(x) > snd(trd(x))$
Dim.
Poichè $nf_m(x) = x$ *abbiamo che* $x = n2cantor_m(cantor_m2n(x))$ *e quindi per il Teorema 4 otteniamo*

$$snd(n2cantor_m(cantor_m2n(x))) > snd(trd(n2cantor_m(cantor_m2n(x)))).$$

Possiamo quindi concludere sostituendo x *a* $n2cantor_m(cantor_m2n(x))$.

Corollario 8
$\forall m : N.\forall x : Cantor(m).(nf_m(x) = x \ \wedge \ x! = 0 \ \wedge \ snd(x) = 0) \rightarrow \ trd(x) = 0$
Dim.
Poichè $nf_m(x) = x$ *abbiamo che* $x = n2cantor_m(cantor_m2n(x))$ *e quindi per il Teorema 5 otteniamo*

$$trd(n2cantor_m(cantor_m2n(x)))) = 0.$$

Possiamo quindi concludere sostituendo x *a* $n2cantor_m(cantor_m2n(x))$.

Corollario 9
$\forall m : N.\forall x : Cantor(m).nf_m(x) = x \rightarrow \ fst(x) < m$
Dim.
Poichè $nf_m(x) = x$ *abbiamo che* $x = n2cantor_m(cantor_m2n(x))$ *e quindi per il Teorema 6 otteniamo*

$$fst(n2cantor_m(cantor_m2n(x)) < m.$$

Possiamo quindi concludere sostituendo x *a* $n2cantor_m(cantor_m2n(x))$.

Teorema 10
$\forall m : N.\forall x : Cantor(m).ord2cantor_m(cantor_m2ord(x)) = x$
Dim. *Per induzione sulla struttura di* x.

Se $x = 0_m$ *allora* $cantor_m2ord(0_m) = 0$ *e* $ord2cantor_m(0) = 0_m$ *per definizione.*
Se $x =< n', \alpha, \beta >_m$ *allora per ipotesi induttiva su* α *e* β *abbiamo*

$$ord2cantor_m(cantor_m2ord(\alpha)) = \alpha$$

$$ord2cantor_m(cantor_m2ord(\beta)) = \beta.$$

Possiamo quindi concludere poichè per definizione di $cantor_m2ord$

$$cantor_m2ord(< n', \alpha, \beta >) =< n', cantor_m2ord(\alpha), cantor_m2ord(\beta) >$$

e per definizione di $ord2cantor_m$

$$ord2cantor_m(< n', cantor_m2ord(\alpha), cantor_m2ord(\beta) >) =$$

$$< n', ord2cantor_m(cantor_m2ord(\alpha)), ord2cantor_m(cantor_m2ord(\beta)) >=$$

$$< n', \alpha, \beta >,$$

sfruttando nell'ultimo passaggio l'ipotesi induttiva su α *e* β.

Teorema 11
$\forall m : N.\forall x : O^{<\epsilon_0}.cantor_m2ord(ord2cantor_m(x))) = x$
Dim. *Per induzione sulla struttura di* x.

Se $x = 0$ *allora* $ord2cantor_m(0) = 0_m$ *e* $cantor_m2ord(0_m) = 0$ *per definizione.*
Se $x =< n', \alpha, \beta >$ *allora per ipotesi induttiva su* α *e* β *abbiamo*

$$cantor_m2ord(ord2cantor_m(\alpha)) = \alpha$$

$$cantor_m2ord(ord2cantor_m(\beta)) = \beta.$$

Possiamo quindi concludere poichè per definizione di $ord2cantor_m$

$$ord2cantor_m(< n', \alpha, \beta >) =< n', ord2cantor_m(\alpha), ord2cantor_m(\beta) >$$

e per definizione di $cantor_m2ord$

$$cantor_m2ord(< n', ord2cantor_m(\alpha), ord2cantor_m(\beta) >) =$$

$$< n', cantor_m2ord(ord2cantor_m(\alpha)), cantor_m2ord(ord2cantor_m(\beta)) >=$$

$$< n', \alpha, \beta >,$$

sfruttando nell'ultimo passaggio l'ipotesi induttiva su α *e* β.

Teorema 12
$\forall m : N.\forall x : O^{<\epsilon_0}.(nf(x)(m) = x \ \wedge \ x! = 0_{O^{<\epsilon_0}} \ \wedge \ snd(x)! = 0_{O^{<\epsilon_0}}) \rightarrow snd(x) > snd(trd(x))$
Dim.
Poichè $nf(x)(m) = x$ *abbiamo che*

$$cantor_m2ord(n2cantor_m(cantor_m2n(ord2cantor_m(x)))) = x$$

e questo, per il Teorema 10, implica

$$n2cantor_m(cantor_m2n(ord2cantor_m(x))) = ord2cantor_m(x),$$

possiamo concludere per il Corollario 7.

Teorema 13
$\forall m : N.\forall x : O^{<\epsilon_0}.(nf(x)(m) = x \wedge x! = 0_{O^{<\epsilon_0}} \wedge snd(x) = 0_{O^{<\epsilon_0}}) \rightarrow trd(x) = 0_{O^{<\epsilon_0}}$
Dim.
Poichè $nf(x)(m) = x$ *abbiamo che*

$$cantor_m 2ord(n2cantor_m(cantor_m 2n(ord2cantor_m(x)))) = x$$

e questo, per il Teorema 10, implica

$$n2cantor_m(cantor_m 2n(ord2cantor_m(x))) = ord2cantor_m(x),$$

possiamo concludere per il Corollario 8.

B.2 Dimostrazioni del Capitolo 5

Teorema 1
$\forall x : O^{<\epsilon_0}.\forall n : N.(nf(x)(s(n)) = x \wedge x! = 0) \rightarrow GP(x)(n) < x$
Dim.
Poichè $nf(x)(s(n)) = x$ *abbiamo che* $x = cantor_{s(n)}2ord(nf_{s(n)}(ord2cantor_{s(n)}(x)))$ *e dobbiamo quindi dimostrare*

$$cantor_{s(n)}2ord(pr_{s(n)}(ord2cantor_{s(n)}(x))) < \\ cantor_{s(n)}2ord(nf_{s(n)}(ord2cantor_{s(n)}(x)))$$

o equivalentemente

$$cantor_{s(n)}2ord(n2cantor_{s(n)}(pred(cantor_{s(n)}2n((ord2cantor_{s(n)}(x)))))) < \\ cantor_{s(n)}2ord(n2cantor_{s(n)}(cantor_{s(n)}2n(ord2cantor_{s(n)}(x)))).$$

Ora, per il Lemma B.7, dimostrare l'ultima disuguaglianza equivale a dimostrare

$$n2cantor_{s(n)}(pred(cantor_{s(n)}2n((ord2cantor_{s(n)}(x))))) < \\ n2cantor_{s(n)}(cantor_{s(n)}2n(ord2cantor_{s(n)}(x)))$$

e poichè, per il lemma B.5, quest'ultima disuguaglianza vale, possiamo concludere.

Teorema 2
$\forall m : N.\forall p : N.\forall k : N.nf(GOS(m)(p)(k))(s(k) + m) = GOS(m)(p)(k)$
Dim.
Applicando la definizione di nf *otteniamo*

$$nf(GOS(m)(p)(k))(k + m) = \\ cantor_{s(k)+m}2ord(nf_{s(k)+m}(ord2cantor_{s(k)+m}(GOS(m)(p)(k))))$$

Ora, per il Teorema 11 e per il fatto che

$$\forall m : N.\forall k : N.\forall x : Cantor(m).cantor_m 2cantor_k(x) = ord2cantor_k(cantor_m 2ord(x))$$

otteniamo

$$cantor_{s(k)+m}2ord(nf_{s(k)+m}(ord2cantor_{s(k)+m}(GOS(m)(p)(k)))) = cantor_{s(k)+m}2ord(nf_{s(k)+m}(cantor_{k+m}2cantor_{s(k)+m}(goodstein(m)(p)(k)))).$$

Quindi, poichè è immediato mostrare che $nf_{m+k}(goodstein(m)(p)(k) = goodstein(m)(p)(k)$, *applicando il Lemma B.11 ed il Teorema 4 otteniamo*

$$cantor_{s(k)+m}2ord(nf_{s(k)+m}(cantor_{k+m}2cantor_{s(k)+m}(goodstein(m)(p)(k)))) = cantor_{m+k}2ord(goodstein(m)(p)(k)) = GOS(m)(p)(k)$$

Corollario 3
$\forall m : N.\forall p : N.\forall k.(GOS(m)(p)(k)! = 0_{O^{<\epsilon_0}}) \rightarrow GOS(m)(p)(s(k)) < GOS(m)(p)(k)$
Dim.
Poichè $GOS(m)(p)(s(k)) = GP(GOS(m)(p)(k))(k + m)$, *possiamo concludere per Teoremi 1 e 2.*

Teorema 4
$\forall m : N.\forall p : N.\forall k.GOS(m)(p)(k) = cantor_{m+k}2ord(goodstein(m)(p)(k))$
Dim. *Per induzione su k.*
Per ipotesi induttiva abbiamo

$$GOS(m)(p)(n) = cantor_{m+n}2ord(goodstein(m)(p)(n))$$

e dobbiamo mostrare

$$GOS(m)(p)(s(n)) = cantor_{m+s(n)}2ord(goodstein(m)(p)(s(n))).$$

Ora, sfruttando l'ipotesi induttiva ed il fatto che

$$\forall m : N.\forall k : N.\forall x : Cantor(m).cantor_m 2cantor_k(x) = ord2cantor_k(cantor_m 2ord(x))$$

otteniamo

$$GOS(m)(p)(s(n)) = GP(GOS(m)(p)(n))(n + m) =$$
$$cantor_{m+s(n)}2ord(pr_{m+s(n)}(ord2cantor_{m+s(n)}(cantor_{m+n}2ord(goodstein(m)(p)(n))))) =$$
$$cantor_{m+s(n)}2ord(pr_{m+s(n)}(cantor_{m+n}2cantor_{m+s(n)}(goodstein(m)(p)(n)))) =$$
$$cantor_{m+s(n)}2ord(goodstein(m)(p)(s(n)))$$

e possiamo concludere.

B.3 Lemmi

Lemma B.4
$\forall m : N.\forall x : Cantor(m).(nf_m(x) = x) \rightarrow inc(x) > x$
Dim. *Per induzione sulla struttura di x.*

Se $x = 0$ *dobbiamo dimostrare* $inc(0) > 0$ *che per definizione di inc equivale a dimostrare* $< s(0), 0, 0 > > 0$.

Se $x =< n', \alpha, \beta >$ *dobbiamo mostrare*

$$inc(< n', \alpha, \beta >) \ > < n', \alpha, \beta >$$

e per ipotesi induttiva su α *e* β *abbiamo*

$$inc(\alpha) > \alpha$$
$$inc(\beta) > \beta$$

Ragioniamo per casi sulle possibili trasformazioni operate da inc su $< n', \alpha, \beta >$*:*

- $\alpha = snd(inc(\beta))$ *e* $n' < pred(m)$
  In tal caso applicando inc otteniamo

  $$inc(< n', snd(inc(\beta)), \beta >) =< s(n'), snd(inc(\beta)), 0 >$$

  e dobbiamo quindi mostrare che

  $$< s(n'), snd(inc(\beta)), 0 >) \ >$$

  $$< n', snd(inc(\beta)), \beta >.$$

  Ora questo, per la definizione di $>$ *equivale a mostrare*

  $$s(n') > n'.$$

- *(*$\alpha = snd(inc(\beta))$ *e* $n' = pred(m)$*) In tal caso*

  $$inc(< n', snd(inc(\beta)), \beta >) =< s(0), inc(snd(inc(\beta))), 0 >$$

  e dobbiamo quindi mostrare che

  $$< s(0), inc(snd(inc(\beta))), 0 > > < n', snd(inc(\beta)), \beta >.$$

  Per definizione di $>$ *questo equivale a mostrare*

  $$inc(snd(inc(\beta))) = inc(\alpha) > \alpha = snd(inc(\beta)$$

  che vale per ipotesi induttiva su α.

- *(caso di default) Nel caso in cui nessuna delle condizioni precedenti dovesse verificarsi otteniamo*

  $$inc(< n', \alpha, \beta >) =< n', \alpha, inc(\beta) >$$

e dobbiamo quindi mostrare che

$$< n', \alpha, inc(\beta >) > > < n', \alpha, \beta >.$$

Per la definizione di $>$ *questo equivale a mostrare* $inc(\beta) > \beta$ *che vale per ipotesi induttiva su* β.

Lemma B.5
$\forall m : N.\forall x : Cantor(m).(nf_m(x) = x \wedge x! = 0_m) \rightarrow \ n2cantor_m(pred(cantor_m 2n(x))) < x$
Dim.
Per ipotesi $nf_m(x) = x$ *e quindi dimostrare*

$$n2cantor_m(pred(cantor_m 2n(x))) < x$$

equivale a dimostrare

$$n2cantor_m(pred(cantor_m 2n(x))) < n2cantor_m(cantor_m 2n(x)).$$

Ora, dato che per ipotesi $x! = 0_m$ *e quindi, per definizione di* $cantor_m 2n$, $cantor_m 2n(x)! = 0$, *possiamo riscrivere la disuguaglianza come*

$$n2cantor_m(pred(cantor_m 2n(x))) < n2cantor_m(s(pred(cantor_m 2n(x)))).$$

Per il Teorema 1 del Capitolo 4

$$n2cantor_m(s(pred(cantor_m 2n(x)))) = inc(n2cantor_m(pred(cantor_m 2n(x))))$$

e possiamo quindi concludere per il Lemma B.4 .

Lemma B.6
$\forall m : N.\forall x : Cantor(m).\forall y : Cantor(m).x = y \rightarrow cantor_m 2ord(x) = cantor_m 2ord(y)$
Dim. *Per induzione sulla struttura di x.*

Se $x = y = 0_m$ *allora* $cantor_m 2ord(x) = 0 = cantor_m 2ord(y)$.
Se $x =< n', \alpha, \beta >$ *dobbiamo dimostrare*

$$< n', \alpha, \beta > = \ y \rightarrow cantor_m 2ord(< n', \alpha, \beta >) = cantor_m 2ord(y)$$

e per ipotesi induttiva su α *e* β *abbiamo che*

$$\forall y : Cantor(m).\alpha = y \rightarrow cantor_m 2ord(\alpha) = cantor_m 2ord(y)$$

$$\forall y : Cantor(m).\beta = y \rightarrow cantor_m 2ord(\beta) = cantor_m 2ord(y).$$

Ora a partire da $< n', \alpha, \beta > = \ y$ *otteniamo*

$$fst(< n', \alpha, \beta >) = n' = fst(y),$$

$$snd(< n', \alpha, \beta >) = \alpha = snd(y),$$

$$trd(< n', \alpha, \beta >) = \beta = trd(y)$$

e applicando le ipotesi induttive otteniamo

$$cantor_m 2ord(\alpha) = cantor_m 2ord(snd(y))$$

e

$$cantor_m 2ord(\beta) = cantor_m 2ord(trd(y)).$$

Possiamo quindi concludere poichè

$$cantor_m 2ord(< n', \alpha, \beta >) =< n', cantor_m 2ord(\alpha), cantor_m 2ord(\beta) >=$$

$$< fst(y), cantor_m 2ord(snd(y)), cantor_m 2ord(trd(y)) >= cantor_m 2ord(y).$$

Lemma B.7
$\forall m : N.\forall x : Cantor(m).\forall y : Cantor(m).x < y \to cantor_m 2ord(x) < cantor_m 2ord(y)$
Dim. *Per induzione sulla struttura di x.*

Se $x = 0_m$ allora $cantor_m 2ord(0_m) = 0$ e $0 < y$ per definizione di $<$ sugli ordinali.
Se $x =< n', \alpha, \beta >$ dobbiamo dimostrare

$$< n', \alpha, \beta > < \ y \to cantor_m 2ord(< n', \alpha, \beta >) < cantor_m 2ord(y)$$

e per ipotesi induttiva su α e β abbiamo che

$$\forall y : Cantor(m).\alpha < y \to cantor_m 2ord(\alpha) < cantor_m 2ord(y)$$

$$\forall y : Cantor(m).\beta < y \to cantor_m 2ord(\beta) < cantor_m 2ord(y).$$

Ragioniamo ora sull'ultimo passo della funzione $<$:

- $\alpha < snd(y)$
  In tal caso per ipotesi induttiva su α abbiamo

  $$cantor_m 2ord(\alpha) < cantor_m 2ord(snd(y))$$

  che per definizione di $<$ implica

  $$cantor_m 2ord(< n', \alpha, \beta >) = (< n', cantor_m 2n(\alpha), cantor_m 2n(\beta) >) \ <$$

  $$(< fst(y), cantor_m 2ord(snd(y)), cantor_m 2ord(trd(y)) >) = cantor_m 2ord(y)$$

  se $cantor_m 2n(y)! = 0$. Nel caso in cui avessimo $y = 0$, ciò contraddirrebbe l'ipotesi $x < y$.

- $\alpha = snd(y) \wedge n' < fst(y)$
  In tal caso per il Lemma B.6

$$cantor_m 2ord(\alpha) = cantor_m 2ord(snd(y))$$

e poichè

$$fst(cantor_m 2ord(< n', \alpha, \beta >)) = n' < fst(y) = fst(cantor_m 2ord(y))$$

abbiamo

$$cantor_m 2ord(< n', \alpha, \beta >) < cantor_m 2ord(y).$$

- $\alpha = snd(y) \wedge n' = fst(y) \wedge \beta < trd(y)$
  In tal caso per il Lemma B.6

$$cantor_m 2ord(\alpha) = cantor_m 2ord(snd(y))$$

e poichè

$$fst(cantor_m 2ord(< n', \alpha, \beta >)) = n' = fst(y) = fst(cantor_m 2ord(y))$$

e per ipotesi induttiva vale

$$cantor_m 2ord(\beta) < cantor_m 2ord(trdy))$$

abbiamo

$$cantor_m 2ord(< n', \alpha, \beta >) < cantor_m 2ord(y)$$

Lemma B.8
$\forall n : N.(n! = 0) \rightarrow \; n2cantor_m(n) =< fst(n2cantor_m(n)), n2cantor_m(cantor_m 2n(snd(n2cantor_m(n)))),$
$n2cantor_m(cantor_m 2n(trd(n2cantor_m(n)))) >$
Dim. *Per induzione su n.*
Per ipotesi induttiva abbiamo che

$$\begin{aligned}(k! = 0) \rightarrow \; n2cantor_m(k) \quad = \quad & < fst(n2cantor_m(k)), \\ & n2cantor_m(cantor_m 2n(snd(n2cantor_m(k)))), \\ & n2cantor_m(cantor_m 2n(trd(n2cantor_m(k)))) >\end{aligned}$$

e dobbiamo dimostrare che

$$\begin{aligned}(s(k)! = 0) \rightarrow \; n2cantor_m(s(k)) \quad = \quad & < fst(n2cantor_m(s(k))), \\ & n2cantor_m(cantor_m 2n(snd(n2cantor_m(s(k))))), \\ & n2cantor_m(cantor_m 2n(trd(n2cantor_m(s(k))))) > .\end{aligned}$$

Nel caso in cui $s(k) = s(0)$ *abbiamo che*

$$\begin{aligned}
n2cantor_m(s(0)) =< s(0), 0, 0 > \quad &= \quad < fst(n2cantor_m(s(0))),\\
&\qquad n2cantor_m(cantor_m 2n(0)),\\
&\qquad n2cantor_m(cantor_m 2n(0)) >\\
&= \quad < fst(n2cantor_m(s(0))),\\
&\qquad n2cantor_m(cantor_m 2n(snd(n2cantor_m(s(0))))),\\
&\qquad n2cantor_m(cantor_m 2n(trd(n2cantor_m(s(0))))) > .
\end{aligned}$$

Se $s(k)! = s(0)$ *allora* $n! = 0$ *e quindi applicando l'ipotesi induttiva otteniamo*

$$\begin{aligned}
n2cantor_m(k) \quad &= \quad < fst(n2cantor_m(k)),\\
&\qquad n2cantor_m(cantor_m 2n(snd(n2cantor_m(k)))),\\
&\qquad n2cantor_m(cantor_m 2n(trd(n2cantor_m(k)))) > .
\end{aligned}$$

Ora dato che per il Teorema 1 del Capitolo 4

$$n2cantor_m(s(k)) = inc(n2cantor_m(k))$$

dobbiamo mostrare che

$$\begin{aligned}
< fst(n2cantor_m(s(k))),&\\
n2cantor_m(cantor_m 2n(snd(n2cantor_m(s(k))))),&\\
n2cantor_m(cantor_m 2n(trd(n2cantor_m(s(k))))) > \quad &=\\
inc(n2cantor_m(k)) \quad &=\\
inc(< fst(n2cantor_m(k)),&\\
n2cantor_m(cantor_m 2n(snd(n2cantor_m(k)))),&\\
n2cantor_m(cantor_m 2n(trd(n2cantor_m(k)))) >).&
\end{aligned}$$

Ragioniamo sulle possibili trasformazioni operate da inc su $n2cantor_m(k)$ *ricordandoci che*

$$\begin{aligned}
n2cantor_m(k) \quad &= \quad < fst(n2cantor_m(k)),\\
&\qquad snd(n2cantor_m(k)),\\
&\qquad trd(n2cantor_m(k)) >\\
&\qquad =< fst(n2cantor_m(k)),\\
&\qquad n2cantor_m(cantor_m 2n(snd(n2cantor_m(k)))),\\
&\qquad n2cantor_m(cantor_m 2n(trd(n2cantor_m(k)))) >
\end{aligned}$$

e quindi

$$\begin{aligned}
&snd(n2cantor_m(k)) = n2cantor_m(cantor_m 2n(snd(n2cantor_m(k))))\\
&trd(n2cantor_m(k)) = n2cantor_m(cantor_m 2n(trd(n2cantor_m(k)))).
\end{aligned}$$

- $n2cantor_m(cantor_m2n(snd(n2cantor_m(k)))) =$
  $snd(inc(n2cantor_m(cantor_m2n(trd(n2cantor_m(k))))))$
  e $fst(n2cantor_m(k)) < pred(m)$.
  In tal caso

  $$\begin{array}{rcl} inc(n2cantor_m(k)) & = & < s(fst(n2cantor_m(k))), \\ & & n2cantor_m(cantor_m2n(snd(n2cantor_m(k)))), 0 > . \end{array}$$

  Ora, dato che $n2cantor_m(s(k)) = inc(n2cantor_m(k))$, *per il Lemma B.12 otteniamo*

  $$\begin{array}{rcl} s(fst(n2cantor_m(k))) & = & fst(inc(n2cantor_m(k))) \\ & = & fst(n2cantor_m(s(k))), \end{array}$$

  $$\begin{array}{l} n2cantor_m(cantor_m2n(snd(n2cantor_m(k)))) = \\ n2cantor_m(cantor_m2n(snd(inc(n2cantor_m(k))))) = \\ n2cantor_m(cantor_m2n(snd(n2cantor_m(s(k))))) \end{array}$$

  e

  $$\begin{array}{rcl} 0 & = & n2cantor_m(cantor_m2n(0)) \\ & = & n2cantor_m(cantor_m2n(trd(inc(n2cantor_m(k))))) \\ & = & n2cantor_m(cantor_m2n(trd(n2cantor_m(s(k))))). \end{array}$$

  Abbiamo quindi mostrato che

  $$\begin{array}{rcl} inc(n2cantor_m(k)) & = & < s(fst(n2cantor_m(k))), \\ & & n2cantor_m(cantor_m2n(snd(n2cantor_m(k)))), 0 > \\ & = & < fst(n2cantor_m(s(k))), \\ & & n2cantor_m(cantor_m2n(snd(n2cantor_m(s(k))))), \\ & & n2cantor_m(cantor_m2n(trd(n2cantor_m(s(k))))) > . \end{array}$$

- $n2cantor_m(cantor_m2n(snd(n2cantor_m(k)))) =$
  $snd(inc(n2cantor_m(cantor_m2n(trd(n2cantor_m(k))))))$
  e $fst(n2cantor_m(k)) = pred(m)$.
  In tal caso

  $$\begin{array}{rcl} inc(n2cantor_m(k)) & = & < s(0), \\ & & inc(n2cantor_m(cantor_m2n(snd(n2cantor_m(k))))), 0 > . \end{array}$$

  Ora, dato che $n2cantor_m(s(k)) = inc(n2cantor_m(k))$, *per il Lemma B.13 otteniamo*

  $$s(0) = fst(inc(n2cantor_m(k))) = fst(n2cantor_m(s(k))),$$

$$inc(n2cantor_m(cantor_m2n(snd(n2cantor_m(k))))) =$$
$$n2cantor_m(s(cantor_m2n(snd(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(inc(snd(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(snd(inc(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(snd(n2cantor_m(s(k)))))$$

dove abbiamo sfruttato i Teoremi 1 e 2 del Capitolo 4 nel primo e secondo passaggio, e

$$0 = n2cantor_m(cantor_m2n(0)) =$$
$$n2cantor_m(cantor_m2n(trd(inc(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(trd(n2cantor_m(s(k))))).$$

Abbiamo quindi mostrato che

$$\begin{aligned} inc(n2cantor_m(k)) &= < s(0), \\ & \quad inc(n2cantor_m(cantor_m2n(snd(n2cantor_m(k))))), 0 > \\ &= < fst(n2cantor_m(s(k))), \\ & \quad n2cantor_m(cantor_m2n(snd(n2cantor_m(s(k))))), \\ & \quad n2cantor_m(cantor_m2n(trd(n2cantor_m(s(k))))) > . \end{aligned}$$

- *(caso di default) Nel caso in cui nessuna delle condizioni precedenti dovesse verificarsi otteniamo*

$$\begin{aligned} inc(n2cantor_m(k)) &= < fst(n2cantor_m(k)), \\ & \quad n2cantor_m(cantor_m2n(snd(n2cantor_m(k)))), \\ & \quad inc(n2cantor_m(cantor_m2n(trd(n2cantor_m(k))))) > . \end{aligned}$$

Ora, dato che $n2cantor_m(s(k)) = inc(n2cantor_m(k))$*, per il Lemma B.14 otteniamo*

$$fst(n2cantor_m(k)) = fst(inc(n2cantor_m(k))) = fst(n2cantor_m(s(k))),$$

$$n2cantor_m(cantor_m2n(snd(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(snd(inc(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(snd(n2cantor_m(s(k)))))$$

e

$$inc(n2cantor_m(cantor_m2n(trd(n2cantor_m(k))))) =$$
$$n2cantor_m(s(cantor_m2n(trd(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(inc(trd(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(trd(inc(n2cantor_m(k))))) =$$
$$n2cantor_m(cantor_m2n(trd(n2cantor_m(s(k)))))$$

dove abbiamo sfruttato i Teoremi 1 e 2 del Capitolo 4 nel primo e secondo passaggio.
Abbiamo quindi mostrato che

$$\begin{aligned} inc(n2cantor_m(k)) &= \; < fst(n2cantor_m(k)), \\ &\quad n2cantor_m(cantor_m2n(snd(n2cantor_m(k)))), \\ &\quad inc(n2cantor_m(cantor_m2n(trd(n2cantor_m(k))))) > \\ &= \; < fst(n2cantor_m(s(k))), \\ &\quad n2cantor_m(cantor_m2n(snd(n2cantor_m(s(k))))), \\ &\quad n2cantor_m(cantor_m2n(trd(n2cantor_m(s(k))))) > . \end{aligned}$$

Lemma B.9
$\forall m : N.\forall x : Cantor(m).nf_m(x) = x \rightarrow (nf_m(snd(x)) = snd(x) \wedge nf_m(trd(x)) = trd(x))$
Dim.
Se $x = 0$ *possiamo concludere poichè* $snd(0) = 0 = nf_m(0)$ *e* $trd(0) = 0 = nf_m(0)$.
Se $x =< n', \alpha, \beta >$ *applicando il Lemma B.8 a* $cantor_m2n(x)$ *otteniamo*

$$\begin{aligned} n2cantor_m(cantor_m2n(x)) &= \; < fst(n2cantor_m(ncantor_m2n(x))), \\ &\quad n2cantor_m(cantor_m2n(snd(n2cantor_m(ncantor_m2n(x))))), \\ &\quad n2cantor_m(cantor_m2n(trd(n2cantor_m(ncantor_m2n(x))))) > \end{aligned}$$

e sfruttando l'ipotesi ($nf_m(x) = x$) *e la definizione di* nf_m *otteniamo*

$$x =< fst(x), nf_m(snd(x)), nf_m(trd(x)) >.$$

Ora, poichè $x =< fst(x), snd(x), trd(x) >$, *applicando snd e trd otteniamo*

$$snd(x) = snd(< fst(x), nf_m(snd(x)), nf_m(trd(x)) >) = nf_m(snd(x))$$
$$trd(x) = trd(< fst(x), nf_m(snd(x)), nf_m(trd(x)) >) = nf_m(trd(x)).$$

Lemma B.10
$\forall m.\forall x : Cantor(m).(fst(x) < m \wedge ((x! = 0 \;\wedge\; snd(x)! = 0) \rightarrow \; snd(x) > snd(trd(x))) \wedge ((x! = 0 \;\wedge\; snd(x) = 0) \rightarrow \; trd(x) = 0) \wedge nf_m(snd(x)) = snd(x) \wedge nf_m(trd(x)) = trd(x)) \rightarrow nf_m(x) = x$
Dim. *Diamo solo uno sketch della dimostrazione.*
A partire dalle ipotesi è infatti possibile mostrare, per la decidibilità dell'uguaglianza, che se non avessimo $nf_m(x) = x$ *otterremmo una contraddizione, ovvero otterremmo* $nf_m(snd(x))! = snd(x)$ *o* $nf_m(trd(x))! = trd(x)$).

Lemma B.11
$\forall m.\forall x : Cantor(m).nf_m(x) = x \rightarrow nf_{s(m)}(cantor_m2cantor_{s(m)}(x)) = x$ ***Dim.*** *Per induzione sulla struttura di x.*
Se $x = 0_m$ *il Lemma vale poichè* $0_{s(m)} = nf_{s(m)}(0_{s(m)})$.
se $x =< n', \alpha, \beta >_m$ *il Lemma vale per l'ipotesi induttiva su* α *e* β *e per il Lemma B.10.*

Lemma B.12
$\forall m : N.\forall x : Cantor(m).(x! = 0 \ \wedge \ nf_m(x) = x \ \wedge \ snd(x) = snd(inc(trd(x))) \ \wedge \ fst(x) < pred(m)) \rightarrow (fst(inc(x)) = s(fst(x)) \ \wedge \ snd(inc(x)) = snd(x) \ \wedge \ trd(inc(x)) = 0)$
Dim.
Applicando inc a x otteniamo

$$inc(x) = inc(< fst(x), snd(x), trd(x) >) =< s(fst(x)), snd(x), 0 >$$

dato che per ipotesi $snd(x) = snd(inc(trd(x))$ *e* $fst(x) < pred(m)$*. Possiamo quindi concludere poichè applicando le funzioni fst, snd, trd al nuovo oggetto otteniamo*

$$fst(inc(x)) = fst(< s(fst(x)), snd(x), 0 >) = s(fst(x))$$

$$snd(inc(x)) = snd(< s(fst(x)), snd(x), 0 >) = snd(x)$$

$$trd(inc(x)) = trd(< s(fst(x)), snd(x), 0 >) = 0)$$

Lemma B.13
$\forall m : N.\forall x : Cantor(m).(x! = 0 \ \wedge \ nf_m(x) = x \ \wedge \ snd(x) = snd(inc(trd(x))) \ \wedge \ fst(x) = pred(m)) \rightarrow (fst(inc(x)) = s(0) \ \wedge \ snd(inc(x)) = inc(snd(x)) \ \wedge \ trd(inc(x)) = 0)$
Dim.
Applicando inc a x otteniamo

$$inc(x) = inc(< fst(x), snd(x), trd(x) >) =< s(0), inc(snd(x)), 0 >$$

dato che per ipotesi $snd(x) = snd(inc(trd(x))$ *e* $fst(x) = pred(m)$*. Possiamo quindi concludere poichè applicando le funzioni fst, snd, trd al nuovo oggetto otteniamo*

$$fst(inc(x)) = fst(< s(0), inc(snd(x)), 0 >) = s(0)$$

$$snd(inc(x)) = snd(< s(0), inc(snd(x)), 0 >) = inc(snd(x))$$

$$trd(inc(x)) = trd(< s(0), inc(snd(x)), 0 >) = 0)$$

Lemma B.14
$\forall m : N.\forall x : Cantor(m).(x! = 0 \wedge nf_m(x) = x \wedge snd(x)! = snd(inc(trd(x)))) \rightarrow (fst(inc(x)) = fst(x) \ \wedge \ snd(inc(x)) = snd(x) \ \wedge \ trd(inc(x)) = inc(trd(x)))$
Dim.
Applicando inc a x otteniamo

$$inc(x) = inc(< fst(x), snd(x), trd(x) >) =< fst(x), snd(x), inc(trd(x)) >$$

dato che per ipotesi $snd(x)! = snd(inc(trd(x))$*. Possiamo quindi concludere poichè applicando le funzioni fst, snd, trd al nuovo oggetto otteniamo*

$$fst(inc(x)) = fst(< fst(x), snd(x), inc(trd(x)) >) = fst(x)$$

$$snd(inc(x)) = snd(< fst(x), snd(x), inc(trd(x)) >) = snd(x)$$

$$trd(inc(x)) = trd(< fst(x), snd(x), inc(trd(x)) >) = inc(trd(x))$$

Bibliografia

[Bishop67] Errett Bishop. Foundations of Constructive Analysis, McGraw-Hill, New York, 1967.

[Cantor92] Georg Cantor. La formazione della teoria degli insiemi, a cura di Gianni Rigamonti,BUS, 1992.

[Dybjer91] Peter Dybjer. Inductive sets and families in Martin-Löf's type theory and their set-theoretic semantics, in Logical Frameworks, 1991, editors Gerard Huet and Gordon Plotkin, pp 280-306, Prentice Hall.

[Girard72] J.Y.Girard. Interprètation fonctionelle et èlimininination des coupures de l'arìthmètique d'ordre supèrieur, Thèse, Universitè Paris 7, 1972

[Goodstein44] R.Goodstein. On the restricted ordinal theorem, Journal of Symbolic Logic, Vol 9, pp. 33-41,1944.

[Hamilton82] A.G.Hamilton. Numbers, sets and axioms, Cambridge University Press, 1982.

[Hancock00] Peter Hancock. Ordinals and Interactive Programs. PhD dissertation, University of Edinburgh, 2000.

[KirbyParis77] Paris, J. and Harrington, L. A mathematical incompleteness in Peano Arithmetic. Studies in Logic and the Foundations of Mathematics 90. Handbook of Mathematical Logic. New York: North-Holland Publishing Company. 1977.

[KirbyParis82] L.Kirby,J.Paris. Accessible independence results for Peano arithmetic, Bull. London Math. Soc., Vol 14, pp. 285-93,1982.

[Martin-Lof71] Per Martin-Lof. A Theory of Types. Technical Report 71-3, University of Stockholm, 1971.

[Martin-Lof84] Per Martin-Lof. Intuitionistic Type Theory. Bibliopolis, Napoli, 1984.

[Martin-Lof75] Per Martin-Lof. An Intuitionistic Theory of Types: Predicative Part. In H. E. Rose and J. C. Shepherdson, editors, Logic Colloquium 1973, pages 73-118, Amsterdam, 1975. North-Holland Publishing Company.

[Martin-Lof96] Per Martin-Lof.On the Meaning of the logical constants and the justifications of the logical laws, Nordic Journal of Philosophical Logic, Vol.1, No.1, pp. 11-60,Scandinavian University Press, 1982.

[Sierpinski65] Waclaw Sierpinski. Cardinal and Ordinal Numbers,Polish Scientific Publishers, 1965.

[Simpson88] Stephen G. Simpson. Ordinal Numbers and the Hilbert Basis Theorem, The Journal of Symbolic Logic, Vol. 53, No. 3. (Sep., 1988), pp. 961-974.

[Taylor96] Paul Taylor. Intuitionistic Sets and Ordinals, The Journal of Symbolic Logic, Vol. 61, No. 3. (Sep., 1996), pp. 705-744.

[Valentini] Silvio Valentini. Formal topology and combinatorics. In fase di pubblicazione.