

Corso istituzionale di Teoria degli Insiemi

Alberto Marcone

Dipartimento di Matematica e Informatica
Università di Udine

`alberto.marcone@dimi.uniud.it`

`http://www.dimi.uniud.it/marcone`

Scuola Estiva AILA 2011
Gargnano, 22–27 agosto 2011

Schema delle lezioni

- 1 Teoria degli Insiemi
- 2 L'aritmetica del second'ordine
- 3 Il sistema base per la *reverse mathematics*
- 4 Comprensione aritmetica
- 5 Un principio di compattezza
- 6 Ricorsione transfinita e oltre

Teoria degli Insiemi

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

- ➊ Introduzione e teoria ingenua degli insiemi
- ➋ La teoria ZF
- ➌ L'assioma della scelta e ZFC
- ➍ Risultati di indipendenza

La teoria degli insiemi

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

La teoria degli insiemi è una teoria matematica di interesse autonomo, ma può anche essere vista come una “fondazione della matematica”.

Certamente la nozione di insieme è tra le più fondamentali in matematica.

Gli oggetti studiati in algebra, analisi, geometria, sono definiti come insiemi dotati di qualche struttura addizionale.

La teoria degli insiemi vuole analizzare a fondo il concetto di insieme, e per farlo procede in modo assiomatico.

Come vedere l'assiomatizzazione

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

L'assiomatizzazione della teoria degli insiemi è, per certi aspetti, diversa dall'assiomatizzazione della teoria dei gruppi.

Gli assiomi dei gruppi vogliono catturare alcune proprietà comuni ad un'ampia collezione di strutture algebriche: gli assiomi isolano queste proprietà comuni per poi mostrare che esse implicano altre proprietà, che saranno quindi condivise da tutte le strutture algebriche in esame.

In teoria degli insiemi non abbiamo (almeno a priori) una "collezione di strutture insiemistiche" di cui vogliamo isolare le proprietà comuni, ma piuttosto una nozione intuitiva di insieme.

Questa situazione è simile a quella geometria euclidea che attraverso una collezione di assiomi cerca di catturare formalmente le proprietà dei concetti intuitivi di punto, retta. . .

Insiemi ereditari

Lo slogan della teoria degli insiemi è

tutto è insieme

Quindi non consideriamo per esempio all'insieme delle persone in questa stanza, i cui elementi non sono insiemi.

Consideriamo solamente insiemi i cui elementi sono insiemi, i cui elementi sono insiemi, i cui elementi sono insiemi, . . .

Chiameremo questi oggetti *insiemi ereditari*.

- Ogni elemento di un insieme ereditario è un insieme ereditario;
- un insieme di insiemi ereditari è un insieme ereditario.

Brevi cenni storici

- A partire dal 1874 Georg Cantor, motivato inizialmente da questioni sulla convergenza delle successioni trigonometriche, considera insiemi “arbitrari” di reali.
- Spinto dalle sue ricerche Cantor inizia a formulare una prima teoria degli insiemi, introducendo la nozione di cardinalità e poi gli ordinali.
- Alla fine dell’800 Frege propone una prima sistemazione assiomatica rigorosa della teoria degli insiemi, che viene demolita dal paradosso di Russell.
- In seguito al paradosso di Russell emerge l’assiomatizzazione di Zermelo-Fraenkel (1908-22), che è quella che vedremo tra poco.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L’assioma
della scelta e
ZFC

Risultati di
indipendenza

La teoria ingenua degli insiemi

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

La nostra intuizione ci suggerisce che se $P(x)$ è una “proprietà” esiste l'insieme degli oggetti che soddisfano P : $\{x \mid P(x)\}$.

Questo è l'assioma di comprensione, e su di esso si basava Cantor e poggiava l'assiomatizzazione di Frege.

Se però $P(x)$ è

x è un insieme che non appartiene a se stesso

e $y = \{x \mid P(x)\}$ si arriva ad una contraddizione:

- se $y \in y$ allora $\neg P(y)$ e $y \notin y$;
- se $y \notin y$ allora $P(y)$ e $y \in y$.

Questo è il paradosso di Russell.

Il linguaggio \mathcal{L}_\in

Il linguaggio della teoria degli insiemi è un linguaggio del prim'ordine con uguaglianza ed un solo simbolo non logico: l'appartenenza \in che è un simbolo di relazione binario.

Abbrevieremo $\in(x, y)$ con $x \in y$ e $\neg(x \in y)$ con $x \notin y$.

Gli unici termini sono le variabili.

Esempi di formule di \mathcal{L}_\in :

$$x \in y \vee \neg(x \in z \wedge w = x) \quad \forall x \exists y y \notin x$$

$$\forall x(x \in y \rightarrow x \neq w) \quad \exists y(y \in x \wedge x \notin y)$$

Le ultime due formule sono abbreviate da

$$\forall x \in y(x \neq w) \text{ e } \exists y \in x(x \notin y).$$

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio

I primi assiomi

Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Estensioni di \mathcal{L}_\in

\mathcal{L}_\in verrà progressivamente ampliato attraverso estensioni per definizione:

- nuovi simboli relazionali si limitano ad abbreviare formule più complesse;
- nuovi simboli di funzione e costante vengono introdotti quando gli assiomi garantiscono le condizioni di esistenza e unicità necessarie.

Il simbolo di relazione \subseteq è tale che $x \subseteq y$ sta per $\forall z \in x \ z \in Y$.

Se abbiamo dimostrato $\exists! z \forall x \ x \notin z$ possiamo estendere il linguaggio con il simbolo di costante \emptyset e aggiungere l'assioma definitorio $\forall x \ x \notin \emptyset$.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio

I primi assiomi

Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

L'assioma di estensionalità

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio

I primi assiomi

Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Assioma di esistenza di insiemi

$$\exists x x = x$$

Questo assioma (a volte) fa parte della logica.

Assioma di estensionalità

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

Questo assioma afferma che un insieme è individuato completamente dai suoi elementi.

Ciò è giustificato dal fatto che gli elementi di un insieme ereditario sono a loro volta insiemi.

Lo schema di separazione

Vogliamo introdurre un assioma che affermi che possiamo formare l'insieme degli insiemi che soddisfano una certa proprietà, ma vogliamo evitare il paradosso di Russell.

Schema di separazione

Se $\varphi(x)$ è una formula in cui y non occorre libera, è un'assioma di separazione la chiusura universale di:

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

Questo assioma asserisce che, dato un insieme z possiamo *separare* al suo interno gli elementi che soddisfano φ , e formare con essi un nuovo insieme.

Rispetto alla comprensione è comparso $x \in z$.

Usando estensionalità si vede subito che l' y di cui si asserisce l'esistenza è unico, e lo denotiamo con $\{x \in z \mid \varphi(x)\}$.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio

I primi assiomi

Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

L'esistenza di \emptyset

Lemma

Esiste un unico insieme z tale che $\forall x x \notin z$.

Dimostrazione.

Sia y un insieme la cui esistenza è garantita dall'assioma di esistenza di insiemi.

Per separazione sia $z = \{x \in y \mid x \neq x\}$.

E' chiaro che $\forall x x \notin z$.

L'unicità di z è garantita dall'assioma di estensionalità. □

Come già annunciato, indicheremo con \emptyset l'insieme di cui abbiamo provato esistenza e unicità.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

L'esistenza dell'intersezione

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio

I primi assiomi

Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Lemma

Dati x e y esiste un unico insieme z tale che

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

Dimostrazione.

Per separazione sia $z = \{u \in x \mid u \in y\}$.

z ha la proprietà richiesta e l'unicità segue dall'assioma di estensionalità. □

Indicheremo con $x \cap y$ l'insieme di cui abbiamo provato esistenza e unicità.

Il paradosso di Russell in ZF

Teorema

Non esiste un insieme z tale che $\forall x x \in z$.

Dimostrazione.

Per assurdo se esiste un tale z poniamo $y = \{x \in z \mid x \notin x\}$.
Dato che $y \in z$ si ha $y \in y \leftrightarrow y \notin y$, contraddizione. \square

Il paradosso di Russell è diventato un teorema della teoria degli insiemi.

Il teorema asserisce che non esiste l'insieme di tutti gli insiemi: quella "collezione" è troppo grande per essere un insieme.

In teoria degli insiemi usiamo informalmente $\{x \mid \varphi(x)\}$ per denotare una *classe*, che non sempre è un insieme.

Abbiamo mostrato che $\mathbb{V} = \{x \mid x = x\}$ e $\{x \mid x \notin x\}$ non sono insiemi, ma **classi proprie**.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza
L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

L'assioma della coppia

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Gli assiomi introdotti finora non garantiscono l'esistenza di nessun insieme oltre a \emptyset . Infatti se l'universo contiene solo \emptyset i tre assiomi sono soddisfatti.

Introduciamo ora assiomi che affermano l'esistenza di insiemi più complessi di quelli di partenza.

Assioma della coppia

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

Lo z di cui si afferma l'esistenza è unico per estensionalità e lo indichiamo con $\{x, y\}$.

Quando $x = y$ usiamo $\{x\}$ al posto di $\{x, x\}$.

Abbiamo quindi “nuovi” insiemi: $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}\}$, ecc

Coppie ordinate

Definiamo ora $\langle x, y \rangle = \{\{x\}, \{x, y\}\}$.

$\langle x, y \rangle$ rappresenta la **coppia ordinata** formata da x e y in quest'ordine (notare che $\langle x, y \rangle \neq \langle y, x \rangle$ quando $x \neq y$).

Lemma

Se $\langle x, y \rangle = \langle u, v \rangle$ allora $x = u$ e $y = v$.

Dimostrazione.

Se $x \neq u$ allora $\{x\} \neq \{u\}$.

Dato che $\{x\} \in \langle x, y \rangle = \langle u, v \rangle$ deve essere $\{x\} = \{u, v\}$.

Ma allora $x = u$, contraddizione. Quindi $x = u$.

Se $y \neq v$ allora $\{x, y\} \neq \{x, v\} = \{u, v\}$.

Quindi $\{x, y\} = \{u\} = \{x\}$ e deve essere $x = y$.

Ma allora $\langle x, y \rangle = \{\{x\}\}$ e $\{u, v\} = \{x\}$.

Perciò $y = x = v$, contraddizione. Quindi $y = v$. □

L'assioma dell'unione

Gli assiomi introdotti finora garantiscono solo l'esistenza di insiemi con al più due elementi.

Assioma dell'unione

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

Lo z di cui si afferma l'esistenza è unico per estensionalità e lo indichiamo con $\bigcup x$. Poniamo anche $x \cup y = \bigcup \{x, y\}$.

Lemma

Per ogni x, y e z esiste un unico insieme $\{x, y, z\}$ tale che

$$\forall u (u \in \{x, y, z\} \leftrightarrow u = x \vee u = y \vee u = z).$$

Dimostrazione.

$$\{x, y, z\} = \bigcup \{\{x, y\}, \{z\}\}.$$



Intersezione

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio

I primi assiomi

Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Non c'è bisogno di un assioma dell'intersezione:

se $x \neq \emptyset$ e $y \in x$ allora $\{z \in y \mid \forall u \in x z \in u\}$ non dipende da y e può essere chiamato $\bigcap x$.

Avevamo già definito $x \cap y$, e si ha $x \cap y = \bigcap\{x, y\}$.

Lo schema di rimpiazzamento

Vorremmo costruire il prodotto cartesiano degli insiemi A e B .

Per farlo è utile, per $y \in B$, poter “rimpiazzare” A con l'insieme delle coppie ordinate $\langle x, y \rangle$ con $x \in A$.

Schema di rimpiazzamento

Se $\varphi(x, y)$ è una formula in cui Y non occorre libera, è un'assioma di rimpiazzamento la chiusura universale di:

$$\forall x \in A \exists! y \varphi(x, y) \rightarrow \exists Y \forall x \in A \exists y \in Y \varphi(x, y)$$

Questo assioma asserisce che, se $\forall x \in A \exists! y \varphi(x, y)$, possiamo *rimpiazzare* gli $x \in A$ con gli y che soddisfano $\varphi(x, y)$ e ottenere un nuovo insieme.

Infatti dato Y definiamo $Y' = \{y \in Y \mid \exists x \in A \varphi(x, y)\}$.

Y' è l'unico insieme tale che

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

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio

I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Immagini di insiemi

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi

Ordinali
Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Se $t(x)$ è un termine (ottenuto con i vari simboli di funzione introdotti) allora si ha $\forall x \in A \exists! y y = t(x)$.

Il rimpiazzamento assicura l'esistenza di un unico Y' tale che

$$\forall y (y \in Y' \leftrightarrow \exists x \in A y = t(x)).$$

Questo Y' viene indicato con $\{t(x) \mid x \in A\}$.

Il prodotto cartesiano

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinabili

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Dati A e B fissiamo $y \in B$.

Poniamo $\text{prod}(A, y) = \{ \langle x, y \rangle \mid x \in A \}$

e poi $\text{prod}'(A, B) = \{ \text{prod}(A, y) \mid y \in B \}$.

Definiamo $A \times B = \bigcup \text{prod}'(A, B)$.

Si verifica che

$$\forall u (u \in A \times B \leftrightarrow \exists x \in A \exists y \in B u = \langle x, y \rangle)$$

e quindi $A \times B$ è effettivamente il prodotto cartesiano di A e B .

Relazioni come insiemi

Diciamo che un insieme R è una **relazione** se i suoi elementi sono coppie ordinate, cioè se $\forall u \in R \exists x, y u = \langle x, y \rangle$.

Per qualsiasi R definiamo

$$\text{dom}(R) = \{x \in \bigcup \bigcup R \mid \exists y \langle x, y \rangle \in R\}$$

$$\text{ran}(R) = \{y \in \bigcup \bigcup R \mid \exists x \langle x, y \rangle \in R\}$$

R è una relazione se e solo se $R \subseteq \text{dom}(R) \times \text{ran}(R)$.

Spesso scriviamo $x R y$ al posto di $\langle x, y \rangle \in R$.

Un **ordine parziale** è una coppia $\langle A, R \rangle$ dove R è una relazione,

$$\forall x \in A \neg x R x \text{ e } \forall x, y, z \in A (x R y \wedge y R z \rightarrow x R z).$$

Un **ordine lineare** è un ordine parziale $\langle A, R \rangle$ tale che

$$\forall x, y \in A (x \neq y \rightarrow x R y \vee y R x).$$

Un **buon ordine** è un ordine lineare $\langle A, R \rangle$ tale che

$$\forall C (C \subseteq A \wedge C \neq \emptyset \rightarrow \exists x \in C \forall y \in C \neg y R x).$$

Funzioni come insiemi

Diciamo che un insieme f è una **funzione** se è una relazione e

$$\forall x \in \text{dom}(f) \exists! y \langle x, y \rangle \in f.$$

$f : A \rightarrow B$ significa

f è una funzione $\wedge \text{dom}(f) = A \wedge \text{ran}(f) \subseteq B$.

Se $f : A \rightarrow B$ e $x \in A$, $f(x)$ è l'unico y tale che $\langle x, y \rangle \in f$.

Se $C \subseteq A$ allora $f \upharpoonright C = f \cap (C \times B)$ è una funzione e poniamo $f''C = \text{ran}(f \upharpoonright C) = \{y \in B \mid \exists x \in C f(x) = y\}$. Questa notazione è diversa da quella dell'analisi, che usa $f(C)$.

Quando $C \subseteq A$ e $C \in A$ quella notazione sarebbe ambigua.

Iniezioni, suriezioni e biiezioni sono definite usualmente.

Siano R e S relazioni. Scriviamo $\langle A, R \rangle \cong \langle B, S \rangle$ se esiste una biiezione $f : A \rightarrow B$ tale che

$$\forall u, v \in A (u R v \leftrightarrow f(u) S f(v)).$$

Ordinali

Un insieme x è una **transitivo** se i suoi elementi sono anche suoi sottoinsiemi, cioè se $\forall y \in x \forall z \in y z \in x$.

Alcuni insiemi transitivi: \emptyset , $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$. Anche gli x tali che $x = \{x\}$.

Alcuni insiemi non transitivi: $\{\{\emptyset\}\}$, $\{\emptyset, \{\{\emptyset\}\}\}$.

Un **ordinale** è un insieme transitivo ben ordinato da \in , cioè $\langle x, \in_x \rangle$ è un buon ordine dove $\in_x = \{ \langle y, z \rangle \in x \times x \mid y \in z \}$.

Alcuni ordinali: \emptyset , $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

Un insieme transitivo che non è un ordinale è $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$. Infatti $\emptyset \in \{\emptyset\} \in \{\{\emptyset\}\}$ ma $\emptyset \notin \{\{\emptyset\}\}$ e quindi \in non è transitiva su questo insieme.

Se $x = \{x\}$, x non è un ordinale perché non ha elemento minimo.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza
L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Alcune proprietà degli ordinali

- 1 Se x è un ordinale e $y \in x$ allora y è un ordinale;
- 2 se x e y sono ordinali e $x \cong y$ (cioè $\langle x, \in_x \rangle \cong \langle y, \in_y \rangle$) allora $x = y$;
- 3 se x e y sono ordinali allora vale esattamente una tra $x \in y$, $x = y$, $y \in x$;
- 4 se x , y e z sono ordinali tali che $x \in y$ e $y \in z$ allora $x \in z$;
- 5 se $\langle A, R \rangle$ è un buon ordine allora esiste un unico ordinale x tale che $x \cong \langle A, R \rangle$.

Le lettere greche minuscole indicano sempre ordinali.

Scriviamo $\alpha < \beta$ al posto di $\alpha \in \beta$.

Insiemi di ordinali

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF
Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza
L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

- Se C è un insieme non vuoto di ordinali $\bigcap C$ è il suo minimo, denotato $\min C$;
- se C è un insieme di ordinali $\bigcap C$ è il suo estremo superiore, denotato $\sup C$;
- non esiste un insieme cui appartengono tutti gli ordinali (paradosso di Burali-Forti).

I naturali come ordinali

Per ogni insieme x poniamo $S(x) = x \cup \{x\}$.

Se x è un ordinale anche $S(x)$ lo è.

\emptyset è un ordinale e, quando visto come ordinale, lo scriviamo 0.

$1 = S(0) = \{0\}$, $2 = S(1) = \{0, 1\}$, $3 = S(2) = \{0, 1, 2\}$

$4 = S(3) = \{0, 1, 2, 3\}$, $5 = S(4) = \{0, 1, 2, 3, 4\}$, \dots

α è un **ordinale successore** se $\exists \beta \alpha = S(\beta)$.

α è un **ordinale limite** se $\alpha \neq 0$ non è un ordinale successore.

α è un **naturale** se $\forall \beta \leq \alpha (\beta = 0 \vee \beta \text{ è un successore})$.

Per ora non possiamo dimostrare l'esistenza dell'insieme dei naturali.

Le lettere $n, m, i, j, k, \ell, \dots$ indicano sempre naturali.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF
Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Induzione sugli ordinali

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF
Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza
L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Teorema (Induzione sugli ordinali)

Se φ è una formula per cui vale $\forall \alpha (\forall \beta < \alpha \varphi(\beta) \rightarrow \varphi(\alpha))$, allora $\forall \alpha \varphi(\alpha)$.

Teorema (Induzione per casi sugli ordinali)

Se φ è una formula per cui valgono

- $\varphi(0)$;
- $\forall \alpha (\varphi(\alpha) \rightarrow \varphi(S(\alpha)))$;
- $\forall \lambda (\lambda \text{ è limite} \wedge \forall \beta < \lambda \varphi(\beta) \rightarrow \varphi(\lambda))$;

allora $\forall \alpha \varphi(\alpha)$.

Induzione sui naturali

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Teorema (Induzione sui naturali)

Se φ è una formula per cui vale $\forall n (\forall m < n \varphi(m) \rightarrow \varphi(n))$, allora $\forall n \varphi(n)$.

Teorema (Induzione per casi sui naturali)

Se φ è una formula per cui valgono

- $\varphi(0)$;
- $\forall n (\varphi(n) \rightarrow \varphi(S(n)))$;

allora $\forall n \varphi(n)$.

L'assioma dell'infinito

Gli assiomi introdotti finora garantiscono solo l'esistenza di insiemi con un numero finito di elementi.

Assioma dell'infinito

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

Se y è l'insieme di cui l'assioma afferma l'esistenza è facile dimostrare per induzione che $\forall n n \in y$.

Allora si può definire l'insieme dei numeri naturali:

$$\omega = \{x \in y \mid x \text{ è un naturale}\}$$

che non dipende da y .

ω è un ordinale, il più piccolo ordinale limite.

Allora anche $S(\omega), S(S(\omega)), \dots$ sono ordinali.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Operazioni sugli ordinali

L'induzione sugli ordinali ci permette di effettuare definizioni per ricorsione sugli ordinali.

Senza descrivere in generale il procedimento, diamo alcuni esempi di operazioni che estendono quelle solite sui naturali:

somma $\alpha + 0 = \alpha$
 $\alpha + S(\beta) = S(\alpha + \beta)$
 $\alpha + \lambda = \sup\{\alpha + \beta \mid \beta < \lambda\};$

prodotto $\alpha \cdot 0 = 0$
 $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha$
 $\alpha \cdot \lambda = \sup\{\alpha \cdot \beta \mid \beta < \lambda\}.$

esponenziazione $\alpha^0 = 1$
 $\alpha^{S(\beta)} = \alpha^\beta \cdot \alpha$
 $\alpha^\lambda = \sup\{\alpha^\beta \mid \beta < \lambda\}.$

Con queste operazioni otteniamo $\omega + \omega, \omega \cdot \omega, \omega^\omega, \dots$

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Realizzazioni concrete di somma e prodotto ordinali

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

$\alpha + \beta$ può essere caratterizzato come l'unico ordinale isomorfo al buon ordine $\langle (\alpha \times \{0\}) \cup (\beta \times \{1\}), R \rangle$ dove

$$(\gamma, i) R (\delta, j) \leftrightarrow i < j \vee (i = j \wedge \gamma < \delta).$$

Analogamente $\alpha \cdot \beta$ è l'unico ordinale isomorfo al buon ordine $\langle \alpha \times \beta, R \rangle$ dove

$$(\gamma, \delta) R (\gamma', \delta') \leftrightarrow \delta < \delta' \vee (\delta = \delta' \wedge \gamma < \gamma').$$

Aritmetica ordinale

Somma e prodotto ordinali non sono commutativi:

- $1 + \omega = \omega < \omega + 1 = S(\omega)$;
- $2 \cdot \omega = \omega < \omega \cdot 2 = \omega + \omega$.

Per ogni α , β e γ

- $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$;
- $\alpha + 0 = 0 + \alpha = \alpha$ e $\alpha + 1 = S(\alpha)$;
- $\beta = \gamma$ se e solo se $\alpha + \beta = \alpha + \gamma$;
- $\beta < \gamma$ se e solo se $\alpha + \beta < \alpha + \gamma$;
- $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$;
- $\alpha \cdot 0 = 0 \cdot \alpha = 0$ e $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$;
- se $\alpha > 0$ allora $\beta = \gamma$ se e solo se $\alpha \cdot \beta = \alpha \cdot \gamma$;
- se $\alpha > 0$ allora $\beta < \gamma$ se e solo se $\alpha \cdot \beta < \alpha \cdot \gamma$;
- $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

L'assioma dell'insieme potenza

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Un ulteriore assioma garantisce l'esistenza di insiemi sempre più grandi.

L'assioma dell'insieme potenza

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$$

Lo z di cui si afferma l'esistenza è unico per estensionalità e lo indichiamo con $\mathcal{P}(x)$.

Equipotenza

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinabili

Gli assiomi
dell'infinito e
dell'insieme
potenza

L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Siano x e y due insiemi

- $x \preceq y$ se esiste $f : x \rightarrow y$ iniettiva;
- $x \approx y$ se esiste $f : x \rightarrow y$ biiettiva (x e y sono **equipotenti**);
- $x \prec y$ se $x \preceq y$ e $x \not\approx y$.

\preceq è riflessiva e transitiva, \approx è una relazione d'equivalenza.

Teorema (di Cantor–Bernstein–Schröder)

Se $x \preceq y$ e $y \preceq x$ allora $x \approx y$.

Il teorema di Cantor

Teorema (di Cantor)

Per ogni insieme x , $x \prec \mathcal{P}(x)$.

Dimostrazione.

$y \mapsto \{y\}$ mostra $x \preceq \mathcal{P}(x)$.

Se $f : x \rightarrow \mathcal{P}(x)$ mostriamo che f non è suriettiva.

Sia $z = \{y \in x \mid y \notin f(y)\}$.

Se fosse $z = f(y)$ per qualche $y \in x$ allora

$$y \in z \leftrightarrow y \in f(y) \leftrightarrow y \notin z.$$

Perciò $z \notin \text{ran}(f)$.



Introduzione e
teoria ingenua
degli insiemi

La teoria ZF
Il linguaggio
I primi assiomi
Ordinali

Gli assiomi
dell'infinito e
dell'insieme
potenza
L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Un assioma limitativo

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF
Il linguaggio
I primi assiomi
Ordinabili

Gli assiomi
dell'infinito e
dell'insieme
potenza
L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Tutti gli assiomi introdotti sinora, salvo estensionalità, hanno garantito l'esistenza di insiemi.

L'assioma di estensionalità ha ristretto l'ambito della teoria degli insiemi agli insiemi ereditari.

L'ultimo assioma di ZF invece limita l'esistenza di insiemi, imponendo che tutti gli insiemi abbiano una certa proprietà.

In realtà anch'esso restringe l'ambito della teoria degli insiemi ad un certo tipo di insiemi: gli insiemi ben fondati.

Gli insiemi ben fondati

Per ricorsione definiamo

$$V_0 = \emptyset;$$

$$V_{\alpha+1} = \mathcal{P}(V_\alpha);$$

$$V_\lambda = \bigcup \{ V_\alpha \mid \alpha < \lambda \}.$$

Sia $\mathbb{WF} = \{ x \mid \exists \alpha x \in V_\alpha \}$.

Un insieme è ben fondato se appartiene a \mathbb{WF} .

La ragione per restringere la nostra attenzione agli insiemi ben fondati è duplice:

- gli insiemi ben fondati si comportano “bene” e non presentano certe “patologie”; ci sono utili strumenti tecnici per studiarli e l’universo degli insiemi ben fondati ha una descrizione semplice ed elegante;
- gli oggetti matematici sono rappresentati (a meno di isomorfismo) negli insiemi ben fondati.

L'assioma di fondazione

L'assioma di fondazione

$$\forall x (x \neq \emptyset \rightarrow \exists y \in x \forall z \in y z \notin x)$$

In altre parole, ogni insieme non vuoto ha un elemento minimale rispetto a \in .

L'assioma di fondazione è equivalente a $\forall = \text{WF}$.

Alcune conseguenze dell'assioma di fondazione sono:

- non esistono insiemi che appartengono a se stessi: se $x \in x$, $\{x\}$ non ha elemento minimale;
- non esistono x e y tali che $x \in y$ e $y \in x$ (considerare $\{x, y\}$);
- non esistono funzioni f con $\text{dom}(f) = \omega$ e $\forall n f(n+1) \in f(n)$ (considerare $\text{ran}(f)$).

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

Il linguaggio
I primi assiomi
Ordinali
Gli assiomi
dell'infinito e
dell'insieme
potenza
L'assioma di
fondazione

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Abbiamo completato la descrizione degli assiomi di ZF,
la teoria degli insiemi di Zermelo-Fraenkel!

L'assioma della scelta

Una **funzione di scelta** su x è una funzione f con $\text{dom}(f) = x$ tale che $\forall y \in x (y \neq \emptyset \rightarrow f(y) \in y)$.

L'assioma della scelta

Ogni insieme ha una funzione di scelta

L'assioma della scelta è indicato con AC.

In ZF AC è equivalente a:

- il teorema del buon ordinamento:

$$\forall x \exists R (\langle x, R \rangle \text{ è un buon ordine});$$

- il lemma di Zorn.

ZFC

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

L'assioma della
scelta
Cardinali
Equivalenti e
forme deboli
dell'assioma
della scelta

Risultati di
indipendenza

Abbiamo completato la descrizione degli assiomi di ZFC,
la teoria degli insiemi di Zermelo-Fraenkel con scelta!

Cardinalità

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

L'assioma della
scelta

Cardinali

Equivalenti e
forme deboli
dell'assioma
della scelta

Risultati di
indipendenza

In ZFC ogni x può venir ben ordinato e esiste α tale che $\alpha \approx x$.

Definizione

Indichiamo con $|x|$ la **cardinalità di x** , cioè il più piccolo ordinale α tale che $\alpha \approx x$.

L'operazione $x \mapsto |x|$ sceglie un rappresentante da ogni classe d'equivalenza rispetto a \approx .

Dal teorema di Cantor segue che $|x| < |\mathcal{P}(x)|$.

Insiemi finiti e infiniti

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

L'assioma della
scelta

Cardinali

Equivalenti e
forme deboli
dell'assioma
della scelta

Risultati di
indipendenza

Definizione

Un insieme x è

- finito, se $|x| < \omega$;
- numerabile, se $|x| = \omega$;
- più che numerabile, se $|x| > \omega$.

Cardinali

Definizione

Un **cardinale** è un ordinale α tale che $|\alpha| = \alpha$,
cioè tale che $\forall \beta < \alpha \beta \not\approx \alpha$.

Le cardinalità di insiemi sono cardinali, cioè ogni $|x|$ è un cardinale.

Si verifica facilmente che ogni ordinale $\leq \omega$ è un cardinale.

I cardinali $\geq \omega$ sono ordinali limite.

Dal teorema di Cantor segue che $\forall \alpha \exists \beta > \alpha$ (β è un cardinale).

Infatti $\beta = |\mathcal{P}(\alpha)|$ fa al caso nostro.

Indichiamo con α^+ il più piccolo cardinale $> \alpha$.

Le lettere κ, μ, ν, \dots indicano sempre cardinali.

La funzione aleph

Per ricorsione definiamo

$$\aleph_0 = \omega;$$

$$\aleph_{\alpha+1} = (\aleph_\alpha)^+;$$

$$\aleph_\lambda = \sup\{\aleph_\alpha \mid \alpha < \lambda\}.$$

La funzione $\alpha \mapsto \aleph_\alpha$ enumera in ordine crescente tutti i cardinali infiniti.

I cardinali della forma $\aleph_{\alpha+1}$ sono detti cardinali successori (sono κ^+ per qualche κ).

Quelli della forma \aleph_λ per λ ordinale limite sono detti cardinali limite.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

L'assioma della
scelta

Cardinali

Equivalenti e
forme deboli
dell'assioma
della scelta

Risultati di
indipendenza

Equivalenti di AC

In ZF AC è equivalente a:

- il teorema di Tychonoff: il prodotto di spazi topologici compatti è compatto;
- ogni gruppo ha un p -sottogruppo massimale (per qualunque p primo fissato);
- ogni anello commutativo con identità ha un ideale massimale;
- ogni insieme che genera uno spazio vettoriale ha una base;
- la sfera unitaria del duale di uno spazio vettoriale normato su \mathbb{R} contiene un punto estremo (cioè un punto che non è nell'interno di nessun segmento contenuto nella sfera).

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

L'assioma della
scelta

Cardinali

Equivalenti e
forme deboli
dell'assioma
della scelta

Risultati di
indipendenza

Equivalenti dell'assioma della scelta numerabile

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

L'assioma della
scelta

Cardinali

Equivalenti e
forme deboli
dell'assioma
della scelta

Risultati di
indipendenza

Indichiamo con AC_ω la restrizione di AC ad insiemi numerabili.
 AC_ω è strettamente più debole di AC.

In ZF AC_ω è equivalente a:

- l'unione di un insieme numerabile di insiemi a due a due disgiunti ha un sottoinsieme numerabile;
- ogni spazio topologico σ -compatto (cioè che è unione numerabile di compatti) è Lindelöf (ogni ricoprimento aperto ha un sottoricoprimento numerabile);
- ogni funzione a valori reali su uno spazio metrico che sia sequenzialmente continua è continua.

Somma e prodotto cardinali

Definiamo somma e prodotto cardinale appoggiandoci sulle corrispondenti operazioni ordinali:

$$\kappa \oplus \mu = |\kappa + \mu|; \quad \kappa \otimes \mu = |\kappa \cdot \mu|.$$

Lemma

Per ogni m e n , $m \oplus n = m + n$ e $m \otimes n = m \cdot n$.

Teorema

Se κ e μ sono > 0 e almeno uno dei due è infinito, $\kappa \oplus \mu = \kappa \otimes \mu = \max\{\kappa, \mu\}$.

Quindi somma e prodotto cardinale non sono molto interessanti.

L'esponenziazione cardinale

Sia ${}^x y = \{ f \mid f \text{ è una funzione} \wedge \text{dom}(f) = x \wedge \text{ran}(f) \subseteq y \}$.
 ${}^x y$ esiste come insieme perché è incluso in $\mathcal{P}(x \times y)$.

Definizione

Se κ e μ sono cardinali l'esponenziazione cardinale è definita da
 $\kappa^\mu = |{}^\mu \kappa|$.

Si vede facilmente che $\mathcal{P}(x) \approx {}^x 2$ e quindi $|\mathcal{P}(x)| = 2^{|x|}$.

Dal teorema di Cantor segue che $\kappa < 2^\kappa$.

Ma qual è la distanza tra κ e 2^κ ? E in particolare tra \aleph_0 e 2^{\aleph_0} ?

L'ultima questione è di particolare rilevanza perché $\aleph_0 = |\mathbb{N}|$ e
 $2^{\aleph_0} = |\mathbb{R}|$.

L'ipotesi del continuo

Cantor nel 1877 formulò l'**ipotesi del continuo CH**: $2^{\aleph_0} = \aleph_1$.

CH afferma che la cardinalità del continuo ($= \mathbb{R}$) è la minima possibile.

Un altro modo di enunciare CH è il seguente:

ogni insieme più che numerabile di reali ha la cardinalità di \mathbb{R} .

CH occupava il primo posto nella lista dei problemi aperti per la matematica del XX secolo preparata da Hilbert per il Congresso Internazionale dei Matematici del 1900 a Parigi.

Hausdorff nel 1908 propose l'**ipotesi generalizzata del continuo GCH**: $\forall \alpha \ 2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

GCH afferma che i valori di 2^{\aleph_α} sono i minimi possibili.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Aritmetica
cardinale

L'ipotesi del
continuo

I risultati di
indipendenza

Equivalenti di CH

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Aritmetica
cardinale

L'ipotesi del
continuo

I risultati di
indipendenza

In ZFC CH è equivalente a:

- esiste un insieme $A \subseteq \mathbb{R}^2$ tale che per ogni $a \in \mathbb{R}$ ambedue gli insiemi $\{x \in \mathbb{R} \mid (x, a) \in A\}$ e $\{y \in \mathbb{R} \mid (a, y) \notin A\}$ sono numerabili.
- esiste una partizione numerabile di \mathbb{R}^2 tale che nessun elemento della partizione contiene i vertici di un triangolo rettangolo.

Il teorema di Gödel

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Aritmetica
cardinale

L'ipotesi del
continuo

I risultati di
indipendenza

Teorema (Gödel, 1940)

Se ZFC è coerente, allora anche $ZFC + CH$ è coerente.

Quindi ZFC non può dimostrare che l'ipotesi del continuo è falsa (a meno che ZFC sia incoerente).

Gödel ottenne il teorema definendo in ZFC una classe propria in cui vale $ZFC + CH$.

Il teorema di Cohen

Teorema (Cohen, 1963)

Se ZFC è coerente, allora anche $ZFC + \neg CH$ è coerente.

Quindi ZFC non può dimostrare che l'ipotesi del continuo è vera (a meno che ZFC sia incoerente).

Diciamo che CH è **indipendente** da ZFC.

Cohen ottenne il teorema introducendo la tecnica del *forcing* per costruire modelli di ZFC con varie proprietà aggiuntive, quali ad esempio $\neg CH$.

A partire dal teorema di Cohen il forcing ha fornito una miriade di risultati di indipendenza.

Introduzione e
teoria ingenua
degli insiemi

La teoria ZF

L'assioma
della scelta e
ZFC

Risultati di
indipendenza

Aritmetica
cardinale

L'ipotesi del
continuo

I risultati di
indipendenza

L'aritmetica del second'ordine

Introduzione

Il linguaggio \mathcal{L}_2

Primi passi in \mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

① Introduzione

② Il linguaggio \mathcal{L}_2

③ Primi passi in \mathbb{Z}_2

④ Parliamo solo di naturali e insiemi di naturali?

L'aritmetica del second'ordine

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

L'aritmetica del second'ordine Z_2 estende l'aritmetica di Peano PA affiancando ai numeri naturali oggetti “del second'ordine”, cioè insiemi di numeri naturali.

Similmente si può sviluppare l'aritmetica del terz'ordine, che considera anche insiemi di insiemi di numeri naturali, e così via.

Il sistema Z_2

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

Z_2 è una teoria nel linguaggio \mathcal{L}_2 che presenteremo tra poco: consiste di tutte le conseguenze logiche degli assiomi che introdurremo.

Nei prossimi giorni studieremo alcuni sottosistemi di Z_2 che si sono rivelati importanti nella formalizzazione della pratica matematica, in particolare nel programma della *reverse mathematics*.

La logica che utilizzeremo è sempre quella **classica**: faremo uso del terzo escluso e di dimostrazioni per assurdo.

Negli ultimi anni è iniziato lo studio della *reverse mathematics* dal punto di vista intuizionistico e costruttivo, che non affronteremo.

Un linguaggio a due sorte

Il linguaggio per l'aritmetica del second'ordine \mathcal{L}_2 è un linguaggio a due sorte.

Le variabili della prima sorta sono tipicamente n, m, ℓ, i, j, \dots e le pensiamo interpretate sui numeri naturali (elementi di \mathbb{N}).

Le variabili della seconda sorta sono tipicamente X, Y, Z, \dots e le pensiamo interpretate sugli insiemi di numeri naturali (sottoinsiemi di \mathbb{N}).

\mathcal{L}_2 può essere visto come un linguaggio del prim'ordine, aggiungendo due predicati unari N e I e mettendo come assioma

$$\forall x ((N(x) \vee I(x)) \wedge \neg(N(x) \wedge I(x))).$$

Introduzione

Il linguaggio
 \mathcal{L}_2

Sintassi
Semantica

Primi passi in
 Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

Simboli non logici di \mathcal{L}_2

I simboli di costante sono 0 e 1, entrambi della sorta numerica.

I simboli di funzione vanno dalla sorta numerica in se stessa:
 $+$ e \cdot sono entrambi binari.

$n + 1$ e $n \cdot (m + n) + 0$ sono termini numerici.

Ci sono tre simboli di relazione binari:

$<$ e $=$ coinvolgono due termini numerici,

\in collega un termine numerico ad una variabile insiemistica.

$n + 1 < 0 + 1 + 1$, $n + 1 = n \cdot (m + n) + 0$,

$n \in X$ e $n \cdot (m + n) + 0 \in Z$ sono formule atomiche.

Stiamo usando le usuali convenzioni di scrittura
e di precedenza tra le operazioni.

Le interpretazioni intese di questi simboli sono quelle ovvie.

Introduzione

Il linguaggio
 \mathcal{L}_2

Sintassi
Semantica

Primi passi in
 Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

Due uguaglianze

Introduzione

Il linguaggio

\mathcal{L}_2

Sintassi

Semantica

Primi passi in

Z_2

Parliamo solo

di naturali e

insiemi di

naturali?

Il simbolo $=$ è inteso essere l'uguaglianza tra numeri, e soddisfare gli usuali assiomi della logica con uguaglianza.

Notiamo invece l'assenza del simbolo di uguaglianza tra insiemi. La formula $X = Y$ è un'abbreviazione per

$$\forall n(n \in X \leftrightarrow n \in Y).$$

Ciò che caratterizza un insieme sono i numeri che gli appartengono.

Quantificatori limitati

Introduzione

Il linguaggio

\mathcal{L}_2

Sintassi

Semantica

Primi passi in

Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

Sia t un termine numerico in cui non compare la variabile n .

- $\forall n < t \varphi$ sta per $\forall n(n < t \rightarrow \varphi)$;
- $\exists n < t \varphi$ sta per $\exists n(n < t \wedge \varphi)$.

Le formule Σ_0^0 sono quelle che non contengono quantificatori insiemistici e in cui tutti i quantificatori numerici sono limitati. Una formula Σ_0^0 può avere variabili insiemistiche libere.

$$\exists n < m + 1(n \cdot m + k \in X) \quad \text{è } \Sigma_0^0$$

Alcune classi di formule

- Una formula è Σ_1^0 se è della forma $\exists n \varphi$ dove φ è Σ_0^0 ;
- una formula è Π_1^0 se è della forma $\forall n \varphi$ dove φ è Σ_0^0 ;
- una formula è Σ_k^0 se è della forma $\exists n_1 \forall n_2 \dots Q n_k \varphi$ dove φ è Σ_0^0 ;
- una formula è Π_k^0 se è della forma $\forall n_1 \exists n_2 \dots Q n_k \varphi$ dove φ è Σ_0^0 .

$X = Y$ (che è $\forall n(n \in X \leftrightarrow n \in Y)$) è Π_1^0 .

Quando diremo che una formula è Σ_k^0 intenderemo sempre a meno di equivalenza. La negazione di una formula Σ_1^0 è Π_1^0 . Una formula Σ_k^0 è anche Σ_{k+1}^0 e Π_{k+1}^0 .

Le formule Σ_1^0 sono strettamente connesse con gli insiemi c.e., e così via.

Altre classi di formule

Una formula è aritmetica se non contiene quantificatori insiemistici.

Le formule Σ_k^0 e Π_k^0 sono aritmetiche.

- Una formula è Σ_1^1 se è della forma $\exists X \varphi$ dove φ è aritmetica;
- una formula è Π_1^1 se è della forma $\forall X \varphi$ dove φ è aritmetica;
- una formula è Σ_k^1 se è della forma $\exists X_1 \forall X_2 \dots Q X_k \varphi$ dove φ è aritmetica;
- una formula è Π_k^1 se è della forma $\forall X_1 \exists X_2 \dots Q X_k \varphi$ dove φ è aritmetica.

Quando diremo che una formula è Σ_k^1 intenderemo sempre a meno di equivalenza. La negazione di una formula Σ_1^1 è Π_1^1 . Una formula Σ_k^1 è anche Σ_{k+1}^1 e Π_{k+1}^1 .

Introduzione

Il linguaggio

\mathcal{L}_2

Sintassi

Semantica

Primi passi in

Z_2

Parliamo solo di naturali e insiemi di naturali?

Modelli per \mathcal{L}_2

Un modello per \mathcal{L}_2 è del tipo

$$\mathcal{M} = (M, \mathcal{S}_{\mathcal{M}}, 0_{\mathcal{M}}, 1_{\mathcal{M}}, +_{\mathcal{M}}, \cdot_{\mathcal{M}}, <_{\mathcal{M}}).$$

M è un insieme su cui variano le variabili numeriche, a cui appartengono $0_{\mathcal{M}}$ e $1_{\mathcal{M}}$, su cui operano le funzioni binarie $+_{\mathcal{M}}$ e $\cdot_{\mathcal{M}}$, i cui elementi possono essere nella relazione binaria $<_{\mathcal{M}}$.
 $=$ è interpretato come l'identità su M .

$\mathcal{S}_{\mathcal{M}}$ è una collezione di sottoinsiemi di M e su di esso variano le variabili insiemistiche.

$t \in X$ è interpretato come vero se $t^{\mathcal{M}}$ (l'interpretazione del termine numerico t in \mathcal{M}) appartiene all'elemento di $\mathcal{S}_{\mathcal{M}}$ cui è assegnata X .

Introduzione

Il linguaggio

\mathcal{L}_2

Sintassi

Semantica

Primi passi in

Z_2

Parliamo solo di naturali e insiemi di naturali?

ω -modelli

Il modello inteso per \mathcal{L}_2 è

$$(\omega, \mathcal{P}(\omega), 0, 1, +, \cdot, <).$$

dove ω è il “vero” insieme dei naturali.

Un ω -modello per \mathcal{L}_2 è un modello della forma

$$(\omega, \mathcal{S}, 0, 1, +, \cdot, <)$$

con $\mathcal{S} \subseteq \mathcal{P}(\omega)$.

In questo caso spesso parliamo dell' ω -modello \mathcal{S} .

Per esempio **REC** è l' ω -modello degli insiemi computabili,

ARITH è l' ω -modello degli insiemi aritmetici

(cioè definibili nel linguaggio senza variabili insiemistiche e \in).

Introduzione

Il linguaggio

\mathcal{L}_2

Sintassi

Semantica

Primi passi in

Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

Gli assiomi aritmetici

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Gli assiomi
Primi sviluppi
algebrici

Parliamo solo
di naturali e
insiemi di
naturali?

- $\forall n(n + 1 \neq 0)$;
- $\forall n \forall m(n + 1 = m + 1 \rightarrow n = m)$;
- $\forall n(n + 0 = n)$;
- $\forall n \forall m(n + (m + 1) = (n + m) + 1)$;
- $\forall n(n \cdot 0 = 0)$;
- $\forall n \forall m(n \cdot (m + 1) = (n \cdot m) + n)$;
- $\forall n \neg(n < 0)$;
- $\forall n \forall m(n < m + 1 \leftrightarrow (n < m \vee n = m))$.

Lo schema di comprensione

Se φ è una formula di \mathcal{L}_2 con una variabile libera numerica n evidenziata, ed in cui X non è libera è un'assioma di comprensione la chiusura universale di:

$$\exists X \forall n (n \in X \leftrightarrow \varphi(n)).$$

X è unico (per la definizione di $=$ tra insiemi) e lo indichiamo con $\{n \mid \varphi(n)\}$.

Ad esempio $\{n \mid \exists m (m + m = n)\}$ è l'insieme dei numeri pari.

Altre variabili (numeriche e insiemistiche) possono essere libere in φ , e si dice che sono parametri nell'istanza di comprensione che stiamo considerando.

Ad esempio se φ è $\exists k (n = m \cdot k) \wedge (n \notin Y \wedge n \in Z)$ comprensione asserisce che, per qualsiasi m, Y, Z , esiste l'insieme dei multipli di m che appartengono a $Z \setminus Y$.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Gli assiomi
Primi sviluppi
algebrici

Parliamo solo
di naturali e
insiemi di
naturali?

L'assioma di induzione

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Gli assiomi
Primi sviluppi
algebrici

Parliamo solo
di naturali e
insiemi di
naturali?

$$\forall X (0 \in X \wedge \forall n (n \in X \rightarrow n + 1 \in X) \rightarrow \forall n (n \in X))$$

Combinando lo schema di comprensione e l'assioma di induzione otteniamo lo schema di induzione:

Se φ è una formula di \mathcal{L}_2 con una variabile libera numerica n evidenziata (e possibilmente altre variabili libere)

$$\varphi(0) \wedge \forall n (\varphi(n) \rightarrow \varphi(n + 1)) \rightarrow \forall n \varphi(n).$$

Come ottenere sottosistemi di Z_2

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Gli assiomi

Primi sviluppi
algebrici

Parliamo solo
di naturali e
insiemi di
naturali?

I sottosistemi di Z_2 che ci interessano si ottengono, in linea di massima, restringendo le formule che compaiono nello schema di comprensione e, in alcuni casi, sostituendo l'assioma di induzione con lo schema di induzione ristretto ad una certa classe di formule.

Per esempio il sistema $\Pi_k^1\text{-CA}_0$ si ottiene restringendo lo schema di comprensione alle formule Π_k^1 .

Si sa che $\Pi_{k+1}^1\text{-CA}_0$ è strettamente più forte di $\Pi_k^1\text{-CA}_0$.

Ovviamente $Z_2 = \bigcup_k \Pi_k^1\text{-CA}_0$ ed è anche chiamato $\Pi_\infty^1\text{-CA}_0$.

Due ω -modelli per Z_2

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Gli assiomi
Primi sviluppi
algebrici

Parliamo solo
di naturali e
insiemi di
naturali?

Il modello inteso $(\omega, \mathcal{P}(\omega), 0, 1, +, \cdot, <)$ è un modello di Z_2 .

$\{ \{ n \mid \varphi(n) \} \mid \varphi \text{ formula di } \mathcal{L}_2 \text{ con } n \text{ unica variabile libera} \}$

è numerabile ed è il più piccolo ω -modello di Z_2 .

Proprietà delle operazioni

- $(m + n) + p = m + (n + p)$
- $0 + m = m$
- $1 + m = m + 1$
- $m + n = n + m$
- $m \cdot (n + p) = m \cdot n + m \cdot p$
- $(m \cdot n) \cdot p = m \cdot (n \cdot p)$
- $(m + n) \cdot p = m \cdot p + n \cdot p$
- $0 \cdot m = 0$
- $1 \cdot m = m$
- $m \cdot n = n \cdot m$

Le chiusure universali di queste proprietà si dimostrano per induzione sull'ultima variabile in ordine alfabetico.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Gli assiomi
Primi sviluppi
algebrici

Parliamo solo
di naturali e
insiemi di
naturali?

Proprietà dell'ordine

- $m < n \wedge n < p \rightarrow m < p$
- $m < n \rightarrow m + 1 < n + 1$
- $m + 1 < n + 1 \rightarrow m < n$
- $n \neq 0 \rightarrow 0 < n$
- $m < n \vee m = n \vee n < m$
- $\neg n < n$
- $m < n \rightarrow m + p < n + p$
- $m + p < n + p \rightarrow m < n$
- $m < m + n + 1$
- $m + p = n + p \rightarrow m = n$
- $p \neq 0 \wedge m < n \rightarrow m \cdot p < n \cdot p$
- $p \neq 0 \wedge m \cdot p < n \cdot p \rightarrow m < n$
- $p \neq 0 \wedge m \cdot p = n \cdot p \rightarrow m = n$

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Gli assiomi
Primi sviluppi
algebrici

Parliamo solo
di naturali e
insiemi di
naturali?

Sottrazione

Vogliamo mostrare che $m < n \rightarrow \exists k < n(m + k + 1 = n)$.

Procediamo per induzione su n .

caso base: $\neg m < 0$ è un assioma e non c'è nulla da provare.

passo induttivo: se $m < n + 1$ per uno degli assiomi $m < n$ oppure $m = n$.

Se $m < n$ per induzione esiste $k < n$ tale che $m + k + 1 = n$.

Allora $k + 1 < n + 1$ e $m + (k + 1) + 1 = n + 1$
per le proprietà precedenti.

Se $m = n$ allora $0 < n + 1$ e $m + 0 + 1 = n + 1$
per un assioma e una proprietà precedente.

In particolare $n \neq 0 \rightarrow \exists m < n(m + 1 = n)$.

Finora abbiamo usato l'induzione solo su formule Σ_0^0 .

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Gli assiomi
Primi sviluppi
algebrici

Parliamo solo
di naturali e
insiemi di
naturali?

Un linguaggio per la matematica

Hermann Weyl (*Das Kontinuum*, 1917) e Hilbert e Bernays (*Grundlagen der Mathematik*, 1968–70) furono tra i primi a mostrare che in (un sistema analogo a) Z_2 si può formalizzare una parte considerevole della matematica usuale.

Ma come è possibile parlare di numeri reali, funzioni continue o derivabili, gruppi, ordini parziali, ordinali, ecc. in un linguaggio in cui abbiamo solo elementi e sottoinsiemi di \mathbb{N} ?

Useremo **codifiche**, analoghe a quelle dei naturali in ZF.

Il limite è quello della numerabilità degli oggetti considerati.

Quindi consideriamo solo strutture algebriche numerabili.

E i reali, che sono più che numerabili?

La struttura metrica e d'ordine di \mathbb{R} sono determinate dal suo essere completamento di \mathbb{Q} , che è numerabile.

Sfrutteremo la separabilità per codificare \mathbb{R} (e le funzioni continue su \mathbb{R}) in Z_2 e nei suoi sottosistemi.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

Insiemi e
successione finite

Funzioni

Strutture
algebriche e
combinatoriali

I sistemi
numerici

Spazi metrici
completi

Le limitazioni della formalizzazione

In \mathcal{L}_2 formalizziamo quindi la *matematica numerabile*, che comprende geometria, analisi classica, analisi reale e complessa, topologia degli spazi metrici completi separabili e teoria descrittiva degli insiemi.

Non possiamo formalizzare in \mathcal{L}_2 la *matematica più che numerabile*:

topologia generale, analisi funzionale astratta, algebra più che numerabile, combinatorica più che numerabile, teoria degli insiemi, . . .

Queste parti della matematica moderna sarebbero inconcepibili senza la rivoluzione insiemistica avviata da Cantor: non è sorprendente che richiedano un linguaggio insiemistico più espressivo di quello di \mathcal{L}_2 .

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

Insiemi e
successione finite

Funzioni

Strutture
algebriche e
combinatoriali

I sistemi
numerici

Spazi metrici
completi

Coppie di numeri

$$(i, j) = (i + j)^2 + i$$

Questo termine definisce una funzione coppia su \mathbb{N} .

Lemma

- $i \leq (i, j)$ e $j \leq (i, j)$;
- $(i, j) = (m, n) \rightarrow i = m \wedge j = n$.

Dimostrazione.

- $i \leq i + j \leq (i + j)^2 \leq (i, j)$;
- Sia $\ell = i + j$. Allora $\ell^2 \leq (i, j) < (\ell + 1)^2$ e non vi sono altri ℓ con questa proprietà, cioè vale anche $\ell = m + n$.
 $i = (i, j) - \ell^2$ e $j = \ell - i$ si ricavano da (i, j) e ℓ
e lo stesso si farebbe con m e n . □

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo
di naturali e
insiemi di
naturali?

Insiemi e
successione finite

Funzioni

Strutture
algebriche e
combinatoriali

I sistemi
numerici

Spazi metrici
completi

Contrazione di quantificatori

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo
di naturali e
insiemi di
naturali?

Insiemi e
successione finite

Funzioni

Strutture
algebriche e
combinatoriali

I sistemi
numerici

Spazi metrici
completi

L'esistenza della funzione coppia su \mathbb{N} permette di contrarre quantificatori numerici dello stesso tipo.

Se θ è Σ_0^0

$$\exists i \exists j \theta \leftrightarrow \exists k \exists i \leq k \exists j \leq k (k = (i, j) \wedge \theta) \quad \text{è } \Sigma_1^0$$

$$\forall i \forall j \theta \leftrightarrow \forall k \forall i \leq k \forall j \leq k (k = (i, j) \rightarrow \theta) \quad \text{è } \Pi_1^0.$$

Coppie di insiemi

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo
di naturali e
insiemi di
naturali?

Insiemi e
successione finite

Funzioni

Strutture
algebriche e
combinatoriali

I sistemi
numerici

Spazi metrici
completi

Le coppie di insiemi possono venir codificate direttamente ponendo

$$\langle A, B \rangle = A \oplus B = \{2n \mid n \in A\} \cup \{2n + 1 \mid n \in B\}.$$

Successioni infinite di insiemi possono venir codificate ponendo

$$\langle A_i : i \in \mathbb{N} \rangle = \{(i, n) \mid n \in A_i\}.$$

Insiemi finiti

Diciamo che X è finito se $\exists k \forall i (i \in X \rightarrow i < k)$.

Lemma

Se X è finito esistono k, m, n tali che

$$\forall i (i \in X \leftrightarrow i < k \wedge m(i + 1) + 1 \text{ divide } n).$$

Questo Lemma è dimostrato sviluppando in \mathbb{Z}_2 alcune parti dell'aritmetica elementare (divisibilità, numeri relativamente primi).

L'esistenza di m e n è dimostrata per induzione: lo schema di induzione è applicato a formule Σ_1^0 .

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Codici per insiemi finiti

Il Lemma ci permette di **codificare** gli insiemi finiti:

Definizione

Se X è finito il suo *codice* è il minimo numero del tipo $(k, (m, n))$ tale che k, m, n soddisfano il Lemma.

Questa codifica è, in un certo senso, arbitraria.

Ciò che importa è che esistono formule di \mathcal{L}_2 che esprimono “ $(k, (m, n))$ è il codice per un insieme finito” e “ i appartiene all’insieme codificato da $(k, (m, n))$ ”.

Entrambe queste formule sono Σ_0^0 .

Se p è il codice per X allora $i < p$ per ogni $i \in X$.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo
di naturali e
insiemi di
naturali?

Insiemi e
successione finite

Funzioni

Strutture
algebriche e
combinatoriali

I sistemi
numerici

Spazi metrici
completi

Successioni finite

Una successione finita di numeri naturali è un insieme finito X tale che

- 1 $\forall n \in X \exists i \exists j n = (i, j)$;
- 2 $\forall i \forall j \forall k ((i, j) \in X \wedge (i, k) \in X \rightarrow j = k)$;
- 3 $\exists \ell \forall i (i < \ell \leftrightarrow \exists j (i, j) \in X)$.

Il numero ℓ è determinato da X ed è la sua lunghezza.

Il codice per la succ X è il suo codice come insieme finito.

$\mathbb{N}^{<\mathbb{N}}$ è l'insieme delle successioni finite di numeri naturali, cioè dei loro codici.

$\mathbb{N}^{<\mathbb{N}}$ esiste per comprensione applicata alla formula

“ p è il codice di un insieme finito” $\wedge 1 \wedge 2 \wedge 3$
che è Σ_0^0 perché tutti i quantificatori sono limitati da p .

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Operazioni su successioni finite

Indicheremo gli elementi di $\mathbb{N}^{<\mathbb{N}}$ con $\sigma, \tau, \rho, \dots$

$|\sigma|$ è la lunghezza della successione codificata da σ .

Se $i < |\sigma|$, $\sigma(i)$ è l'unico j tale che " $(i, j) \in \sigma$ ".

$$\sigma = \langle \sigma(0), \sigma(1), \dots, \sigma(|\sigma| - 1) \rangle = \langle \sigma(i) : i < |\sigma| \rangle$$

$$\sigma \hat{\ } \tau = \langle \sigma(0), \dots, \sigma(|\sigma| - 1), \tau(0), \dots, \tau(|\tau| - 1) \rangle$$

$$\sigma \hat{\ } \langle m \rangle = \langle \sigma(0), \dots, \sigma(|\sigma| - 1), m \rangle$$

$$\sigma[n] = \langle \sigma(0), \dots, \sigma(n - 1) \rangle = \langle \sigma(i) : i < n \rangle$$

$\sigma \subseteq \tau$ significa che σ è un segmento iniziale di τ , cioè

$$\exists n \leq |\tau| \ \sigma = \tau[n].$$

Le formule $|\sigma| = \ell$, $\sigma(i) = j$, $\sigma \hat{\ } \tau = \rho$, $\sigma \subseteq \tau$ sono Σ_0^0 .

Inoltre $|\sigma| \leq \sigma$ e $\sigma(i) < \sigma$.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e
insiemi di
naturali?

Insiemi e
successione finite

Funzioni

Strutture
algebriche e
combinatoriali

I sistemi
numerici

Spazi metrici
completi

Quantificatori limitati e complessità di formule

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Usando le successioni finite abbiamo

$$\begin{aligned}\forall i < k \exists j \theta(i, j, k) &\leftrightarrow \exists \sigma (|\sigma| = k \wedge \forall i < k \theta(i, \sigma(i), k)) \\ &\leftrightarrow \exists \sigma (|\sigma| = k \wedge \forall i < k \exists j < \sigma(j = \sigma(i) \wedge \theta(i, j, k)))\end{aligned}$$

Questa equivalenza mostra che se φ è Σ_k^0 o Π_k^0 , allora $\forall i < k \varphi$ e $\exists i < k \varphi$ sono pure Σ_k^0 o Π_k^0 .

Composizione

$$X \times Y = \{ k \mid \exists i \leq k \exists j \leq k (i \in X \wedge j \in Y \wedge k = (i, j)) \}.$$

Una funzione $f : X \rightarrow Y$ è un insieme $f \subseteq X \times Y$ tale che

$$\forall i \in X \exists! j \in Y (i, j) \in f.$$

Se $f : X \rightarrow Y$ e $i \in X$, $f(i)$ è l'unico $j \in Y$ tale che $(i, j) \in f$.

In \mathbb{Z}_2 si dimostra che le funzioni sono chiuse per composizione, cioè se $f : X \rightarrow Y$ e $g : Y \rightarrow Z$ sono funzioni

$$\begin{aligned} gf &= \{ (i, k) \mid \exists j ((i, j) \in f \wedge (j, k) \in g) \} \\ &= \{ (i, k) \mid i \in X \wedge \forall j ((i, j) \in f \rightarrow (j, k) \in g) \} \end{aligned}$$

è una funzione da X a Z .

Notiamo che gf può essere definito per comprensione in due modi diversi: usando una formula Σ_1^0 oppure una formula Π_1^0 .

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Ricorsione primitiva

Le funzioni k -arie $f : X^k \rightarrow Y$ si codificano ponendo $X^k = \{ \sigma \in \mathbb{N}^{<\mathbb{N}} \mid |\sigma| = k \wedge \forall i < |\sigma| \sigma(i) \in X \}$.

In \mathbb{Z}_2 si dimostra che le funzioni sono chiuse per ricorsione primitiva, cioè date $f : \mathbb{N}^k \rightarrow \mathbb{N}$ e $g : \mathbb{N}^{k+2} \rightarrow \mathbb{N}$ esiste unica $h : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ tale che

$$h(0, n_1, \dots, n_k) = f(n_1, \dots, n_k);$$

$$h(m+1, n_1, \dots, n_k) = g(h(m, n_1, \dots, n_k), m, n_1, \dots, n_k).$$

Si dimostra per induzione su m che esiste $\sigma \in \mathbb{N}^{m+1}$ tale che

$$\sigma(0) = h(0, n_1, \dots, n_k) \wedge \forall i < m \sigma(i+1) = g(\sigma(i), i, n_1, \dots, n_k).$$

Si noti che l'induzione è su una formula Σ_1^0 .

Possiamo per esempio definire l'esponenziale m^n .

Introduzione

Il linguaggio \mathcal{L}_2

Primi passi in \mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Gruppi

La codifica di una struttura algebrica (numerabile) è a questo punto semplice.

Definizione

Un gruppo G consiste di un insieme $|G| \subseteq \mathbb{N}$,
di un elemento $1_G \in |G|$
e di funzioni $\cdot_G : |G| \times |G| \rightarrow |G|$ e $^{-1} : |G| \rightarrow |G|$
che soddisfano gli usuali assiomi per i gruppi.
 G è abeliano se \cdot_G è commutativo.
In questo caso si usano 0_G , $+_G$ e $-_G$.

Similmente si definiscono anelli, campi, spazi vettoriali, ecc

Introduzione

Il linguaggio

\mathcal{L}_2

Primi passi in

\mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Ordini

Definizione

Se $X \subseteq \mathbb{N} \times \mathbb{N}$ poniamo

$$\text{fld}(X) = \{ i \mid \exists j((i, j) \in X \vee (j, i) \in X) \},$$
$$i \leq_X j \leftrightarrow (i, j) \in X \text{ e } i <_X j \leftrightarrow i \leq_X j \wedge i \neq j.$$

$X \subseteq \mathbb{N} \times \mathbb{N}$ è **ben fondato** se non esiste $f : \mathbb{N} \rightarrow \text{fld}(X)$ tale che $\forall n f(n+1) <_X f(n)$.

$X \subseteq \mathbb{N} \times \mathbb{N}$ è un **ordine parziale** se valgono:

- $\forall i \in \text{fld}(X)(i \leq_X i)$;
- $\forall i, j \in \text{fld}(X)(i \leq_X j \wedge j \leq_X i \rightarrow i = j)$;
- $\forall i, j, k \in \text{fld}(X)(i \leq_X j \wedge j \leq_X k \rightarrow i \leq_X k)$.

X è un **ordine lineare** se vale anche:

- $\forall i, j \in \text{fld}(X)(i \leq_X j \vee j \leq_X i)$.

Un ordine lineare ben fondato è un **buon ordine**.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Numeri interi

Definiamo una relazione d'equivalenza, pensando (m, n) come $m - n$: $(m, n) =_{\mathbb{Z}} (p, q) \leftrightarrow m + q = n + p$.

Operazioni e ordine sono definiti naturalmente

$$(m, n) +_{\mathbb{Z}} (p, q) = (m + p, n + q)$$

$$(m, n) \cdot_{\mathbb{Z}} (p, q) = (m \cdot p + n \cdot q, m \cdot q + n \cdot p)$$

$$(m, n) <_{\mathbb{Z}} (p, q) \leftrightarrow m + q < n + p$$

Scegliamo come rappresentante di ogni classe d'equivalenza l'elemento minimo.

$$\mathbb{Z} = \{ (m, n) \mid \forall (p, q) < (m, n) (m, n) \neq_{\mathbb{Z}} (p, q) \}$$

Le operazioni si trasferiscono su \mathbb{Z} : se $a, b \in \mathbb{Z}$, $a + b$ è l'unico $c \in \mathbb{Z}$ tale che $c =_{\mathbb{Z}} a +_{\mathbb{Z}} b$.

\mathbb{Z}_2 dimostra che \mathbb{Z} è un dominio d'integrità Euclideo ordinato, ecc

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Numeri razionali

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo
di naturali e
insiemi di
naturali?

Insiemi e
successione finite

Funzioni

Strutture
algebriche e
combinatoriali

I sistemi
numerici

Spazi metrici
completi

La codifica di \mathbb{Q} è analoga, pensando $(a, b) \in \mathbb{Z} \times \mathbb{Z}^+$ come $\frac{a}{b}$:

$$(a, b) =_{\mathbb{Q}} (c, d) \leftrightarrow a \cdot d = c \cdot b.$$

\mathbb{Z}_2 dimostra che \mathbb{Q} è un campo ordinato.

Una successione di razionali è una funzione $f : \mathbb{N} \rightarrow \mathbb{Q}$.
Spesso la indicheremo con $\langle q_k : k \in \mathbb{N} \rangle$, dove $q_k = f(k)$.

Numeri reali

La codifica dei numeri reali comporta dei problemi nuovi: mentre abbiamo definito \mathbb{Z} e \mathbb{Q} come sottoinsiemi di \mathbb{N} non possiamo sperare di fare lo stesso con \mathbb{R} .

I singoli reali saranno sottoinsiemi di \mathbb{N} , e precisamente successioni di Cauchy di razionali convergenti a velocità prescritta.

Questa rappresentazione è la migliore per lavorare con i reali in sottosistemi deboli di Z_2 .

Definizione

Un **numero reale** è una successione di razionali $\langle q_k : k \in \mathbb{N} \rangle$ tale che $\forall k \forall i (|q_k - q_{k+i}| \leq 2^{-k})$.

Due reali $\langle q_k : k \in \mathbb{N} \rangle$ e $\langle r_k : k \in \mathbb{N} \rangle$ sono uguali se $\forall k (|q_k - r_k| \leq 2^{-k+1})$.

Π_1^0

L'uguaglianza tra reali è una relazione d'equivalenza.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Operazioni e ordine sui reali

Usiamo x, y, z, \dots come variabili per i reali.

\mathbb{R} verrà usato informalmente in espressioni come $\exists x \in \mathbb{R} \dots$,
 $\forall n x_n \in \mathbb{R}$, ma **non esiste** come insieme in Z_2 .

\mathbb{Q} viene immerso in \mathbb{R} : $q \in \mathbb{Q} \mapsto x_q = \langle q : k \in \mathbb{N} \rangle \in \mathbb{R}$.

Siano $x = \langle q_k : k \in \mathbb{N} \rangle$ e $y = \langle r_k : k \in \mathbb{N} \rangle$ due reali:

$$x + y = \langle q_{k+1} + r_{k+1} : k \in \mathbb{N} \rangle;$$

$$x \cdot y = \langle q_{n+k} \cdot r_{n+k} : k \in \mathbb{N} \rangle \quad \text{dove } |q_0| + |r_0| + 2 \leq n;$$

$$x \leq y \leftrightarrow \forall k q_k \leq r_k + 2^{-k+1};$$

$$x < y \leftrightarrow \exists k q_k < r_k - 2^{-k+1}.$$

 Π_1^0 Σ_1^0

Z_2 dimostra che \mathbb{R} è un campo ordinato Archimedeo.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Completezza di \mathbb{R}

La completezza di \mathbb{R} non può venir formulata in \mathcal{L}_2 :
non possiamo considerare un arbitrario sottoinsieme di \mathbb{R} .

Una successione di reali è una funzione $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Q}$ tale che $(f)_n$ definita da $(f)_n(k) = f(n, k)$ è un reale per ogni n .
Spesso la indicheremo con $\langle x_n : n \in \mathbb{N} \rangle$, dove $x_n = (f)_n$.

Teorema (Completezza sequenziale di \mathbb{R})

Z_2 dimostra che se $\langle x_n : n \in \mathbb{N} \rangle$ è una successione di reali e esiste $x \in \mathbb{R}$ tale che $\forall n x_n < x$, allora esiste $y \in \mathbb{R}$ tale che $y = \sup\{x_n \mid n \in \mathbb{N}\}$.

Si può definire la nozione di convergenza:

$$x = \lim x_n \leftrightarrow \forall \varepsilon > 0 \exists n \forall i (|x_{n+i} - x| < \varepsilon).$$

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Spazi metrici completi

Definizione

Un (codice per uno) spazio metrico completo \hat{A} consiste di un insieme A e di una successione di reali $d : A \times A \rightarrow \mathbb{R}$ tale che $d(a, a) = 0$, $d(a, b) = d(b, a) \geq 0$ e $d(a, c) \leq d(a, b) + d(b, c)$ per ogni $a, b, c \in A$.

Un punto di \hat{A} è una successione $x = \langle a_k : k \in \mathbb{N} \rangle$ di elementi di A tale che $\forall k \forall i d(a_k, a_{k+i}) \leq 2^{-k}$. Scriviamo $x \in \hat{A}$.

Se $x = \langle a_k : k \in \mathbb{N} \rangle$ e $y = \langle b_k : k \in \mathbb{N} \rangle$ sono punti di \hat{A} poniamo $d(x, y) = \lim d(a_k, b_k)$.

$x = y$ sta per $d(x, y) = 0$, cioè $\forall k d(a_k, b_k) \leq 2^{-k+1}$ (è Π_1^0).

A viene immerso in \hat{A} : $a \in A \mapsto x_a = \langle a : k \in \mathbb{N} \rangle \in \hat{A}$.

A è denso in \hat{A} : $\forall x \in \hat{A} \forall \varepsilon > 0 \exists a \in A d(a, x) < \varepsilon$.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 \mathbb{Z}_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Costruire spazi metrici completi

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

\mathbb{R} è uno spazio metrico completo, con $A = \mathbb{Q}$ e $d(q, r) = |q - r|$, (ma abbiamo usato \mathbb{R} per definire gli spazi metrici completi).

Gli intervalli chiusi di \mathbb{R} sono spazi metrici completi.

In Z_2 si possono costruire spazi metrici completi che sono prodotti, finiti o numerabili, di spazi metrici completi dati.

Queste costruzioni riproducono le definizioni usuali dei prodotti di spazi metrici.

In particolare otteniamo $2^{\mathbb{N}}$ (spazio di Cantor), $\mathbb{N}^{\mathbb{N}}$ (spazio di Baire), $[0, 1]^{\mathbb{N}}$ (cubo di Hilbert), $\mathbb{R}^{\mathbb{N}}$.

Aperti

Sia \hat{A} uno spazio metrico completo: $(a, r) \in A \times \mathbb{Q}^+$ rappresenta $B(a; r)$, la palla aperta di centro a e raggio r . Gli aperti di \hat{A} sono unioni di queste palle aperte.

Definizione

Un (codice per un) aperto in \hat{A} è un insieme $U \subseteq \mathbb{N} \times A \times \mathbb{Q}^+$. Se $x \in \hat{A}$ diciamo che $x \in U$ quando $\exists (n, a, r) \in U$ $d(a, x) < r$.

$x \in U$ è Σ_1^0 , e in un certo senso vale il contrario.

Teorema

Sia \hat{A} uno spazio metrico completo e $\varphi(x)$ una formula Σ_1^0 con la proprietà che se $x, y \in \hat{A}$, $\varphi(x)$ e $x = y$ allora $\varphi(y)$. Allora Z_2 dimostra l'esistenza di un aperto U in \hat{A} tale che

$$x \in U \leftrightarrow \varphi(x).$$

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Funzioni continue

Siano \hat{A} e \hat{B} spazi metrici completi: il codice di una funzione continua ϕ da \hat{A} in \hat{B} conterrà informazioni del tipo “ ϕ manda la palla $B(a; q)$ di \hat{A} nella chiusura della palla $B(b; r)$ di \hat{B} ”.

Se $(a, q), (a', q') \in A \times \mathbb{Q}^+$, $(a, q) \Subset (a', q')$ sta per $d(a, a') < q' - q$.

Se $(a, q) \Subset (a', q')$ allora $B(a; q) \subseteq B(a'; q')$.

Definizione

Un (codice per una) funzione continua parziale ϕ da \hat{A} in \hat{B} è un insieme $\Phi \subseteq \mathbb{N} \times A \times \mathbb{Q}^+ \times B \times \mathbb{Q}^+$ che soddisfa

- se $(a, q)\Phi(b, r)$ e $(a, q)\Phi(b', r')$ allora $d(b, b') < r + r'$;
- se $(a, q)\Phi(b, r)$ e $(a', q') \Subset (a, q)$ allora $(a', q')\Phi(b, r)$;
- se $(a, q)\Phi(b, r)$ e $(b, r) \Subset (b', r')$ allora $(a, q)\Phi(b', r')$;

dove $(a, q)\Phi(b, r)$ significa $\exists n (n, a, q, b, r) \in \Phi$.

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Dominio di una funzione continua

Introduzione

Il linguaggio
 \mathcal{L}_2

Primi passi in
 Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Se Φ è il codice per una funzione continua ϕ da \hat{A} in \hat{B} e $x \in \hat{A}$ diciamo che $x \in \text{dom}(\phi)$ quando

$$\forall \varepsilon > 0 \exists a, q, b, r ((a, q)\Phi(b, r) \wedge d(a, x) < q \wedge r < \varepsilon).$$

Z_2 prova che se $x \in \text{dom}(\phi)$ esiste un unico $y \in \hat{B}$ tale che

$$\forall a, q, b, r ((a, q)\Phi(b, r) \wedge d(a, x) < q \rightarrow d(b, y) \leq r).$$

Poniamo $\phi(x) = y$.

ϕ è totale se $\forall x \in \hat{A} x \in \text{dom}(\phi)$, e scriviamo $\phi : \hat{A} \rightarrow \hat{B}$, sottintendendo la continuità (nel nostro linguaggio non possiamo considerare funzioni arbitrarie da \hat{A} in \hat{B}).

Alcune funzioni continue

Definiamo un codice per $id : \hat{A} \rightarrow \hat{A}$.

$(a, q) \in (a', q')$ è Σ_1^0 e possiamo scriverlo come $\exists n \theta(n, a, q, a', q')$ con $\theta \in \Sigma_0^0$.

Sia $\Phi = \{ (n, a, q, a', q') \mid \theta(n, a, q, a', q') \}$.

Se $y \in \hat{B}$ la funzione costante $\phi_y : \hat{A} \rightarrow \hat{B}$ ha codice Φ_y tale che $(a, q)\Phi_y(b, r) \leftrightarrow d(y, b) < r$.

Analogamente Z_2 dimostra che

- la funzione distanza $d : \hat{A} \times \hat{A} \rightarrow \mathbb{R}$ è continua;
- somma, differenza, prodotto e divisione sono continue su \mathbb{R} ;
- le funzioni continue sono chiuse per composizione.

Introduzione

Il linguaggio \mathcal{L}_2

Primi passi in Z_2

Parliamo solo di naturali e insiemi di naturali?

Insiemi e successione finite

Funzioni

Strutture algebriche e combinatoriali

I sistemi numerici

Spazi metrici completi

Il sistema base per la reverse mathematics

- ① Breve carrellata storica e bibliografia
- ② Il sistema RCA_0
- ③ Analisi
- ④ Logica
- ⑤ Algebra

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica

Algebra

Breve carrellata storica

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica

Algebra

La ricerca sistematica dei sottosistemi di Z_2 sufficienti e necessari alla dimostrazione di teoremi matematici è stata iniziata da Harvey Friedman intorno al 1970.

Friedman iniziò a lavorare nel contesto dei sottosistemi di Z_2 ed individuò il sistema base RCA_0 , che definiremo e svilupperemo tra poco.

Egli iniziò a dimostrare in RCA_0 l'equivalenza tra teoremi e assiomi, e conìò il termine *reverse mathematics*.

Alla fine degli anni '70 Steve Simpson mostrò che per la maggior parte dei teoremi T , RCA_0 dimostra T oppure l'equivalenza tra T e uno tra WKL_0 , ACA_0 , ATR_0 e $\Pi_1^1\text{-}CA_0$.

RCA_0 , WKL_0 , ACA_0 , ATR_0 e $\Pi_1^1\text{-}CA_0$ sono i *big five* della *reverse mathematics*.

Breve carrellata storica

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica

Algebra

Negli anni '90 un numero crescente di logici si è interessato alla *reverse mathematics*.

Si sono scoperti alcuni teoremi che non ricadono nello schema dei *big five*. Per alcuni di essi il problema della relazione con i cinque sistemi è in parte ancora aperto.

Oggi la *reverse mathematics* è un campo di ricerca molto attivo in cui vengono utilizzate tecniche provenienti da molte parti della logica.

Bibliografia sulla reverse mathematics 1

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica

Algebra



Stephen G. Simpson

Subsystems of second order arithmetic.

Cambridge University Press, 2nd ed., 2009.



Stephen G. Simpson

The Gödel hierarchy and reverse mathematics.

in *Kurt Gödel, Essays for His Centennial*,
vol 33 of *Lecture Notes in Logic*

Association for Symbolic Logic, 2010.



Richard A. Shore

Reverse mathematics: the playground of logic.

The Bulletin of Symbolic Logic **16** (2010), 378–402.

Bibliografia sulla reverse mathematics 2

Breve
carrellata
storica e
bibliografia

Il sistema
RCA₀

Analisi

Logica

Algebra



Alberto Marcone

Equivalenze tra teoremi: il programma di ricerca della reverse mathematics.

La Matematica nella Società e nella Cultura, Rivista dell'Unione Matematica Italiana **2** (2009), 101–126.



Stephen G. Simpson, editor

Reverse mathematics 2001,
vol 21 of *Lecture Notes in Logic*.
Association for Symbolic Logic, 2005.



Antonio Montalbán

Open questions in Reverse Mathematics.
The Bulletin of Symbolic Logic, to appear.

Gli assiomi di RCA₀ sono:

- gli assiomi aritmetici di \mathbb{Z}_2 ;
- lo schema di Δ_1^0 -comprensione:
se φ e ψ sono formule Σ_1^0 e Π_1^0 in cui X non è libera

$$\forall n(\varphi(n) \leftrightarrow \psi(n)) \rightarrow \exists X \forall n(n \in X \leftrightarrow \varphi(n));$$

- lo schema di Σ_1^0 -induzione: se φ è Σ_1^0

$$\varphi(0) \wedge \forall n(\varphi(n) \rightarrow \varphi(n+1)) \rightarrow \forall n \varphi(n).$$

RCA abbrevia Recursive Comprehension Axiom.



Perché Σ_1^0 -induzione?

In RCA_0 al posto dell'assioma di induzione abbiamo lo schema di Σ_1^0 -induzione.

Σ_1^0 -induzione è necessaria per la codifica degli insiemi finiti: si sa che questa codifica non è possibile nel sistema con il solo assioma di induzione.

Un sistema utilizzato a volte è RCA_0^* , che è formulata nel linguaggio ottenuto aggiungendo a \mathcal{L}_2 una funzione binaria per l'esponenziale.

RCA_0^* consiste degli assiomi aritmetici più $\forall n(n^0 = 1)$ e $\forall n \forall m(n^{m+1} = n^m \cdot n)$, l'assioma di induzione e lo schema di Δ_1^0 -comprensione.

RCA_0^* è strettamente più debole di RCA_0 , ma in esso si possono codificare gli insiemi finiti.

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Gli assiomi
 ω -modelli
Alcuni principi
derivabili

Analisi

Logica

Algebra

ω -modelli di RCA_0

Teorema

$\mathcal{S} \subseteq \mathcal{P}(\omega)$ è un ω -modello di RCA_0 se e solo se \mathcal{S} è un ideale di Turing, cioè

- $\mathcal{S} \neq \emptyset$;
- se $X, Y \in \mathcal{S}$ allora $X \oplus Y = \{2n \mid n \in X\} \cup \{2n+1 \mid n \in Y\} \in \mathcal{S}$;
- se $X \in \mathcal{S}$ e $Y \leq_T X$ allora $Y \in \mathcal{S}$.

Questo segue dal fatto che Y è c.e. in X se e solo se Y è definibile da una formula Σ_1^0 con parametro X .

Quindi $Y \leq_T X_1 \oplus \dots \oplus X_k$ se e solo se Y e $\omega \setminus Y$ sono definibili da formule Σ_1^0 con parametri X_1, \dots, X_k .

In particolare **REC** è il più piccolo ω -modello di RCA_0 .

Insiemi infiniti e funzioni

RCA_0 è sufficiente per le codifiche di insiemi e successioni finite. In RCA_0 le funzioni sono chiuse sotto composizione e ricorsione primitiva.

Lemma (RCA_0)

Se X è infinito esiste $\pi_X : \mathbb{N} \rightarrow \mathbb{N}$ tale che

$\forall m \forall m' < m \pi_X(m') < \pi_X(m)$ e

$\forall n (n \in X \leftrightarrow \exists m \pi_X(m) = n)$.

Dimostrazione.

$\nu_X = \{ (k, n) \mid k \leq n \wedge n \in X \wedge \forall n' < n (k \leq n' \rightarrow n' \notin X) \}$

$\nu_X : \mathbb{N} \rightarrow X$ calcola il prossimo elemento di X .

Per ricorsione primitiva definiamo π_X :

$$\pi_X(0) = \nu_X(0); \quad \pi_X(m+1) = \nu_X(\pi_X(m) + 1).$$

Per Σ_0^0 -induzione si dimostrano le proprietà di π_X . □

Formule Σ_1^0 e funzioni

Lemma

Sia $\varphi(n)$ una formula Σ_1^0 in cui X e f non occorrono libere. RCA_0 dimostra che vale una delle seguenti possibilità:

- esiste un insieme finito X tale che $\forall n(\varphi(n) \leftrightarrow n \in X)$;
- esiste una funzione iniettiva $f : \mathbb{N} \rightarrow \mathbb{N}$ tale che $\forall n(\varphi(n) \leftrightarrow \exists m f(m) = n)$.



Dimostrazione.

Supponiamo non valga la prima possibilità.

Sia $\varphi(n) \leftrightarrow \exists j \theta(j, n)$ con $\theta \Sigma_0^0$.

Per Σ_0^0 -comprensione sia

$$X = \{ (j, n) \mid \theta(j, n) \wedge \forall i < j \neg \theta(i, n) \}.$$

X è infinito e sia π_X come prima.

Se $p_2((j, n)) = n$, $f = p_2 \circ \pi_X$ è la funzione cercata. □

Σ_1^0 -comprensione limitata

Lemma (Σ_1^0 -comprensione limitata)

Sia $\varphi(i)$ una formula Σ_1^0 in cui X non occorre libera.

RCA_0 dimostra $\forall n \exists X \forall i (i \in X \leftrightarrow (i < n \wedge \varphi(i)))$.

Dimostrazione.

Fissiamo n e per assurdo supponiamo che X finito con la proprietà desiderata non esista.

Sia $f : \mathbb{N} \rightarrow \mathbb{N}$ iniettiva che enumera gli i tali che $i < n \wedge \varphi(i)$.

In particolare $f \upharpoonright \{0, \dots, n\}$ è una funzione finita iniettiva da $\{0, \dots, n\}$ in $\{0, \dots, n-1\}$.

Per Σ_1^0 -induzione è facile dimostrare che nessuna funzione finita ha questa caratteristica. □

[La Σ_1^0 -comprensione limitata è equivalente alla Σ_1^0 -induzione, nella teoria con l'assioma di induzione.]

Π_1^0 -induzione

Lemma

Per ogni formula Π_1^0 $\psi(n)$ RCA_0 dimostra
$$\psi(0) \wedge \forall n(\psi(n) \rightarrow \psi(n+1)) \rightarrow \forall n \psi(n).$$

Dimostrazione.

Assumiamo $\psi(0)$ e $\forall n(\psi(n) \rightarrow \psi(n+1))$ e fissiamo n .

Per Σ_1^0 -comprensione limitata sia X tale che

$$\forall i(i \in X \leftrightarrow i \leq n \wedge \neg \psi(i)).$$

Per Σ_0^0 -comprensione esiste

$$Y = \{i \mid i \notin X\} = \{i \mid i > n \vee \psi(i)\}.$$

Le ipotesi implicano $0 \in Y$ e $\forall i(i \in Y \rightarrow i+1 \in Y)$.

Per l'assioma di induzione $Y = \mathbb{N}$ e in particolare $n \notin X$,
cioè $\psi(n)$. □

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Gli assiomi
 ω -modelli

Alcuni principi
derivabili

Analisi

Logica

Algebra

Fallimento della completezza sequenziale di \mathbb{R} in RCA_0

RCA_0 è sufficiente per la codifica dei sistemi numerici sviluppata in Z_2 , ma RCA_0 non basta per mostrare la completezza sequenziale di \mathbb{R} .

Controesempio

Sia f iniettiva e computabile con immagine un insieme non computabile A .

Per ogni n sia $x_n = \sum_{i < n} 2^{-f(i)}$.

La successione $\langle x_n : n \in \mathbb{N} \rangle$ è computabile e limitata da 2.

Se $x = \sup\{x_n \mid n \in \mathbb{N}\}$ si ha per ogni j

$$\begin{aligned}j \in A &\leftrightarrow \exists i f(i) = j \\ &\leftrightarrow \forall n (|x - x_n| < 2^{-j} \rightarrow \exists i < n f(i) = j)\end{aligned}$$

Quindi $A \leq_T x$ e x non è computabile.



Perciò **REC** non è un modello per la completezza sequenziale di \mathbb{R} e RCA_0 non la dimostra.

Completezza per intervalli annidati in RCA_0

Teorema (RCA_0)

Se $\langle a_n : n \in \mathbb{N} \rangle$ e $\langle b_n : n \in \mathbb{N} \rangle$ sono successioni di reali tali che $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ per ogni n e $\lim(b_n - a_n) = 0$, allora esiste un reale x tale che $x = \lim a_n = \lim b_n$.

Dimostrazione.

Siano $\langle q_{nk} : n, k \in \mathbb{N} \rangle$ e $\langle q'_{nk} : n, k \in \mathbb{N} \rangle$ le successioni di razionali tali che $a_n = \langle q_{nk} : k \in \mathbb{N} \rangle$ e $b_n = \langle q'_{nk} : k \in \mathbb{N} \rangle$. Per ogni k sia $f(k) = \min n (n \geq k + 3 \wedge |q_{nn} - q'_{nn}| < 2^{-k-2})$. Se $r_k = q_{f(k)f(k)}$ allora $x = \langle r_k : k \in \mathbb{N} \rangle$ è un reale. 
 $|x - a_{f(k)}| \leq |x - r_k| + |r_k - a_{f(k)}| \leq 2^{-k} + 2^{-f(k)} < 2^{-k+1}$ e quindi $x = \lim a_n$.
 $|x - b_{f(k)}| \leq |x - r_k| + |r_k - q'_{f(k)f(k)}| + |q'_{f(k)f(k)} - b_{f(k)}| \leq 2^{-k} + 2^{-k-2} + 2^{-f(k)} < 2^{-k+1}$ e quindi $x = \lim b_n$. 

x è un reale perché...

$$a_n \leq a_{n+1} \leq b_{n+1} \leq b_n,$$

$$a_n = \langle q_{nk} : k \in \mathbb{N} \rangle \text{ e } b_n = \langle q'_{nk} : k \in \mathbb{N} \rangle.$$

$$f(k) = \min n (n \geq k + 3 \wedge |q_{nn} - q'_{nn}| < 2^{-k-2}), \quad r_k = q_{f(k)f(k)}.$$

$x = \langle r_k : k \in \mathbb{N} \rangle$ è un reale perché

$$\begin{aligned} |r_{f(k)} - r_{f(k+i)}| &\leq |r_{f(k)} - a_{f(k)}| + |a_{f(k)} - b_{f(k+i)}| \\ &\quad + |b_{f(k+i)} - q'_{f(k+i)f(k+i)}| + |q'_{f(k+i)f(k+i)} - r_{f(k+i)}| \\ &\leq 2^{-f(k)} + |a_{f(k)} - b_{f(k)}| + 2^{-f(k+i)} + 2^{-k-i-2} \\ &\leq 2^{-k-3} + |a_{f(k)} - r_{f(k)}| + |r_{f(k)} - q'_{f(k)f(k)}| \\ &\quad + |q'_{f(k)f(k)} - b_{f(k)}| + 2^{-k-4} + 2^{-k-3} \\ &\leq 2^{-k-3} + 2^{-k-3} + 2^{-k-2} + 2^{-k-3} + 2^{-k-4} + 2^{-k-3} \\ &< 2^{-k}. \end{aligned}$$

\mathbb{R} è più che numerabile in RCA_0

Teorema (RCA_0)

Se $\langle x_n : n \in \mathbb{N} \rangle$ è una successione di reali allora esiste $x \in \mathbb{R}$ tale che $\forall n x \neq x_n$.

Dimostrazione.

Sia $\langle q_{nk} : n, k \in \mathbb{N} \rangle$ la successione di razionali tale che $x_n = \langle q_{nk} : k \in \mathbb{N} \rangle$.

Per ricorsione primitiva definiamo $(a_0, b_0) = (0, 1)$ e

$$(a_{n+1}, b_{n+1}) = \begin{cases} \left(\frac{a_n + 3b_n}{4}, b_n \right) & \text{se } q_{n,2n+3} \leq \frac{a_n + b_n}{2}; \\ \left(a_n, \frac{3a_n + b_n}{4} \right) & \text{altrimenti.} \end{cases}$$

$|b_n - a_n| = 2^{-2n}$ e $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$, perciò esiste $x = \lim a_n = \lim b_n$.

Se $q_{n,2n+3} \leq \frac{a_n + b_n}{2}$ allora $x_n \leq \frac{a_n + b_n}{2} + 2^{-2n-3} < a_{n+1} \leq x$.

Altrimenti $x_n \geq \frac{a_n + b_n}{2} - 2^{-2n-3} > b_{n+1} \geq x$. □

Funzioni continue da ieri

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi
I reali
Spazi metrici
completi

Logica

Algebra

Definizione

Un (codice per una) funzione continua parziale ϕ da \hat{A} in \hat{B} è un insieme $\Phi \subseteq \mathbb{N} \times A \times \mathbb{Q}^+ \times B \times \mathbb{Q}^+$ che soddisfa

- se $(a, q)\Phi(b, r)$ e $(a, q)\Phi(b', r')$ allora $d(b, b') < r + r'$;
- se $(a, q)\Phi(b, r)$ e $(a', q') \in (a, q)$ allora $(a', q')\Phi(b, r)$;
- se $(a, q)\Phi(b, r)$ e $(b, r) \in (b', r')$ allora $(a, q)\Phi(b', r')$;

dove $(a, q)\Phi(b, r)$ significa $\exists n (n, a, q, b, r) \in \Phi$ e ci dice che “ ϕ manda la palla $B(a; q)$ di \hat{A}

nella chiusura della palla $B(b; r)$ di \hat{B} ”.

Il teorema del valor medio in RCA_0

Teorema (RCA_0)

Se $\phi : [0, 1] \rightarrow \mathbb{R}$ è continua e $\phi(0) < 0 < \phi(1)$
allora esiste $x \in [0, 1]$ tale che $\phi(x) = 0$.

Dimostrazione.

Se $\phi(s) = 0$ per qualche $s \in \mathbb{Q}$, siamo a posto.

Altrimenti $X = \{s \in \mathbb{Q} \mid \phi(s) < 0\}$ esiste per Δ_1^0 -comp:

$$\begin{aligned}\phi(s) < 0 &\leftrightarrow \exists(n, a, q, b, r) \in \Phi (a - q < s < a + q \wedge b + r < 0) \\ &\leftrightarrow \forall(n, a, q, b, r) \in \Phi (a - q < s < a + q \rightarrow b - r < 0)\end{aligned}$$

Per ricorsione primitiva definiamo $(a_0, b_0) = (0, 1)$ e

$$(a_{n+1}, b_{n+1}) = \begin{cases} (\frac{a_n + b_n}{2}, b_n) & \text{se } \frac{a_n + b_n}{2} \in X; \\ (a_n, \frac{a_n + b_n}{2}) & \text{se } \frac{a_n + b_n}{2} \notin X. \end{cases}$$

Per Σ_0^0 -ind si ha $\forall n (\phi(a_n) < 0 < \phi(b_n) \wedge |b_n - a_n| = 2^{-n})$.

Se $x = \lim a_n = \lim b_n$ si ha $\phi(x) = 0$. □

Spazi metrici completi da ieri

Definizione

Un (codice per uno) spazio metrico completo \hat{A} consiste di un insieme A e di una successione di reali $d : A \times A \rightarrow \mathbb{R}$ tale che $d(a, a) = 0$, $d(a, b) = d(b, a) \geq 0$ e $d(a, c) \leq d(a, b) + d(b, c)$ per ogni $a, b, c \in A$.

Un punto di \hat{A} è una successione $x = \langle a_k : k \in \mathbb{N} \rangle$ di elementi di A tale che $\forall k \forall i d(a_k, a_{k+i}) \leq 2^{-k}$. Scriviamo $x \in \hat{A}$.

Se $x = \langle a_k : k \in \mathbb{N} \rangle$ e $y = \langle b_k : k \in \mathbb{N} \rangle$ sono punti di \hat{A} poniamo $d(x, y) = \lim d(a_k, b_k)$.

$x = y$ sta per $d(x, y) = 0$, cioè $\forall k d(a_k, b_k) \leq 2^{-k+1}$ (è Π_1^0).

Definizione

Un (codice per un) aperto in \hat{A} è un insieme $U \subseteq \mathbb{N} \times A \times \mathbb{Q}^+$. Se $x \in \hat{A}$ diciamo che $x \in U$ quando $\exists (n, a, r) \in U d(a, x) < r$.

Aperti e formule Σ_1^0 in RCA_0

Teorema

Sia $\varphi(x) \Sigma_1^0$ tale che se $x, y \in \hat{A}$, $\varphi(x)$ e $x = y$ allora $\varphi(y)$.
Allora RCA_0 dimostra l'esistenza di U tale che $x \in U \leftrightarrow \varphi(x)$.

Dimostrazione.

Sia $\theta(n) \Sigma_0^0$ tale che RCA_0 prova che se $x = \langle b_n \rangle \in \hat{A}$,

$$\varphi(x) \leftrightarrow \exists k \theta(\langle b_n : n \leq k \rangle).$$

$$U = \{ (\langle a_n : n \leq k \rangle, a_k, 2^{-k-1}) \mid \\ \theta(\langle a_n : n \leq k \rangle) \wedge \forall i \leq k \forall j < i d(a_i, a_j)_{k+1} \leq 2^{-j-1} \}$$

(dove se $d(a, b) = \langle q_m : m \in \mathbb{N} \rangle$, $d(a, b)_k = q_k$) è un aperto.

Si dimostra che $\forall x \in \hat{A} (x \in U \leftrightarrow \varphi(x))$. \square

Altri teoremi sugli spazi metrici completi in RCA_0

Paracompattezza degli spazi metrici completi:

Teorema (RCA_0)

Se \hat{A} è uno spazio metrico completo e $\langle U_n : n \in \mathbb{N} \rangle$ un suo ricoprimento aperto, esiste un ricoprimento aperto $\langle V_n : n \in \mathbb{N} \rangle$ tale che $V_n \subseteq U_n$ per ogni n e $\langle V_n \rangle$ è localmente finito (cioè per ogni $x \in \hat{A}$ esiste U aperto con $x \in U$ tale che $U \cap V_n \neq \emptyset$ per finiti n).

Teorema di estensione di Tietze:

Teorema (RCA_0)

Se \hat{A} è uno spazio metrico completo, C un suo chiuso e $\phi : C \rightarrow [0, 1]$, esiste $\psi : \hat{A} \rightarrow [0, 1]$ tale che $\psi(x) = \phi(x)$ per ogni $x \in C$.

Nozioni logiche

Fissiamo un linguaggio numerabile $L \subseteq \mathbb{N}$
ed una numerazione di Gödel di termini e formule.
Usiamo solo \neg , \wedge e \forall .

Sistema alla Hilbert, con il *modus ponens* come unica regola.

Per ric prim si definiscono gli insiemi Term_L (termini),
 Form_L (formule), En_L (enunciati), Ass_L (assiomi logici).

$$\text{Dim}(X, p) \leftrightarrow p \in \mathbb{N}^{<\mathbb{N}} \wedge \forall k < |p| (p(k) \in \text{Form}_L) \wedge \Sigma_0^0 \\ \forall k < |p| (p(k) \in X \cup \text{Ass}_L \vee \exists i, j < k (p(i) = 'p(j) \rightarrow p(k)')).$$

$$\text{Prov}(X, \varphi) \leftrightarrow \exists p (\text{Dim}(X, p) \wedge p(|p| - 1) = \varphi) \quad \Sigma_1^0$$

$$\text{Ch}(X) \leftrightarrow \forall \sigma \in \text{En}_L (\text{Prov}(X, \sigma) \rightarrow \sigma \in X) \quad \Pi_1^0$$

$$\text{Coer}(X) \leftrightarrow \forall \sigma \in \text{En}_L (\neg \text{Prov}(X, \sigma) \vee \neg \text{Prov}(X, \neg \sigma)) \quad \Pi_1^0$$

$$\text{Compl}(X) \leftrightarrow \forall \sigma \in \text{En}_L (\text{Prov}(X, \sigma) \vee \text{Prov}(X, \neg \sigma)) \quad \Pi_2^0$$

Breve
carrellata
storica e
bibliografia

Il sistema
RCA₀

Analisi

Logica

Nozioni logiche
Il teorema di
completezza
Il teorema di
correttezza

Algebra

Una versione debole del lemma di Lindenbaum in RCA_0

Lemma (RCA_0)

Sia $X \subseteq \text{En}_L$ tale che $\text{Coer}(X)$ e $\text{Ch}(X)$. Esiste $X^* \subseteq \text{En}_L$ tale che $X \subseteq X^*$, $\text{Coer}(X^*)$, $\text{Ch}(X^*)$ e $\text{Compl}(X^*)$.

Dimostrazione.

Sia $\langle \sigma_n : n \in \mathbb{N} \rangle$ un'enumerazione iniettiva di En_L .

Per ricorsione primitiva definiamo

$$\sigma_n^* = \begin{cases} \sigma_n & \text{se } (\sigma_0^* \wedge \dots \wedge \sigma_{n-1}^* \rightarrow \sigma_n) \in X; \\ \neg \sigma_n & \text{altrimenti.} \end{cases}$$

$X^* = \{ \sigma_n^* \mid n \in \mathbb{N} \} = \{ \sigma_n \mid \sigma_n = \sigma_n^* \}$ esiste per Σ_0^0 -comp.

$X \subseteq X^*$, $\text{Ch}(X^*)$ e $\text{Compl}(X^*)$ sono immediati.

Per Π_1^0 -ind si dimostra $\forall n \text{ Coer}(X \cup \{ \sigma_0^*, \dots, \sigma_{n-1}^* \})$. □

L'ipotesi $\text{Ch}(X)$ usualmente non compare e la condizione della prima clausola è $\text{Prov}(X \cup \{ \sigma_0^*, \dots, \sigma_{n-1}^* \}, \sigma_n)$.

Modelli in RCA_0

Definizione

Un **modello** è una funzione $M : T_M \cup E_M \rightarrow |M| \cup \{0, 1\}$ dove $|M| \subseteq \mathbb{N}$ (universo di M) e T_M, E_M sono gli insiemi dei termini chiusi e degli enunciati di $L_M = L \cup \{\underline{m} \mid m \in |M|\}$. M soddisfa le condizioni della definizione di verità di Tarski:

- se $t \in T_M$ allora $M(t) \in |M|$;
- $M(\underline{m}) = m$;
- se $\sigma \in E_M$ allora $M(\sigma) \in \{0, 1\}$;
- se $t_0, s_0, \dots, t_n, s_n \in T_M$ sono tali che $M(t_i) = M(s_i)$ allora $M(f(\bar{t})) = M(f(\bar{s}))$ e $M(r(\bar{t})) = M(r(\bar{s}))$ per ogni simbolo di funzione f e simbolo di relazione r di L ;
- $M(\neg\sigma) = 1 - M(\sigma)$;
- $M(\sigma_1 \wedge \sigma_2) = M(\sigma_1) \cdot M(\sigma_2)$;
- $M(\forall v \varphi(v)) = \prod_{m \in |M|} M(\varphi(\underline{m}))$.

Una versione debole del teorema di completezza di Gödel in RCA_0

Teorema (RCA_0)

Sia $X \subseteq \text{En}_L$ tale che $\text{Coer}(X)$ e $\text{Ch}(X)$.

Esiste un modello M tale che $\forall \sigma \in X M(\sigma) = 1$.

Dimostrazione.

Siano $C = \{c_n\}$ nuovi simboli di costante e $\{\varphi_n(x)\}$ le formule con una variabile libera di $L_1 = L \cup C$. c_n non compare in φ_i per $i \leq n$. η_n è $\exists x \varphi_n(x) \rightarrow \varphi(c_n)$ (enunciati di Henkin).

Se $\tau \in \text{En}_{L_1}$, $\bar{\tau} \in \text{En}_L$ è la ch univ di τ con c_n sostituita da z_n .

$X_1 = \{ \sigma \in \text{En}_{L_1} \mid \text{Prov}(X \cup \{ \eta_n \mid n \in \mathbb{N} \}, \sigma) \} =$
 $\{ \sigma \in \text{En}_{L_1} \mid \overline{\eta_0 \wedge \dots \wedge \eta_{m_\sigma} \rightarrow \sigma} \in X \}$ esiste per Σ_0^0 -comp.

$X \subseteq X_1$, $\text{Ch}(X_1)$ e $\text{Coer}(X_1)$. Per il lemma di Lindenbaum esiste X_1^* , completamento di X_1 . M si "legge" da X_1^* :

$|M| = \{ c_n \mid \forall i < n (c_i = c_n) \notin X_1^* \},$

$M(t) = \min\{ c_n \mid (c_n = t) \in X_1^* \}, M(\sigma) = 1$ sse $\sigma \in X_1^*$. \square

Un'altra versione debole del teorema di completezza di Gödel in RCA_0

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica

Nozioni logiche
Il teorema di
completezza
Il teorema di
correttezza

Algebra

Teorema (RCA_0)

Sia $X \subseteq \text{En}_L$ tale che $\text{Coer}(X)$ e $\text{Compl}(X)$.

Esiste un modello M tale che $\forall \sigma \in X M(\sigma) = 1$.

Dimostrazione.

Per ogni $\sigma \in \text{En}_L$ si ha

$$\text{Prov}(X, \sigma) \leftrightarrow \neg \text{Prov}(X, \neg \sigma).$$

Quindi $X_1 = \{ \sigma \in \text{En}_L \mid \text{Prov}(X, \sigma) \}$ esiste per Δ_1^0 -comp.

$\text{Coer}(X_1)$, $\text{Ch}(X_1)$ e si può applicare il teorema precedente.

Dato che $X \subseteq X_1$ siamo a posto. □

Fallimento del teorema di completezza di Gödel in RCA_0

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica
Nozioni logiche
Il teorema di
completezza
Il teorema di
correttezza

Algebra

Il teorema di completezza di Gödel asserisce:

$\text{Coer}(X)$ *implica l'esistenza di un modello M per X .*

Controesempio

Se \mathbf{Q} sono i finiti assiomi dell'aritmetica di Robinson,
 $\text{REC} \models \text{Coer}(\mathbf{Q})$, ma \mathbf{Q} non ha modelli computabili.

Quindi RCA_0 non dimostra il teorema di completezza di Gödel.

Il teorema di correttezza in RCA_0

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica
Nozioni logiche
Il teorema di
completezza
Il teorema di
correttezza

Algebra

Teorema (RCA_0)

*Siano $X \subseteq \text{En}_L$ e M un modello tale che $\forall \sigma \in X M(\sigma) = 1$.
Allora $\text{Coer}(X)$.*

Dimostrazione.

Se $\text{Dim}(X, p)$ per induzione su $k < |p|$ si dimostra
 $M(\forall(p(k))) = 1$.

Perciò $\text{Prov}(X, \sigma)$ implica $M(\sigma) = 1$ e quindi $M(\neg\sigma) = 0$,
cioè $\neg\text{Prov}(X, \neg\sigma)$. □

Un rafforzamento del teorema di correttezza in RCA_0

Definizione

Sia $X \subseteq \text{En}_L$. Un **modello debole di X** è una funzione $M : T_M \cup E_M^X \rightarrow |M| \cup \{0, 1\}$ dove $E_M^X \subseteq E_M$ sono le combinazioni proposizionali di istanze di sostituzione di sottoformule di elementi di X .

M deve soddisfare le stesse condizioni di un modello, ma la clausola su $M(\forall v \varphi(v))$ si applica solo se $\forall v \varphi(v) \in E_M^X$. Inoltre chiediamo che $\forall \sigma \in X M(\sigma) = 1$.

Teorema (RCA_0)

Siano $X \subseteq \text{En}_L$ e M un modello debole di X . Allora $\text{Coer}(X)$.

La dimostrazione sfrutta un calcolo dei sequenti con eliminazione del taglio.

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica
Nozioni logiche
Il teorema di
completezza
Il teorema di
correttezza

Algebra

Campi

Un **campo** K consiste di un insieme $|K|$, di elementi 0_K e 1_K , di operazioni binarie $+_K$ e \cdot_K e di un'operazione unaria $-_K$, che soddisfano gli usuali assiomi per i campi.

L'**anello dei polinomi su K** è

$$K[x] = \{ \langle a_0, \dots, a_n \rangle \mid \forall i \leq n \ a_i \in K \wedge (n > 0 \rightarrow a_n \neq 0_K) \}.$$

Scriveremo $f(x) = \sum_{i=0}^n a_i x^i$ al posto di $\langle a_0, \dots, a_n \rangle$ e $f(a) = \sum_{i=0}^n a_i a^i$ quando $a \in K$.

K è **algebricamente chiuso** se per ogni $f(x) \in K[x]$ di grado ≥ 1 esiste $a \in K$ tale che $f(a) = 0_K$.

Una **chiusura algebrica** di K consiste di un campo algebricamente chiuso \tilde{K} e di un monomorfismo $h : K \rightarrow \tilde{K}$ tali che $\forall b \in \tilde{K} \exists f(x) \in K[x] (f(x) \neq 0_K \wedge h(f)(b) = 0_{\tilde{K}})$.

RCA₀ **non dimostra** l'esistenza dell'immagine di h .

Eliminazione dei quantificatori per campi algebricamente chiusi in RCA_0

Siano $L = \{0, 1, -, +, \cdot\}$ e $F \subset \text{En}_L$ gli assiomi di campo.

L'insieme ACF degli assiomi per campi algebricamente chiusi è

$$F \cup \{ \forall x_0 \dots \forall x_n \exists y (y^{n+1} + x_n \cdot y^n + \dots + x_0 = 0) \mid n \in \mathbb{N} \}.$$

Lemma (RCA_0)

- Per ogni $\varphi \in \text{En}_L$ esiste $\varphi^* \in \text{En}_L$ priva di quantificatori tale che $\text{Prov}(\text{ACF}, \varphi \leftrightarrow \varphi^*)$;
- se $\varphi \in \text{En}_L$ è priva di quantificatori e $\text{Prov}(\text{ACF}, \varphi)$ allora $\text{Prov}(F, \varphi)$.

Le usuali dimostrazioni puramente sintattiche possono venir copiate in RCA_0 .

Esistenza della chiusura algebrica

Teorema (RCA_0)

Ogni campo (numerabile) K ha una chiusura algebrica.

Sia Δ_K l'insieme degli enunciati privi di quantificatori di L_K che sono veri in K . Siano $X = \Delta_K \cup F$ e $X' = \Delta_K \cup ACF$.

A partire da K è facile costruire un modello debole per X .

Per il rafforzamento del teorema di correttezza, $\text{Coer}(X)$.

Allora $\text{Coer}(X')$ per la seconda parte dell'eliminazione dei quantificatori.

Per la prima parte $\text{Compl}(X')$.

Per completezza X' ha un modello M .

$|M|$ può essere visto come un campo algebricamente chiuso e esiste $k : K \hookrightarrow |M|$.

Però $|M|$ può essere troppo grande...

Completamento della dimostrazione

Breve
carrellata
storica e
bibliografia

Il sistema
 RCA_0

Analisi

Logica

Algebra
Campi

$|M|$ è algebricamente chiuso e esiste $k : K \hookrightarrow |M|$.

$$\varphi(b) \leftrightarrow b \in |M| \wedge \exists f(x) \in K[x] \setminus \{0_K\} k(f)(b) = M(0) \quad \Sigma_1^0$$

Sia $g : \mathbb{N} \rightarrow |M|$ iniettiva con $\forall b \in |M| (\varphi(b) \leftrightarrow \exists j g(j) = b)$.

Usiamo g per copiare $\{b \in |M| \mid \varphi(b)\}$ su \mathbb{N} e ottenere \tilde{K} :

$$|\tilde{K}| = \mathbb{N}, 0_{\tilde{K}} = g^{-1}(0_M), \dots, i +_{\tilde{K}} j = g^{-1}(g(i) +_M g(j)), \dots$$

$h = g^{-1} \circ k : K \rightarrow \tilde{K}$ è il monomorfismo richiesto. \square

RCA_0 **non dimostra** l'unicità della chiusura algebrica.

Comprensione aritmetica

Il sistema
 ACA_0

Analisi

Algebra

Combinatorica

① Il sistema ACA_0

② Analisi

③ Algebra

④ Combinatorica

ACA₀

Ricordiamo che le formule aritmetiche sono quelle senza quantificatori sui variabili insiemistiche.

Possono però contenere variabili insiemistiche libere.

Gli assiomi di ACA₀ sono quelli di RCA₀ più lo schema di comprensione aritmetica:

se φ è aritmetica e X non è libera in φ

$$\exists X \forall n (n \in X \leftrightarrow \varphi(n))$$

In presenza di questo schema, la Σ_1^0 -induzione può essere sostituita dall'assioma di induzione.

ACA abbrevia Arithmetic Comprehension Axiom.


Una utile riformulazione

Teorema (RCA_0)

Sono equivalenti:

- 1 ACA_0 ;
- 2 Σ_1^0 -comprensione;
- 3 per tutte le funzioni iniettive $f : \mathbb{N} \rightarrow \mathbb{N}$ esiste $X \subseteq \mathbb{N}$ tale che $\forall n (n \in X \leftrightarrow \exists m f(m) = n)$.

Dimostrazione.

$1 \rightarrow 2$ e $2 \rightarrow 3$ sono immediate. $3 \rightarrow 2$ per un lemma .

$2 \rightarrow 1$ Ogni formula aritmetica è Σ_k^0 per qualche $k \in \omega$ e basta dimostrare per induzione (metateorica) Σ_k^0 -comprensione.

Se $k \leq 1$ non c'è nulla da dimostrare.

Se $\varphi(n)$ è Σ_{k+1}^0 è della forma $\exists j \psi(n, j)$ con $\psi \Pi_k^0$.

Per ipotesi induttiva esiste $Y = \{ (n, j) \mid \neg \psi(n, j) \}$.

Per Σ_1^0 -comp $X = \{ n \mid \exists j (n, j) \notin Y \}$ esiste. □

ω -modelli di ACA_0

Il sistema
 ACA_0

Gli assiomi
 ω -modelli

Analisi

Algebra

Combinatorica

Teorema

$S \subseteq \mathcal{P}(\omega)$ è un ω -modello di ACA_0 se e solo se S è un ideale di Turing chiuso sotto jump, cioè

- $S \neq \emptyset$;
- se $X, Y \in S$ allora
 $X \oplus Y = \{2n \mid n \in X\} \cup \{2n+1 \mid n \in Y\} \in S$;
- se $X \in S$ e $Y \leq_T X$ allora $Y \in S$;
- se $X \in S$ allora $X' \in S$.

In particolare $\mathbf{ARITH} = \{X \subseteq \omega \mid \exists n X \leq_T \emptyset^{(n)}\}$
è il più piccolo ω -modello di ACA_0 .

Completezza sequenziale di \mathbb{R} in ACA_0

Teorema (ACA_0)

Se $\langle x_n : n \in \mathbb{N} \rangle$ è una successione limitata di reali allora esiste $y = \sup\{x_n \mid n \in \mathbb{N}\}$.

Dimostrazione.

Possiamo assumere $0 \leq x_n \leq 1$ per ogni n .

Sia $f(k)$ il massimo $i < 2^k$ tale che $\exists n i \cdot 2^{-k} \leq x_n$.

f esiste per comprensione aritmetica.

$y = \langle f(k) \cdot 2^{-k} : k \in \mathbb{N} \rangle$ è un reale e

$\forall n x_n \leq y, \forall z < y \exists n z < x_n$.

In altre parole $y = \sup\{x_n \mid n \in \mathbb{N}\}$. □

Il teorema di Bolzano-Weierstrass in ACA_0

Teorema (ACA_0)

Ogni successione limitata di reali ha una sottosuccessione convergente.

Dimostrazione.

Sia $\langle x_n : n \in \mathbb{N} \rangle$ limitata e assumiamo $0 \leq x_n \leq 1$ per ogni n .
Sia $f(k)$ il massimo $i < 2^k$ tale che $\forall m \exists n > m \ i \cdot 2^{-k} \leq x_n$.
 f esiste per compressione aritmetica.

$y = \langle f(k) \cdot 2^{-k} : k \in \mathbb{N} \rangle$ è un reale e

$$\forall \varepsilon > 0 \forall m \exists n > m \ |y - x_n| < \varepsilon.$$

Poniamo $n_0 = 0$, $n_{k+1} = \min\{n > n_k \mid |y - x_n| < 2^{-k}\}$.

E' chiaro che $y = \lim x_{n_k}$. □

Il primo teorema di reverse mathematics

Teorema (RCA_0)

Sono equivalenti:

- 1 ACA_0 ;
- 2 ogni successione limitata di reali ha una sottosuccessione convergente;
- 3 ogni successione di Cauchy di reali converge;
- 4 ogni successione limitata di reali ha estremo superiore;
- 5 ogni successione limitata e crescente di reali converge.

$\langle x_n : n \in \mathbb{N} \rangle$ è di Cauchy se $\forall \varepsilon > 0 \exists m \forall n > m |x_n - x_m| < \varepsilon$.

1 \rightarrow 2 e 1 \rightarrow 4 già dimostrati. 2 \rightarrow 3 e 4 \rightarrow 5 immediati.

3 \rightarrow 5 perché una successione limitata e crescente è di Cauchy.

Resta da dimostrare il reversal 5 \rightarrow 1.

Il primo reversal

Il sistema
 ACA_0

Analisi
I reali
Spazi metrici
completi

Algebra

Combinatorica

Mostriamo in RCA_0 che se ogni successione limitata e crescente di reali converge, allora **vale ACA_0 . l'immagine di una funzione iniettiva è un insieme.**

Sia $f : \mathbb{N} \rightarrow \mathbb{N}$ iniettiva e poniamo $x_n = \sum_{i \leq n} 2^{-f(i)}$.
 $\langle x_n : n \in \mathbb{N} \rangle$ è crescente e limitata da 2 e per ipotesi converge a $x = \sum_i 2^{-f(i)}$.
Per ogni j vale

$$\exists i f(i) = j \leftrightarrow \forall n (|x - x_n| < 2^{-j} \rightarrow \exists i < n f(i) = j)$$

e quindi l'immagine di f esiste per Δ_1^0 -comprensione.

Generalizzazione agli spazi metrici completi

Definizione (RCA_0)

Uno spazio metrico completo \hat{A} è **compatto** se esiste una succ infinita di succ finite $\langle \langle x_{ij} : i \leq n_j \rangle : j \in \mathbb{N} \rangle$ con $x_{ij} \in \hat{A}$ tale che $\forall x \in \hat{A} \forall j \exists i \leq n_j d(x, x_{ij}) < 2^{-j}$.

Teorema (RCA_0)

Sono equivalenti:

- 1 ACA_0 ;
- 2 *negli spazi metrici compatti ogni successione ha una sottosuccessione convergente;*
- 3 *negli spazi metrici completi ogni succ di Cauchy converge.*

1 \rightarrow 2 e 1 \rightarrow 3: generalizzare gli argomenti per \mathbb{R}
(in cui $x_{ij} = i \cdot 2^{-j}$ per $i \leq 2^j$).

2 \rightarrow 1 e 3 \rightarrow 1 seguono dal reversal fatto.

Il lemma di Ascoli-Arzelà

Il sistema
 ACA_0

Analisi
I reali
Spazi metrici
completi

Algebra

Combinatorica

Teorema (RCA_0)

Sono equivalenti:

- 1 ACA_0 ;
- 2 se \hat{A} e \hat{B} sono spazi metrici compatti, ogni successione equicontinua di funzioni continue $f_n : \hat{A} \rightarrow \hat{B}$ ha una sottosuccessione uniformemente convergente.

$2 \rightarrow 1$ è immediato perché il lemma di Ascoli-Arzelà implica che ogni successione limitata di reali ha una sottosuccessione convergente.

Elementi di torsione

Il sistema
 ACA_0

Analisi

Algebra

Gruppi

Spazi vettoriali
Anelli

Combinatorica

Definizione (RCA_0)

Un **gruppo abeliano** $(|G|, 0_G, +_G, -_G)$ consiste di $|G| \subseteq \mathbb{N}$, $0_G \in |G|$, un'operazione binaria $+_G$ e un'operazione unaria $-_G$ che soddisfano gli usuali assiomi.

Per ricorsione primitiva definiamo ng per $n \in \mathbb{N}$ e $g \in |G|$.

D'ora in poi scriviamo G per $|G|$ e omettiamo i pedici $_G$.

Definizione (RCA_0)

$g \in G$ è un elemento di torsione se $\exists n > 0 (ng = 0)$.

Reverse mathematics per gli elementi di torsione

Il sistema

ACA_0

Analisi

Algebra

Gruppi

Spazi vettoriali

Anelli

Combinatoria

Teorema (RCA_0)

Sono equivalenti:

- 1 ACA_0 ;
- 2 ogni gruppo abeliano ha un sottogruppo che consiste dei suoi elementi di torsione.

1 \rightarrow 2 è immediato per definizione:

$$T = \{ g \in G \mid \exists n > 0 (ng = 0) \}.$$

2 \rightarrow 1 è il reversal.

Il reversal

Mostriamo in RCA_0 che se ogni gruppo abeliano ha un sottogruppo che consiste dei suoi elementi di torsione allora l'immagine di una funzione iniettiva f è un insieme.

G è il gruppo abeliano con generatori $\langle x_n : n \in \mathbb{N} \rangle$ e relazioni $(2m + 1)x_{f(m)} = 0$.

G è realizzato in RCA_0 come

$$\left\{ \sum_{n < k} \ell_n x_n \mid k \in \mathbb{N} \wedge \forall n < k (\ell_n \in \mathbb{Z} \wedge \forall m < |\ell_n| f(m) \neq n) \right\}$$

con le operazioni naturali.

Sia $T \subseteq G$ il sottogruppo degli elementi di torsione.

Per ogni n si ha $\exists m f(m) = n \leftrightarrow x_n \in T$.

Basi in spazi vettoriali

Il sistema
ACA₀

Analisi

Algebra

Gruppi

Spazi vettoriali

Anelli

Combinatoria

Definizione (RCA₀)

Sia K un campo. Uno **spazio vettoriale V su K** è un gruppo abeliano $(|V|, 0_V, +_V, -_V)$ con un'ulteriore funzione $\cdot_V : |K| \times |V| \rightarrow |V|$ che soddisfa gli usuali assiomi per il prodotto scalare.

Una **base per V** è un insieme $B \subseteq |V|$ tale che ogni $v \in |V|$ si scrive in modo unico come $\sum_{b \in B_0} a_b \cdot_V b$ dove $B_0 \subseteq B$ è finito e $0_K \neq a_b \in |K|$ per ogni $b \in B_0$.

D'ora in poi scriviamo V per $|V|$ e omettiamo i pedici $_V$.

Esistenza di basi in ACA_0

Il sistema
 ACA_0

Analisi

Algebra

Gruppi
Spazi vettoriali
Anelli

Combinatorica

Teorema (ACA_0)

Ogni spazio vettoriale V su un campo K ha una base.

Dimostrazione.

Sia $S = \{ \langle v_0, \dots, v_n \rangle \mid \exists \langle a_0, \dots, a_{n-1} \rangle (v_n = \sum_{i < n} a_i \cdot v_i) \}$.

Per ricorsione primitiva sia

$$b_n = \min \{ v \in V \mid \langle b_0, \dots, b_{n-1}, v \rangle \notin S \}.$$

[La ricorsione può fermarsi dopo un numero finito di passi]

$B = \{ b_0, b_1, \dots \}$ è una base per V . □

Reverse mathematics per l'esistenza di basi

Il sistema
 ACA_0

Analisi

Algebra

Gruppi
Spazi vettoriali
Anelli

Combinatoria

Teorema (RCA_0)

Sono equivalenti:

- 1 ACA_0 ;
- 2 ogni spazio vettoriale ha una base;
- 3 ogni spazio vettoriale su \mathbb{Q} ha una base.

1 \rightarrow 2 appena dimostrato.

2 \rightarrow 3 ovvio.

3 \rightarrow 1 è il reversal.

Il reversal

Mostriamo in RCA_0 che se ogni spazio vett su \mathbb{Q} ha una base allora l'immagine di una funzione iniettiva f è un insieme.

Sia V_0 l'insieme delle somme formali $\sum_{i \in I} q_i \cdot x_i$ dove $I \subset \mathbb{N}$ è finito e $q_i \in \mathbb{Q} \setminus \{0\}$.

V_0 è uno spazio vett su \mathbb{Q} con base $X = \{x_n \mid n \in \mathbb{N}\}$.

Siano $u_m = x_{2f(m)} + m \cdot x_{2f(m)+1}$ per ogni m e V_1 il sottospazio generato da $U = \{u_m \mid m \in \mathbb{N}\}$.

V_1 ha una definizione Σ_1^0 e inoltre

$$\sum_{i \in I} q_i \cdot x_i \in V_1 \leftrightarrow \forall n (q_{2n} \neq 0 \rightarrow f(q_{2n+1}/q_{2n}) = n).$$

$$V = V_0/V_1 = \{v \in V_0 \mid \forall w < v (w \in V_0 \rightarrow v - w \notin V_1)\}$$

V è spazio vettoriale su \mathbb{Q} e ha una base B .

$U \cup B$ è base per V_0 .

Per ogni n , $\exists m f(m) = n$ se e solo se

in almeno una delle scritture di x_{2n} e x_{2n+1} come combinazione lineare di elementi di $U \cup B$ compare u_m con $f(m) = n$. Π_1^0

Un rafforzamento

Definizione (RCA₀)

Uno spazio vettoriale V su K ha **dimensione finita** se ha una base finita.

$Y \subseteq V$ è **linearmente indipendente** se $\sum_{i=0}^k a_i \cdot y_i \neq 0$ quando $y_0, \dots, y_k \in Y$ sono distinti e $a_0, \dots, a_k \neq 0$.

Teorema (RCA₀)

Sono equivalenti:

- 1 ACA₀;
- 2 ogni spazio vettoriale su \mathbb{Q} ha dimensione finita oppure contiene un insieme infinito linearmente indipendente.

1 \rightarrow 2 segue da quanto visto.

2 \rightarrow 1 richiede più lavoro.

Ideali in anelli

Definizione (RCA_0)

Un **anello** (commutativo) $(|A|, 0_A, 1_A, +_A, -_A, \cdot_A)$ consiste di $|A| \subseteq \mathbb{N}$, $0_A \neq 1_A \in |A|$, operazioni binarie $+_A$ e \cdot_A , un'operazione unaria $-_A$ che soddisfano gli usuali assiomi.

Un **dominio d'integrità** è un anello tale che

$$\forall a, b \in |A| (a \cdot_A b = 0_A \rightarrow a = 0_A \vee b = 0_A).$$

D'ora in poi scriviamo A per $|A|$ e omettiamo i pedici $_A$.

Definizione (RCA_0)

Un **ideale di A** è un insieme $I \subseteq |A|$ tale che $0 \in I$, $1 \notin I$,

$$\forall a, b \in I \ a + b \in I \text{ e } \forall a \in I \ \forall b \in A \ a \cdot b \in I.$$

Un **ideale massimale di A** è un ideale M tale che

$$\forall a \in A \setminus M \ \exists b \in A (a \cdot b - 1 \in M).$$

Un **ideale primo di A** è un ideale P tale che

$$\forall a, b \in A (a \cdot b \in P \rightarrow a \in P \vee b \in P).$$

Esistenza di ideali massimali in ACA_0

RCA_0 dimostra che ogni ideale massimale è primo.

Teorema (ACA_0)

Ogni anello A ha un ideale massimale.

Dimostrazione.

Diciamo che $X \subseteq A$ è *buono* se $\sum_{i < n} a_i \cdot x_i \neq 1$ quando $\forall i < n (x_i \in X \wedge a_i \in A)$.

Π_1^0

Sia $\langle a_n : n \in \mathbb{N} \rangle$ un'enumerazione di A .

Per ricorsione primitiva definiamo $f : \mathbb{N} \rightarrow \{0, 1\}$:

$$f(n) = \begin{cases} 1 & \text{se } \{a_m \mid m < n \wedge f(m) = 1\} \cup \{a_n\} \text{ è buono;} \\ 0 & \text{altrimenti.} \end{cases}$$

$M = \{a_m \mid f(m) = 1\}$ è un ideale massimale in A . □

Reverse mathematics per l'esistenza di ideali massimali

Il sistema
 ACA_0

Analisi

Algebra

Gruppi
Spazi vettoriali
Anelli

Combinatorica

Teorema (RCA_0)

Sono equivalenti:

- 1 ACA_0 ;
- 2 ogni anello ha un ideale massimale;
- 3 ogni dominio d'integrità ha un ideale massimale.

1 \rightarrow 2 appena dimostrato.

2 \rightarrow 3 ovvio.

3 \rightarrow 1 è il reversal.

Il reversal

Mostriamo in RCA_0 che se ogni dominio d'integrità ha un ideale massimale allora l'immagine di una funzione iniettiva f è un insieme.

$A_0 = \mathbb{Q}[\langle x_n \rangle]$ è l'anello dei polinomi su \mathbb{Q} con infinite variabili.

$K_0 = \mathbb{Q}(\langle x_n \rangle)$ è il campo delle frazioni di A_0 .

Sia $\varphi(b)$ la formula Σ_1^0

$b \in K_0 \wedge$ il denom contiene un monomio $qx_{f(m_1)}^{e_1} \cdots x_{f(m_k)}^{e_k}$.

$\{b \in K_0 \mid \varphi(b)\} \supseteq A_0$, se esistesse (cosa che RCA_0 non garantisce), sarebbe un dominio d'integrità.

Esiste invece $h : \mathbb{N} \rightarrow K_0$ iniettiva con $\varphi(b) \leftrightarrow \exists m h(m) = b$.

Definiamo su \mathbb{N} le operazioni di un dominio d'integrità A in modo che h sia un monomorfismo.

Sia M un ideale massimale in A .

Mostreremo che per ogni n

$$\exists m f(m) = n \leftrightarrow h^{-1}(x_n) \notin M.$$

Verifica di $\exists m f(m) = n \leftrightarrow h^{-1}(x_n) \notin M$

\Rightarrow Se $f(m) = n$ allora vale $\varphi(1/x_n)$

e perciò $h^{-1}(1/x_n)$ è l'inverso di $h^{-1}(x_n)$ in A .

Quindi $h^{-1}(x_n)$ non appartiene a nessun ideale e $h^{-1}(x_n) \notin M$.

\Leftarrow Se $h^{-1}(x_n) \notin M$ per massimalità di M

esistono $b \in A$ e $c \in M$ tali che $h^{-1}(x_n) \cdot b - 1 = c$.

c non è invertibile in A e se $h(c) = r/s$ con $r, s \in A_0$, $s \neq 0$,

r non può contenere monomi della forma $qx_{f(m_1)}^{e_1} \cdots x_{f(m_k)}^{e_k}$,

mentre s ne contiene almeno uno.

$x_n \cdot h(b) - 1 = r/s$ implica $x_n \cdot h(b) \cdot s = s + r$.

Dato che $s + r$ contiene un monomio della forma

$qx_{f(m_1)}^{e_1} \cdots x_{f(m_k)}^{e_k}$ deve essere $n = f(m)$ per qualche m .

Alberi finitamente generati

Definizione (RCA_0)

Un **albero** è un insieme $T \subseteq \mathbb{N}^{<\mathbb{N}}$ tale che

$$\forall \sigma \in T \forall \tau \subseteq \sigma \tau \in T.$$

Un **cammino** in un albero T è una funzione $f : \mathbb{N} \rightarrow \mathbb{N}$ tale che

$$\forall n f[n] = \langle f(i) : i < n \rangle \in T.$$

L'albero T è **finitamente generato** se

$$\forall \sigma \in T \exists n \forall m (\sigma \frown \langle m \rangle \in T \rightarrow m < n).$$

Gli elementi di un albero sono chiamati nodi.

Un successore immediato di σ è una successione della forma $\sigma \frown \langle m \rangle$.

Il lemma di König è l'affermazione:

ogni albero infinito e finitamente generato ha un cammino.

Il lemma di König in ACA_0

Teorema (ACA_0)

Il lemma di König.

Dimostrazione.

Dato T albero infinito e finitamente generato sia

$$T^* = \{ \sigma \in T \mid \text{esistono infiniti } \tau \in T \text{ con } \sigma \subseteq \tau \}.$$

$\langle \rangle \in T^*$ perché T è infinito.

Se $\sigma \in T^*$ esiste m tale che $\sigma \hat{\ } \langle m \rangle \in T^*$

perché T è finitamente generato.

Per ricorsione primitiva sia

$$f(n) = \min \{ m \in \mathbb{N} \mid f[n] \hat{\ } \langle m \rangle \in T^* \}.$$

f è un cammino in T^* e quindi in T .



Reverse mathematics per il lemma di König

Il sistema
 ACA_0

Analisi

Algebra

Combinatoria

Il lemma di
König

Il teorema di
Ramsey

Teorema (RCA_0)

Sono equivalenti:

- 1 ACA_0 ;
- 2 *il lemma di König*;
- 3 *il lemma di König per alberi in cui ogni nodo ha al più due successori immediati.*

1 \rightarrow 2 appena dimostrato.

2 \rightarrow 3 è ovvio.

3 \rightarrow 1 è il reversal.

Il reversal

Mostriamo in RCA_0 che il lemma di König implica che l'immagine di una funzione iniettiva f è un insieme.

Sia T l'insieme delle $\sigma \in \mathbb{N}^{<\mathbb{N}}$ tali che

- 1 $\forall m, n < |\sigma| (f(m) = n \leftrightarrow \sigma(n) = m + 1)$ e
- 2 $\forall n < |\sigma| (\sigma(n) > 0 \rightarrow f(\sigma(n) - 1) = n)$

$\sigma \in T$ con $|\sigma| = n$ ha al più due successori immediati in T : $\sigma \hat{\ } \langle 0 \rangle$ (che per essere in T richiede che $\forall m < n f(m) \neq n$) e $\sigma \hat{\ } \langle m + 1 \rangle$ per l'eventuale unico m tale che $f(m) = n$.

Dato k definiamo $\sigma \in T$ con $|\sigma| = k$:

$$\sigma(n) = \begin{cases} 0 & \text{se } \neg \exists m < k f(m) = n; \\ m + 1 & \text{se } m < k \text{ e } f(m) = n. \end{cases}$$

Quindi T è infinito.

Per il lemma di König sia g un cammino in T .

Per ogni n si ha $\exists m f(m) = n \leftrightarrow g(n) > 0$.

Colorazioni di insiemi finiti

Definizione (RCA_0)

Se $X \subseteq \mathbb{N}$ sia $[X]^k$ l'insieme delle successioni $\sigma \in \mathbb{N}^{<\mathbb{N}}$ tali che
 $|\sigma| = k \wedge \forall i < k (\sigma(i) \in X \wedge \forall j < i \sigma(j) < \sigma(i))$.

Gli elementi di $[X]^k$ sono identificati con i sottoinsiemi di X con k elementi.

Una ℓ -colorazione di $[X]^k$ è una $f : [X]^k \rightarrow \{0, \dots, \ell - 1\}$.

Spesso scriveremo $f(n_1, \dots, n_k)$ al posto di $f(\langle n_1, \dots, n_k \rangle)$, sottintendendo $n_1 < \dots < n_k$.

Se f è una ℓ -colorazione di $[X]^k$, $Y \subseteq X$ è **omogeneo per f** se Y è infinito e $\exists i < \ell \forall \sigma \in [Y]^k f(\sigma) = i$.

Il teorema di Ramsey per esponente k e ℓ colori (RT_ℓ^k) è:
ogni ℓ -colorazione di $[\mathbb{N}]^k$ ha un insieme omogeneo.

Il teorema di Ramsey per esponente k (RT^k) è $\forall \ell \text{RT}_\ell^k$.

Il teorema di Ramsey in ACA_0

Il sistema
 ACA_0

Analisi

Algebra

Combinatorica

Il lemma di
König

Il teorema di
Ramsey

Teorema (ACA_0)

RT^0 e $\forall k(RT^k \rightarrow RT^{k+1})$.

RT^0 è banale.

$\forall k(RT^k \rightarrow RT^{k+1})$ verrà mostrato tra poco.

Notiamo che non abbiamo la Π_2^1 -induzione necessaria per concludere dal teorema che ACA_0 dimostra $\forall k RT^k$.

Il teorema implica che per ogni $k \in \omega$, ACA_0 dimostra RT^k .

L'albero di Erdős-Radó

Per mostrare che RT^k implica RT^{k+1} fissiamo una ℓ -colorazione f di $[\mathbb{N}]^{k+1}$.

T è l'insieme dei $\sigma \in \mathbb{N}^{<\mathbb{N}}$ tali che per ogni $n < |\sigma|$, $\sigma(n)$ è il minimo j tale che

- 1 $\forall m < n \sigma(m) < j$;
- 2 $f(\sigma(m_1), \dots, \sigma(m_k), \sigma(m)) = f(\sigma(m_1), \dots, \sigma(m_k), j)$
per ogni $m_1 < m_2 < \dots < m_k < m \leq n$.

T esiste per Σ_0^0 -comprensione.

T è finitamente generato perché $\sigma \in T$ ha al più $\ell^{|\sigma|^k}$ successori immediati in T .

T è infinito perché per ogni j , $\exists \tau \in T \exists n < |\tau| \tau(n) = j$. Infatti se σ è massimale nell'insieme delle successioni che soddisfano 1 e 2 (almeno $\langle \rangle$ le soddisfa), $\sigma \hat{\langle j \rangle} \in T$.

Per il lemma di König esiste un cammino g in T .

Conclusione della dimostrazione di

$$RT^k \rightarrow RT^{k+1}$$

T è l'insieme dei $\sigma \in \mathbb{N}^{<\mathbb{N}}$ tali che per ogni $n < |\sigma|$, $\sigma(n)$ è il minimo j tale che

- 1 $\forall m < n \sigma(m) < j$;
- 2 $f(\sigma(m_1), \dots, \sigma(m_k), \sigma(m)) = f(\sigma(m_1), \dots, \sigma(m_k), j)$
per ogni $m_1 < m_2 < \dots < m_k < m \leq n$.

g cammino in T .

g è strettamente crescente per 1.

Definiamo $f' : [\mathbb{N}]^k \rightarrow \{0, \dots, \ell - 1\}$ ponendo

$$f'(m_1, \dots, m_k) = f(g(m_1), \dots, g(m_k), g(m))$$

(per 2 il valore non dipende dalla scelta di $m > m_k$).

Per RT^k esiste X' omogeneo per f' .

$X = \{g(m) \mid m \in X'\}$ è omogeneo per f .

Reversal per il teorema di Ramsey

Teorema (RCA_0)

RT^3 implica ACA_0 .

Dimostrazione.

Sia $f : \mathbb{N} \rightarrow \mathbb{N}$ una funzione iniettiva.

Definiamo $g : [\mathbb{N}]^3 \rightarrow \{0, 1\}$ ponendo $g(a, b, c) = 1$ se e solo se

$$\forall n < a (\exists m < b f(m) = n \leftrightarrow \exists m < c f(m) = n).$$

Per RT^3 esiste X omogeneo per g di colore $i < 2$. **Quale?**

Se $a \in X$ sia $Y = \{n < a \mid \exists m f(m) = n\}$.

Se j è tale che $\forall n \in Y \exists m \leq j f(m) = n$ siano $b, c \in X$ con $\max(j, a) < b < c$.

Allora $g(a, b, c) = 1$ e quindi $i = 1$.

Per ogni n si ha $\exists m f(m) = n$ se e solo se

$\forall a, b \in X (n < a < b \rightarrow \exists m < b f(m) = n)$. □

RT³ e RT²

Per quanto visto ACA_0 è equivalente a RT^k per qualsiasi $k \in \omega$ con $k \geq 3$.

RT^2 invece non implica ACA_0 e la sua classificazione è ancora incompleta.

Si sa che WKL_0 non dimostra RT^2 , ma non si sa se RT^2 implica WKL_0 .

Si sa anche che RT^2 è strettamente più forte di RT^2_ℓ per qualunque $\ell \in \omega$ fissato.

[La dimostrazione vista mostra invece che RT^3_2 implica ACA_0 ed è quindi equivalente a RT^3]

Un principio di compattezza

Il sistema
 WKL_0

Analisi

Logica

Algebra

① Il sistema WKL_0

② Analisi

③ Logica

④ Algebra

WKL₀

Il sistema
WKL₀
Gli assiomi
 ω -modelli

Analisi

Logica

Algebra

L'assioma principale di WKL₀ è una forma debole del lemma di König, che ieri abbiamo dimostrato in ACA₀.

Sia $2^{<\mathbb{N}} = \{ \sigma \in \mathbb{N}^{<\mathbb{N}} \mid \forall i < |\sigma| \sigma(i) < 2 \}$.

Gli assiomi di WKL₀ sono quelli di RCA₀ più il lemma di König debole:

ogni albero infinito contenuto in $2^{<\mathbb{N}}$ ha un cammino

WKL abbrevia Weak König Lemma.

ACA₀ implica WKL₀, che a sua volta implica RCA₀.

Perché il lemma di König debole è un principio di compattezza?

Lo spazio di Cantor $2^{\mathbb{N}}$ è l'insieme delle funzioni $f : \mathbb{N} \rightarrow \{0, 1\}$ con la topologia generata dagli aperti di base della forma $N_\sigma = \{f \mid \sigma \subset f\}$ per $\sigma \in 2^{<\mathbb{N}}$.

Se un albero $T \subseteq 2^{<\mathbb{N}}$ non ha cammini $\{\sigma \mid \sigma \in T\}$ è un ricoprimento aperto di $2^{\mathbb{N}}$.

Il lemma di König debole afferma che un tale albero è finito, cioè che il ricoprimento aperto sopra ha il sottoricoprimento finito $\{\sigma \in T \mid \forall n < |\sigma|, \sigma \upharpoonright n \in T\}$.

Il lemma di König debole afferma quindi la compattezza dello spazio di Cantor.

Vedremo che WKL_0 è equivalente alla compattezza nel senso dei ricoprimenti di diversi spazi metrici completi, ed anche al teorema di compattezza della logica.

Il lemma di König limitato

Un albero $T \subseteq \mathbb{N}^{<\mathbb{N}}$ si dice **limitato** se esiste una funzione $f : \mathbb{N} \rightarrow \mathbb{N}$ tale che $\forall \sigma \in T \forall i < |\sigma| \sigma(i) < f(i)$.

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 *il lemma di König limitato: ogni albero infinito e limitato ha un cammino.*

$2 \rightarrow 1$ perché gli alberi contenuti in $2^{<\mathbb{N}}$ sono limitati dalla funzione costante 2.

Per $1 \rightarrow 2$ trasformeremo ogni albero limitato in un albero contenuto in $2^{<\mathbb{N}}$.

WKL₀ dimostra il lemma di König limitato

Sia $T \subseteq \mathbb{N}^{<\mathbb{N}}$ un albero infinito limitato da f .

Vogliamo trovare un cammino in T .

Per ogni $\sigma \in T$ definiamo $\sigma^* \in 2^{<\mathbb{N}}$ con $|\sigma^*| = \sum_{i < |\sigma|} f(i)$:
dato $n < \sum_{i < |\sigma|} f(i)$ siano $j_n < |\sigma|$ e $k_n < f(i_n)$ tali che
 $n = \sum_{i < j_n} f(i) + k_n$ e poniamo

$$\sigma^*(n) = \begin{cases} 0 & \text{se } k_n < \sigma(j_n); \\ 1 & \text{se } \sigma(j_n) \leq k_n. \end{cases}$$

$T^* = \{ \rho \in 2^{<\mathbb{N}} \mid \exists \sigma \in T \rho \subseteq \sigma^* \}$ esiste per Δ_1^0 -comprensione
(si può restringere il quantificatore ai $\sigma \in T$ con
 $|\sigma| = \min\{ j \mid |\rho| \leq \sum_{i < j} f(i) \}$) ed è un albero infinito.

Per WKL₀ esiste un cammino g^* in T^* .

Poniamo $g(j) = \min\{ k \mid g^*(\sum_{i < j} f(i) + k) = 1 \}$.
 g è un cammino in T .

Σ_1^0 -separazione

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 Σ_1^0 -separazione: se $\varphi_0(n)$ e $\varphi_1(n)$ sono formule Σ_1^0 in cui X non è libera e per cui vale $\neg \exists n (\varphi_0(n) \wedge \varphi_1(n))$ allora $\exists X \forall n ((\varphi_0(n) \rightarrow n \in X) \wedge (\varphi_1(n) \rightarrow n \notin X))$;
- 3 se $f_0, f_1 : \mathbb{N} \rightarrow \mathbb{N}$ sono funzioni iniettive tali che $\forall m_0 \forall m_1 f_0(m_0) \neq f_1(m_1)$ allora esiste $X \subseteq \mathbb{N}$ tale che $\forall n ((\exists m f_0(m) = n \rightarrow n \in X) \wedge (\exists m f_1(m) = n \rightarrow n \notin X))$.

2 \rightarrow 3 è immediato.

3 \rightarrow 2 per un lemma.

Resta da mostrare $1 \leftrightarrow 2$.

WKL₀ implica Σ_1^0 -separazione

Il sistema
WKL₀
Gli assiomi
 ω -modelli

Analisi

Logica

Algebra

Siano $\varphi_0(n) \equiv \exists m \theta_0(m, n)$ e $\varphi_1(n) \equiv \exists m \theta_1(m, n)$ con $\theta_i \in \Sigma_0^0$ e valga $\neg \exists n (\varphi_0(n) \wedge \varphi_1(n))$.

$T = \{ \sigma \in 2^{<\mathbb{N}} \mid \forall i < 2 \forall m, n < |\sigma| (\theta_i(m, n) \rightarrow \sigma(n) = i) \}$
esiste per Σ_0^0 -comprensione ed è un albero.

T è infinito perché per ogni k esiste $\sigma \in T$ con $|\sigma| = k$.

Per il lemma di König debole esiste un cammino f in T .

Definiamo $X = \{ n \mid f(n) = 0 \}$.

Allora $\forall n ((\varphi_0(n) \rightarrow n \in X) \wedge (\varphi_1(n) \rightarrow n \notin X))$.

Σ_1^0 -separazione implica WKL_0

Sia $T \subseteq 2^{<\mathbb{N}}$ un albero infinito.

$\theta(n, \sigma) \leftrightarrow \exists \tau \in 2^{<\mathbb{N}} (\tau \in T \wedge |\tau| = n \wedge \sigma \subseteq \tau)$ è Σ_0^0 .

$\varphi(\sigma, i) \leftrightarrow \exists n (\theta(n, \sigma \widehat{\langle i \rangle}) \wedge \neg \theta(n, \sigma \widehat{\langle 1-i \rangle}))$ è Σ_1^0 .

Vale $\neg \exists \sigma (\varphi(\sigma, 0) \wedge \varphi(\sigma, 1))$ e per Σ_1^0 -separazione esiste X con $\forall \sigma ((\varphi(\sigma, 0) \rightarrow \sigma \in X) \wedge (\varphi(\sigma, 1) \rightarrow \sigma \notin X))$.

Definiamo per ricorsione primitiva $\langle \sigma_k : k \in \mathbb{N} \rangle$ con $|\sigma_k| = k$:

$$\sigma_0 = \langle \rangle; \quad \sigma_{k+1} = \begin{cases} \sigma_k \widehat{\langle 0 \rangle} & \text{se } \sigma_k \in X; \\ \sigma_k \widehat{\langle 1 \rangle} & \text{se } \sigma_k \notin X. \end{cases}$$

Fissato n , mostriamo per induzione $\forall k \leq n \theta(n, \sigma_k)$.

In particolare $\theta(n, \sigma_n)$, cioè $\sigma_n \in T$.

Allora $f = \bigcup_k \sigma_k$ (cioè la funzione definita da $f(n) = \sigma_{n+1}(n)$) è un cammino in T .

ω -modelli di WKL_0

Il sistema
 WKL_0

Gli assiomi
 ω -modelli

Analisi

Logica

Algebra

Esistono insiemi computabilmente enumerabili disgiunti che sono computabilmente inseparabili. Perciò **REC** non soddisfa Σ_1^0 -separazione e non è un modello di WKL_0 .

Quindi WKL_0 è strettamente più forte di RCA_0 .

Si possono costruire ω -modelli di WKL_0 i cui elementi sono tutti low (X è low se $X' \equiv_T \emptyset'$). Questi ω -modelli non sono chiusi sotto jump e non soddisfano ACA_0 .

Quindi WKL_0 è strettamente più debole di ACA_0 .

Non esiste il più piccolo ω -modello di WKL_0 .

REC è l'intersezione di tutti gli ω -modelli di WKL_0 .

Compattezza di $[0, 1]$ in WKL_0

Il teorema di Heine-Borel afferma che ogni ricoprimento aperto di $[0, 1]$ ha un sottoricoprimento finito.

Se $x, y, z \in \mathbb{R}$ scriviamo $x \in [y, z]$ per $y \leq x \leq z$
e $x \in (y, z)$ per $y < x < z$.

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 se $\langle c_i : i \in \mathbb{N} \rangle, \langle d_i : i \in \mathbb{N} \rangle$ sono successioni in \mathbb{R} tali che
$$\forall x \in [0, 1] \exists i x \in (c_i, d_i),$$

allora esiste n tale che
$$\forall x \in [0, 1] \exists i \leq n x \in (c_i, d_i).$$

Dimostreremo $1 \rightarrow 2$ in due passi, considerando dapprima il caso in cui $c_i, d_i \in \mathbb{Q}$.

Per dimostrare $2 \rightarrow 1$ useremo l'insieme di Cantor.

WKL₀ dimostra il teorema di Heine-Borel per intervalli a estremi razionali

Supponiamo che $\langle c_i : i \in \mathbb{N} \rangle$, $\langle d_i : i \in \mathbb{N} \rangle$ siano successioni in \mathbb{Q} tali che $\forall x \in [0, 1] \exists i x \in (c_i, d_i)$.

Se $\sigma \in 2^{<\mathbb{N}}$ siano $a_\sigma = \sum_{i < |\sigma|} \sigma(i) \cdot 2^{-i-1}$ e $b_\sigma = a_\sigma + 2^{-|\sigma|}$.

Per ogni n , $\{ [a_\sigma, b_\sigma] \mid \sigma \in 2^{<\mathbb{N}} \wedge |\sigma| = n \}$ è la divisione di $[0, 1]$ in 2^n intervalli di larghezza 2^{-n} .

$T = \{ \sigma \in 2^{<\mathbb{N}} \mid \neg \exists i < |\sigma| (c_i < a_\sigma < b_\sigma < d_i) \}$ esiste per Σ_0^0 -comprensione ed è un albero.

Fissato $f : \mathbb{N} \rightarrow \{0, 1\}$, $x = \sum_{i \in \mathbb{N}} f(i) \cdot 2^{-i-1}$ è l'unico reale tale che $\forall n x \in [a_{f[n]}, b_{f[n]}]$.

Se $c_i < x < d_i$ esiste n tale che $c_i < a_{f[n]} < b_{f[n]} < d_i$ e $f[n] \notin T$, cioè f non è un cammino in T .

Per WKL₀ T è finito, cioè esiste n tale che $\forall \sigma \in T \mid \sigma \mid < n$.

Allora $\forall \sigma (|\sigma| < n \rightarrow \exists i < |\sigma| (c_i < a_\sigma < b_\sigma < d_i))$
e quindi $\forall x \in [0, 1] \exists i \leq n x \in (c_i, d_i)$.

Il sistema
WKL₀

Analisi

I reali

Funzioni
continue

Equazioni
differenziali e
teoremi di punto
fisso

Logica

Algebra

WKL₀ dimostra il teorema di Heine-Borel

Se le successioni $\langle c_i : i \in \mathbb{N} \rangle$ e $\langle d_i : i \in \mathbb{N} \rangle$ degli estremi degli intervalli aperti sono reali anziché razionali, ci riconduciamo al caso precedente come segue.

Sia $\varphi(q, r) \leftrightarrow q, r \in \mathbb{Q} \wedge \exists i (c_i < q < r < d_i)$.

φ è Σ_1^0 ed esiste $f : \mathbb{N} \rightarrow \mathbb{Q} \times \mathbb{Q}$ tale che

$$\forall q, r (\varphi(q, r) \leftrightarrow \exists j f(j) = (q, r)).$$

Scrivendo $f(j) = (q_j, r_j)$ si ha $\forall x \in [0, 1] \exists j x \in (q_j, r_j)$.

Per quanto già dimostrato, esiste m tale che

$$\forall x \in [0, 1] \exists j \leq m x \in (q_j, r_j).$$

Dato che $c_i < q_j < r_j < d_i$ è Σ_1^0 esiste una funzione $g : \mathbb{N} \rightarrow \mathbb{N}$ tale che $\forall j (c_{g(j)} < q_j < r_j < d_{g(j)})$.

Allora se $n = \max\{g(j) \mid j \leq m\}$ si ha

$$\forall x \in [0, 1] \exists i \leq n x \in (c_i, d_i).$$

Una versione parallela di Heine-Borel

Il sistema
WKL₀

Analisi

I reali

Funzioni
continue

Equazioni
differenziali e
teoremi di punto
fisso

Logica

Algebra

Il teorema di Heine-Borel può essere generalizzato in modo da considerare simultaneamente infiniti ricoprimenti.

Teorema (WKL₀)

Se $\langle c_{ni} : n, i \in \mathbb{N} \rangle$ e $\langle d_{ni} : n, i \in \mathbb{N} \rangle$ sono successioni in \mathbb{R} tali che

$$\forall n \forall x \in [0, 1] \exists i x \in (c_{ni}, d_{ni}),$$

allora esiste $f : \mathbb{N} \rightarrow \mathbb{N}$ tale che

$$\forall n \forall x \in [0, 1] \exists i \leq f(n) x \in (c_{ni}, d_{ni}).$$

Si ripete la dimostrazione precedente “in parallelo” per ogni n .

L'insieme di Cantor

L'insieme di Cantor C consiste di tutti i reali della forma

$$\sum_{i \in \mathbb{N}} 2f(i) \cdot 3^{-i-1} \text{ per qualche } f : \mathbb{N} \rightarrow \{0, 1\}.$$

$C \subseteq [0, 1]$ è omeomorfo a $2^{\mathbb{N}}$ e identificheremo cammini in $2^{<\mathbb{N}}$ con elementi di C .

Se $\sigma \in 2^{<\mathbb{N}}$ siano $a_\sigma = \sum_{i < |\sigma|} 2\sigma(i) \cdot 3^{-i-1}$ e $b_\sigma = a_\sigma + 3^{-|\sigma|}$.
 $[a_{\sigma \frown \langle 0 \rangle}, b_{\sigma \frown \langle 0 \rangle}]$ è il terzo di sinistra di $[a_\sigma, b_\sigma]$.

Sia $x \in [0, 1]$:

- se $x \in C$ c'è un'unica $f : \mathbb{N} \rightarrow \{0, 1\}$ tale che $\forall n x \in [a_{f \upharpoonright n}, b_{f \upharpoonright n}]$;
- se $x \notin C$ c'è un'unica $\sigma \in 2^{<\mathbb{N}}$ tale che $x \in (b_{\sigma \frown \langle 0 \rangle}, a_{\sigma \frown \langle 1 \rangle})$.

Siano anche $a'_\sigma = a_\sigma - 3^{-|\sigma|-1}$ e $b'_\sigma = b_\sigma + 3^{-|\sigma|-1}$.

$(a'_\sigma, b'_\sigma) \cap (a'_\tau, b'_\tau) = \emptyset$ quando $\sigma \not\subseteq \tau$ e $\tau \not\subseteq \sigma$.

Il teorema di Heine-Borel implica WKL_0

Il sistema
 WKL_0

Analisi

I reali

Funzioni
continue

Equazioni
differenziali e
teoremi di punto
fisso

Logica

Algebra

Sia $T \subseteq 2^{<\mathbb{N}}$ un albero senza cammini: vogliamo mostrare che è finito.

Sia $T' = \{ \tau \in 2^{<\mathbb{N}} \mid \tau \notin T \wedge \forall n < |\tau| \tau[n] \in T \}$.

Se $\tau, \sigma \in T'$ con $\tau \neq \sigma$ allora $\sigma \not\subseteq \tau$ e $\tau \not\subseteq \sigma$.

$$\{ (a'_\tau, b'_\tau) \mid \tau \in T' \} \cup \{ (b_{\sigma \smallfrown \langle 0 \rangle}, a_{\sigma \smallfrown \langle 1 \rangle}) \mid \sigma \in 2^{<\mathbb{N}} \}$$

è un ricoprimento di $[0, 1]$.

Per il teorema di Heine-Borel esiste un sottoricoprimento finito e, dato che gli intervalli in $\{ (a'_\tau, b'_\tau) \mid \tau \in T' \}$ sono a due a due disgiunti, T' è finito.

Ma allora $T = \{ \tau[n] \mid \tau \in T' \wedge n < |\tau| \}$ è finito.

Generalizzazione agli spazi metrici completi

Il sistema
WKL₀

Analisi

I reali

Funzioni
continue

Equazioni
differenziali e
teoremi di punto
fisso

Logica

Algebra

Teorema (RCA₀)

Sono equivalenti:

- 1 WKL₀;
- 2 ogni ricoprimento di uno spazio metrico compatto ha un sottoricoprimento finito.

1 → 2: generalizzare gli argomenti usati per $[0, 1]$, utilizzando il lemma di König limitato.

2 → 1 segue dal reversal fatto.

Uniforme continuità

Il sistema
WKL₀

Analisi

I reali
Funzioni
continue

Equazioni
differenziali e
teoremi di punto
fisso

Logica

Algebra

Definizione (RCA₀)

Sia $\phi : [0, 1] \rightarrow \mathbb{R}$ una funzione continua.

ϕ è **uniformemente continua** se

$\forall \varepsilon > 0 \exists \delta > 0 \forall x, y \in [0, 1] (|x - y| < \delta \rightarrow |\phi(x) - \phi(y)| < \varepsilon).$

$h : \mathbb{N} \rightarrow \mathbb{N}$ è un **modulo di uniforme continuità** per ϕ se

$\forall n \forall x, y \in [0, 1] (|x - y| < 2^{-h(n)} \rightarrow |\phi(x) - \phi(y)| < 2^{-n}).$

Ovviamente se una funzione ha un modulo di uniforme continuità è uniformemente continua.

Esistenza di moduli di uniforme continuità

Teorema (WKL₀)

Ogni funzione continua $\phi : [0, 1] \rightarrow \mathbb{R}$ ha un modulo di uniforme continuità.

Dimostrazione.

Sia Φ un codice per ϕ . Definiamo

$\psi(n, q, r) \leftrightarrow q \in \mathbb{Q} \wedge r \in \mathbb{Q}^+ \wedge \exists s, t ((q, 2r)\Phi(s, t) \wedge t < 2^{-n-1})$.

ψ è Σ_1^0 e esiste $\langle (q_{ni}, r_{ni}) : n, i \in \mathbb{N} \rangle$ tale che per ogni n

$$\forall q, r (\psi(n, q, r) \leftrightarrow \exists i (q, r) = (q_{ni}, r_{ni})).$$

$\langle B(q_{ni}, r_{ni}) : i \in \mathbb{N} \rangle$ è un ricoprimento aperto per ogni n .

Per la versione parallela del teorema di Heine-Borel esiste

$f : \mathbb{N} \rightarrow \mathbb{N}$ tale che $\forall n \forall x \in [0, 1] \exists i \leq f(n) x \in B(q_{ni}, r_{ni})$.

$h(n) = \min\{j \mid \forall i \leq f(n) 2^{-j} < r_{ni}\}$ è un modulo di uniforme

continuità per ϕ . Infatti se $|x - y| < 2^{-h(n)}$ e $x \in B(q_{ni}, r_{ni})$

con $i \leq f(n)$, dato che $\psi(n, q_{ni}, r_{ni})$ esistono s e $t < 2^{-n-1}$

tali che $\phi(x), \phi(y) \in B(s, t)$, e quindi $|\phi(x) - \phi(y)| < 2^{-n}$. \square

Esistenza del massimo

Teorema (WKL₀)

Per ogni funzione continua $\phi : [0, 1] \rightarrow \mathbb{R}$ ha massimo, cioè esiste $x \in [0, 1]$ tale che $\forall x' \in [0, 1] \phi(x') \leq \phi(x)$.

Dimostrazione.

Useremo la costruzione della dimostrazione precedente.

Sia $y = \lim_n \max\{\phi(q_{ni}) \mid i \leq f(n)\}$. L'esistenza di y ed il fatto che $y = \sup\{\phi(x) \mid x \in [0, 1]\}$ si dimostrano in RCA₀.

Resta da mostrare che $\exists x \phi(x) = y$.

Sia $\psi(q, r, s, t) \leftrightarrow (q, r) \Phi(s, t) \wedge s + t < y$.

ψ è Σ_1^0 e esiste $\langle (q_i, r_i, s_i, t_i) : i \in \mathbb{N} \rangle$ tale che

$$\forall q, r, s, t (\psi(q, r, s, t) \leftrightarrow \exists i (q, r, s, t) = (q_i, r_i, s_i, t_i)).$$

Se $\phi(x) < y$ per ogni x allora $\langle B(q_i, r_i) : i \in \mathbb{N} \rangle$ ricopre $[0, 1]$ e per HB ha un sottoricoprimento finito, $\langle B(q_i, r_i) : i \leq k \rangle$.

Se $z = \max\{s_i + t_i \mid i \leq k\}$ si ha $z < y$ e $\phi(x) \leq z$ per ogni $x \in [0, 1]$, contraddicendo una proprietà di y . □

Proprietà delle funzioni continue su $[0, 1]$

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 ogni funzione continua su $[0, 1]$ è uniformemente continua;
- 3 ogni funzione continua su $[0, 1]$ è limitata;
- 4 ogni funzione limitata e uniformemente continua su $[0, 1]$ ha estremo superiore;
- 5 ogni funzione limitata e uniformemente continua su $[0, 1]$ che ha estremo superiore lo raggiunge.

$1 \rightarrow 2 \wedge 3 \wedge 4 \wedge 5$: già dimostrato.

Per i reversal dimostreremo $\neg 1 \rightarrow \neg 2 \wedge \neg 3 \wedge \neg 4 \wedge \neg 5$.

Una funzione continua e illimitata

Per tutti i reversal supponiamo $\neg \text{WKL}_0$:

sia $T \subseteq 2^{<\mathbb{N}}$ un albero infinito senza cammini e poniamo $T' = \{ \tau \in 2^{<\mathbb{N}} \mid \tau \notin T \wedge \forall n < |\tau| \tau[n] \in T \}$, pure infinito.

Siano C , a_σ e b_σ come nella discussione dell'insieme di Cantor.

$\langle [a_\tau, b_\tau] : \tau \in T' \rangle$ ricopre C con elementi a due a due disgiunti.

Ogni $x \notin \bigcup \{ [a_\tau, b_\tau] \mid \tau \in T' \}$ appartiene ad un unico intervallo (b_τ, a_σ) con $\tau, \sigma \in T'$.

Definiamo una funzione continua illimitata $\phi : [0, 1] \rightarrow \mathbb{R}$ ponendo $\phi(x) = |\tau|$ se $x \in [a_\tau, b_\tau]$ per qualche $\tau \in T'$, ed estendendo linearmente negli intervalli del tipo (b_τ, a_σ) per $\tau, \sigma \in T'$.

Dato che T' è infinito, ϕ è illimitata e quindi non uniformemente continua.

Perciò sia 2 che 3 sono falsi.

Una funzione uniformemente continua senza estremo superiore

Il sistema
WKL₀

Analisi

I reali

Funzioni
continue

Equazioni
differenziali e
teoremi di punto
fisso

Logica

Algebra

Continuiamo a supporre $\neg\text{WKL}_0$ e usiamo la stessa notazione.

Da $\neg\text{WKL}_0$ segue $\neg\text{ACA}_0$ ed esiste una successione crescente e limitata di reali senza estremo superiore:

$$c_0 < c_1 < \dots < c_n < \dots < 2.$$

Definiamo $\phi_4 : [0, 1] \rightarrow \mathbb{R}$ ponendo $\phi_4(x) = c_{|\tau|}$ se $x \in [a_\tau, b_\tau]$ per qualche $\tau \in T'$, ed estendendo linearmente negli intervalli del tipo (b_τ, a_σ) per $\tau, \sigma \in T'$.

Dato che $\langle c_n \rangle$ non ha estremo superiore, neppure ϕ_4 ce l'ha. ϕ_4 è uniformemente continua e 4 è falso.

Una funzione uniformemente continua con estremo superiore e senza massimo

Il sistema
WKL₀

Analisi

I reali

Funzioni
continue

Equazioni
differenziali e
teoremi di punto
fisso

Logica

Algebra

Definiamo $\phi_5 : [0, 1] \rightarrow \mathbb{R}$ ponendo $\phi_5(x) = 1 - 2^{-|\tau|}$ se $x \in [a_\tau, b_\tau]$ per qualche $\tau \in T'$, ed estendendo linearmente negli intervalli del tipo (b_τ, a_σ) per $\tau, \sigma \in T'$.

$\sup\{\phi_5(x) \mid x \in [0, 1]\} = 1$ ma $\phi_5(x) < 1$ per ogni x .

ϕ_5 è uniformemente continua e 5 è falso.

Il teorema di approssimazione di Weierstrass

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 se $\phi : [0, 1] \rightarrow \mathbb{R}$ è continua e $\varepsilon > 0$ esiste un polinomio p tale che $\forall x \in [0, 1] |\phi(x) - p(x)| < \varepsilon$;
- 3 se $\phi : [0, 1] \rightarrow \mathbb{R}$ è continua esistono polinomi $\langle p_n : n \in \mathbb{N} \rangle$ tali che $\forall n \forall x \in [0, 1] |\phi(x) - p(x)| < 2^{-n}$.

Dimostrazione.

$1 \rightarrow 2 \wedge 3$: 2 per ϕ uniformemente continua e 3 per ϕ con modulo di uniforme continuità si dimostrano in RCA_0 .

In WKL_0 le funzioni continue hanno queste caratteristiche.

$2 \vee 3 \rightarrow 1$ perché i polinomi sono limitati. □

L'integrale di Riemann

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 se $\phi : [0, 1] \rightarrow \mathbb{R}$ è continua $\int_0^1 \phi(x) dx$ (definito in modo standard) esiste ed è finito.

Dimostrazione.

$1 \rightarrow 2$: se ϕ ha modulo di uniforme continuità l'integrale si definisce in RCA_0 con la solita costruzione.

$\neg 1 \rightarrow \neg 2$: se $\neg WKL_0$ definiamo $\phi : [0, 1] \rightarrow \mathbb{R}$ ponendo $\phi(x) = 3^{|\tau|} = (b_\tau - a_\tau)^{-1}$ se $x \in [a_\tau, b_\tau]$ per qualche $\tau \in T'$, e linearmente negli intervalli del tipo (b_τ, a_σ) per $\tau, \sigma \in T'$.

$\int_0^1 \phi(x) dx$ è infinito. □

Il teorema di esistenza di Peano

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 se $F : [-a, a] \times [-b, b] \rightarrow \mathbb{R}$ è *continua*, $M = \max F$ e $c = \max\{a, b/M\}$ allora esiste $\phi : [-c, c] \rightarrow \mathbb{R}$ *continua* con $\phi(0) = 0$ e $\phi'(x) = F(x, \phi(x))$ per ogni $x \in [-c, c]$;
- 3 lo stesso enunciato per F con modulo di uniforme continuità.

Il lemma di Ascoli-Arzelà, che viene normalmente usato nelle dimostrazioni del teorema di Peano, è equivalente a ACA_0 .

Quindi $1 \rightarrow 2$ non usa il lemma di Ascoli-Arzelà.

La dimostrazione del teorema di Peano in WKL_0 è più “costruttiva”, ma non più semplice, di quella usuale.

Due teoremi di punto fisso

Il sistema
WKL₀

Analisi

I reali

Funzioni
continue

Equazioni
differenziali e
teoremi di punto
fisso

Logica

Algebra

Teorema (RCA₀)

Sono equivalenti:

- 1 WKL₀;
- 2 se $\phi : [0, 1] \times [0, 1] \rightarrow [0, 1] \times [0, 1]$ è continua allora esiste $x_0 \in [0, 1] \times [0, 1]$ tale che $\phi(x_0) = x_0$;
- 3 se C è chiuso e convesso in $[-1, 1]^{\mathbb{N}}$ e $\phi : C \rightarrow C$ è continua allora esiste $x_0 \in C$ tale che $\phi(x_0) = x_0$.

2 è il teorema di punto fisso di Brouwer, mentre 3 è noto come teorema di punto fisso di Schauder.

Nozioni logiche

Fissiamo un linguaggio numerabile $L \subseteq \mathbb{N}$
ed una numerazione di Gödel di termini e formule.
Usiamo solo \neg , \wedge e \forall .

Sistema alla Hilbert, con il *modus ponens* come unica regola.

Per ric prim si definiscono gli insiemi Term_L (termini),
 Form_L (formule), En_L (enunciati), Ass_L (assiomi logici).

$$\text{Dim}(X, p) \leftrightarrow p \in \mathbb{N}^{<\mathbb{N}} \wedge \forall k < |p| (p(k) \in \text{Form}_L) \wedge \Sigma_0^0 \\ \forall k < |p| (p(k) \in X \cup \text{Ass}_L \vee \exists i, j < k (p(i) = 'p(j) \rightarrow p(k)'))).$$

$$\text{Prov}(X, \varphi) \leftrightarrow \exists p (\text{Dim}(X, p) \wedge p(|p| - 1) = \varphi) \quad \Sigma_1^0$$

$$\text{Ch}(X) \leftrightarrow \forall \sigma \in \text{En}_L (\text{Prov}(X, \sigma) \rightarrow \sigma \in X) \quad \Pi_1^0$$

$$\text{Coer}(X) \leftrightarrow \forall \sigma \in \text{En}_L (\neg \text{Prov}(X, \sigma) \vee \neg \text{Prov}(X, \neg \sigma)) \quad \Pi_1^0$$

$$\text{Compl}(X) \leftrightarrow \forall \sigma \in \text{En}_L (\text{Prov}(X, \sigma) \vee \text{Prov}(X, \neg \sigma)) \quad \Pi_2^0$$

Il lemma di Lindenbaum in WKL_0

Lemma (WKL_0)

Sia $X \subseteq \text{En}_L$ tale che $\text{Coer}(X)$. Esiste $X^* \subseteq \text{En}_L$ tale che $X \subseteq X^*$, $\text{Coer}(X^*)$, $\text{Ch}(X^*)$ e $\text{Compl}(X^*)$.

Dimostrazione.

Sia $\langle \sigma_i : i \in \mathbb{N} \rangle$ un'enumerazione di En_L .

Sia T l'insieme dei $\tau \in 2^{<\mathbb{N}}$ tali che per ogni $i, j, p < |\tau|$ si ha

- 1 $\sigma_i \in X \rightarrow \tau(i) = 1$;
- 2 $\text{Dim}(\{ \sigma_i \mid \tau(i) = 1 \}, p) \rightarrow$
 $\forall k < |p| (p(k) = \sigma_j \rightarrow \tau(j) = 1)$;
- 3 $\sigma_i = \neg \sigma_j \rightarrow \tau(i) = 1 - \tau(j)$.

$\text{Coer}(X)$ implica che T è infinito e quindi ha un cammino g .

$X^* = \{ \sigma_i \mid g(i) = 1 \}$ è il completamento cercato. \square

Modelli in RCA_0

Definizione

Un **modello** è una funzione $M : T_M \cup E_M \rightarrow |M| \cup \{0, 1\}$ dove $|M| \subseteq \mathbb{N}$ (universo di M) e T_M, E_M sono gli insiemi dei termini chiusi e degli enunciati di $L_M = L \cup \{\underline{m} \mid m \in |M|\}$. M soddisfa le condizioni della definizione di verità di Tarski:

- se $t \in T_M$ allora $M(t) \in |M|$;
- $M(\underline{m}) = m$;
- se $\sigma \in E_M$ allora $M(\sigma) \in \{0, 1\}$;
- se $t_0, s_0, \dots, t_n, s_n \in T_M$ sono tali che $M(t_i) = M(s_i)$ allora $M(f(\bar{t})) = M(f(\bar{s}))$ e $M(r(\bar{t})) = M(r(\bar{s}))$ per ogni simbolo di funzione f e simbolo di relazione r di L ;
- $M(\neg\sigma) = 1 - M(\sigma)$;
- $M(\sigma_1 \wedge \sigma_2) = M(\sigma_1) \cdot M(\sigma_2)$;
- $M(\forall v \varphi(v)) = \prod_{m \in |M|} M(\varphi(\underline{m}))$.

Reverse mathematics dei teoremi logici

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 *il lemma di Lindenbaum;*
- 3 *il teorema di completezza di Gödel: se $Coer(X)$ allora X ha un modello M (cioè $\forall \sigma \in X M(\sigma) = 1$);*
- 4 *il teorema di compattezza: se ogni sottoinsieme finito di X ha un modello, allora X ha un modello;*
- 5 *il teorema di completezza per la logica proposizionale;*
- 6 *il teorema di compattezza per la logica proposizionale.*

1 \rightarrow 2 appena dimostrato. 2 \rightarrow 3 come due giorni fa.

3 \rightarrow 4 e 5 \rightarrow 6 standard. 3 \rightarrow 5 e 4 \rightarrow 6 ovvi.

6 \rightarrow 1 è il reversal.

Il reversal

Consideriamo la logica proposizionale con atomi $\langle a_i : i \in \mathbb{N} \rangle$.
Poniamo $a_i^0 = \neg a_i$ e $a_i^1 = a_i$.

Sia $T \subseteq 2^{<\mathbb{N}}$ un albero infinito. Per ogni n definiamo

$$\sigma_n = \bigvee \left\{ a_0^{\tau(0)} \wedge \cdots \wedge a_{n-1}^{\tau(n-1)} \mid \tau \in T \wedge |\tau| = n \right\}.$$

Dato che esiste $\tau \in T$ con $|\tau| = n$ ogni σ_n ha un modello, che è anche un modello per σ_m con $m < n$. Quindi ogni sottoinsieme finito di $X = \{ \sigma_n \mid n \in \mathbb{N} \}$ ha un modello.

Per compattezza X ha un modello M , che associa ad ogni formula 0 (falso) o 1 (vero).

g definita da $g(i) = M(a_i)$ è un cammino in T .

Ideali in anelli

Definizione (RCA_0)

Un **anello** (commutativo) $(|A|, 0_A, 1_A, +_A, -_A, \cdot_A)$ consiste di $|A| \subseteq \mathbb{N}$, $0_A \neq 1_A \in |A|$, operazioni binarie $+_A$ e \cdot_A , un'operazione unaria $-_A$ che soddisfano gli usuali assiomi.

Un **dominio d'integrità** è un anello tale che

$$\forall a, b \in |A| (a \cdot_A b = 0_A \rightarrow a = 0_A \vee b = 0_A).$$

D'ora in poi scriviamo A per $|A|$ e omettiamo i pedici $_A$.

Definizione (RCA_0)

Un **ideale di A** è un insieme $I \subseteq |A|$ tale che $0 \in I$, $1 \notin I$,

$$\forall a, b \in I \ a + b \in I \text{ e } \forall a \in I \ \forall b \in A \ a \cdot b \in I.$$

Un **ideale massimale di A** è un ideale M tale che

$$\forall a \in A \setminus M \ \exists b \in A (a \cdot b - 1 \in M).$$

Un **ideale primo di A** è un ideale P tale che

$$\forall a, b \in A (a \cdot b \in P \rightarrow a \in P \vee b \in P).$$

Esistenza di ideali primi

Il sistema
 WKL_0

Analisi

Logica

Algebra

Anelli
Campi

Teorema (WKL_0)

Ogni anello A ha un ideale primo.

La dimostrazione usuale di questo teorema avviene mostrando che ogni anello ha un ideale massimale e osservando che ogni ideale massimale è primo.

Questa dimostrazione non può essere fatta in WKL_0 , perché l'esistenza di ideali massimali è equivalente a ACA_0 .

La nostra dimostrazione seguirà altre strade.

Primo passo per costruire un ideale primo

Sia $\langle a_i : i \in \mathbb{N} \rangle$ un'enumerazione di A con $a_0 = 0$ e $a_1 = 1$.

Definiamo ricorsivamente una succ di insiemi finiti

$\langle X_\sigma : \sigma \in 2^{<\mathbb{N}} \rangle$, iniziando da $X_{\langle \rangle} = \{0\}$.

Se X_σ è definito e $|\sigma| = 4 \cdot ((i, j), m) + k$ con $0 \leq k < 4$:

$k = 0$ se $a_i \cdot a_j \notin X_\sigma$, $X_{\sigma \frown \langle 0 \rangle} = X_{\sigma \frown \langle 1 \rangle} = X_\sigma$;

se $a_i \cdot a_j \in X_\sigma$, $X_{\sigma \frown \langle 0 \rangle} = X_\sigma \cup \{a_i\}$ e

$X_{\sigma \frown \langle 1 \rangle} = X_\sigma \cup \{a_j\}$;

$k = 1$ $X_{\sigma \frown \langle 0 \rangle} = \emptyset$; se $a_i, a_j \in X_s$, $X_{\sigma \frown \langle 1 \rangle} = X_\sigma \cup \{a_i + a_j\}$,

se $a_i \notin X_s$ oppure $a_j \notin X_s$, $X_{\sigma \frown \langle 1 \rangle} = X_\sigma$;

$k = 2$ $X_{\sigma \frown \langle 0 \rangle} = \emptyset$; se $a_i \in X_s$, $X_{\sigma \frown \langle 1 \rangle} = X_\sigma \cup \{a_i \cdot a_j\}$,

se $a_i \notin X_s$, $X_{\sigma \frown \langle 1 \rangle} = X_\sigma$;

$k = 3$ $X_{\sigma \frown \langle 0 \rangle} = \emptyset$; se $1 \in X_s$, $X_{\sigma \frown \langle 1 \rangle} = \emptyset$,

se $1 \notin X_s$, $X_{\sigma \frown \langle 1 \rangle} = X_\sigma$.

Se $|\sigma|$ non è del tipo $4 \cdot ((i, j), m) + k$ con $0 \leq k < 4$,

$X_{\sigma \frown \langle 0 \rangle} = \emptyset$ e $X_{\sigma \frown \langle 1 \rangle} = X_\sigma$.

$S = \{\sigma \in \mathbb{N}^{<\mathbb{N}} \mid X_\sigma \neq \emptyset\}$ è un albero.

L'infinità di S

Per dimostrare che S è infinito mostriamo per Π_1^0 -induzione che per ogni n esiste $\sigma \in S$ con $|\sigma| = n$ tale che X_σ non genera A come A -modulo (cioè nessuna combinazione lineare di elementi di X_σ con coefficienti in A è uguale a 1).

Per $n = 0$, $X_{\langle \rangle} = \{0\}$ e siamo a posto.

Per il passo induttivo sia $\sigma \in S$ con $|\sigma| = n$ tale che X_σ che non genera A (e quindi $1 \notin X_\sigma$).

I casi $k = 1, 2, 3$ sono banali, perché gli elementi eventualmente aggiunti a X_σ per ottenere $X_{\sigma \frown \langle 1 \rangle}$ sono c.l. di elementi di X_σ .

Il caso $k = 0$ e $a_i \cdot a_j \notin X_\sigma$ è l'unico interessante: si deve dimostrare che non è possibile che sia $X_{\sigma \frown \langle 0 \rangle} = X_\sigma \cup \{a_i\}$ che $X_{\sigma \frown \langle 1 \rangle} = X_\sigma \cup \{a_j\}$ generino A .

Altrimenti $1 = c + ra_i = d + sa_j$ con $r, s \in A$ e c, d c.l. di elementi di X_σ . Ma allora

$$1 = (c + ra_i) \cdot (d + sa_j) = cd + csa_j + dra_i + rs(a_i a_j)$$

è una c.l. di elementi di X_σ .

Un'illusione

Il sistema
 WKL_0

Analisi

Logica

Algebra

Anelli
Campi

Allora S ha un cammino g .

Si verifica facilmente che $\bigcup_n A_{g[n]}$ è un ideale primo.

Ma WKL_0 non dimostra l'esistenza di $\bigcup_n A_{g[n]}$!

(ci vuole Σ_1^0 -comprensione)

Ci salveremo con la Σ_1^0 -comprensione limitata...

Finalmente l'ideale primo

Il sistema
WKL₀

Analisi

Logica

Algebra

Anelli
Campi

Sia T l'insieme dei $\sigma \in 2^{<\mathbb{N}}$ tali che $\sigma(0) = 1$ se $|\sigma| > 0$, $\sigma(1) = 0$ se $|\sigma| > 1$ e, per ogni $i, j, k < |\sigma|$ si ha

- 1 se $\sigma(i) = \sigma(j) = 1$ e $a_i + a_j = a_k$ allora $\sigma(k) = 1$;
- 2 se $\sigma(i) = 1$ e $a_i \cdot a_j = a_k$ allora $\sigma(k) = 1$;
- 3 se $\sigma(i) = \sigma(j) = 0$ e $a_i \cdot a_j = a_k$ allora $\sigma(k) = 0$.

T è un albero.

Dato m sia $Y = \{i < m \mid \exists n a_i \in A_{g[n]}\}$ e definiamo $\sigma \in 2^{<\mathbb{N}}$ con $|\sigma| = m$ ponendo per $i < m$, $\sigma(i) = 1$ se e solo se $i \in Y$. Dato che $\sigma \in T$, T è infinito e ha un cammino h .

$P = \{a_i \mid h(i) = 1\}$ è un ideale primo in A .

Reverse mathematics dell'esistenza degli ideali primi

Definizione

Un **ideale radicale di A** è un ideale R tale che

$$\forall a \in A \forall n (a^n \in R \rightarrow a \in R).$$

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 ogni anello ha un'ideale primo;
- 3 ogni anello ha un'ideale radicale.

1 \rightarrow 2 appena dimostrato.

2 \rightarrow 3: in RCA_0 si dimostra che ogni ideale primo è radicale.

3 \rightarrow 1 è il reversal.

Il reversal

In RCA_0 dimostriamo che se ogni anello ha un'ideale radicale allora le immagini disgiunte delle funzioni iniettive f, g sono separate da un insieme.

Sia $A_0 = \mathbb{Q}[\langle x_n : n \in \mathbb{N} \rangle]$ l'anello dei polinomi su \mathbb{Q} in infinite variabili.

$\{x_{f(m)}^{m+1} \mid m \in \mathbb{N}\} \cup \{x_{g(m)}^{m+1} - 1 \mid m \in \mathbb{N}\}$ genera un ideale I .

Dato $f \in A_0$, f ha una forma normale f^* modulo I :

se x_n^k occorre in f^* allora $k \neq f(m), g(m)$ per ogni $m < k$.

Questo mostra che $I = \{f \in A_0 \mid f^* = 0\}$ esiste.

Sia $A = A_0/I$ e per 3 sia J un ideale radicale in A .

$J_0 = \{f \in A_0 \mid [f]_I \in J\}$ è un ideale radicale di A_0 .

$x_{f(m)} \in J_0$ (perché $x_{f(m)}^{m+1} \in I \subseteq J_0$ e J_0 è radicale).

$x_{f(m)} \notin J_0$ perché altrimenti $1 \cong_I x_{g(m)}^{m+1} \in J_0$.

Perciò $\{n \mid x_n \in J_0\}$ separa le immagini di f e g .

Campi

Un **campo** K consiste di un insieme $|K|$, di elementi 0_K e 1_K , di operazioni binarie $+_K$ e \cdot_K e di un'operazione unaria $-_K$, che soddisfano gli usuali assiomi per i campi.

L'**anello dei polinomi su K** è

$$K[x] = \{ \langle a_0, \dots, a_n \rangle \mid \forall i \leq n a_i \in K \wedge (n > 0 \rightarrow a_n \neq 0_K) \}.$$

Scriveremo $f(x) = \sum_{i=0}^n a_i x^i$ al posto di $\langle a_0, \dots, a_n \rangle$ e $f(a) = \sum_{i=0}^n a_i a^i$ quando $a \in K$.

K è **algebricamente chiuso** se per ogni $f(x) \in K[x]$ di grado ≥ 1 esiste $a \in K$ tale che $f(a) = 0_K$.

Una **chiusura algebrica** di K consiste di un campo algebricamente chiuso \tilde{K} e di un monomorfismo $h : K \rightarrow \tilde{K}$ tali che $\forall b \in \tilde{K} \exists f(x) \in K[x] (f(x) \neq 0_K \wedge h(f)(b) = 0_{\tilde{K}})$.

RCA₀ **non dimostra** l'esistenza dell'immagine di h .

Unicità della chiusura algebrica

Teorema (WKL₀)

Ogni campo K ha un'unica chiusura algebrica: se $h_i : K \rightarrow \tilde{K}_i$ ($i = 1, 2$) sono chiusure algebriche di K esiste un isomorfismo $h : \tilde{K}_1 \rightarrow \tilde{K}_2$ tale che $h(h_1(a)) = h_2(a)$ per ogni $a \in K$.

Dimostrazione.

Siano $\langle a_i : i \in \mathbb{N} \rangle$ e $\langle b_i : i \in \mathbb{N} \rangle$ enumerazioni di K e \tilde{K}_1 .

Sia $\langle p_i : i \in \mathbb{N} \rangle$ una succ di polinomi con $h_1(p_i)(b_i) = 0$.

Sia T l'insieme dei $\sigma \in \mathbb{N}^{<\mathbb{N}}$ tali che per ogni $i, j, k < |\sigma|$ si ha

- (1) $\sigma(i) \in \tilde{K}_2$; (2) se $b_i + b_j = b_k$ allora $\sigma(i) + \sigma(j) = \sigma(k)$;
- (3) se $b_i \cdot b_j = b_k$ allora $\sigma(i) \cdot \sigma(j) = \sigma(k)$; (4) se $b_i = h_1(a_j)$ allora $\sigma(i) = h_2(a_j)$; (5) $h_2(p_i)(\sigma(i)) = 0$.

T è un albero infinito (considerando estensioni finite di K) e limitato per (5): $\sigma(i) \leq \max\{c \in \tilde{K}_2 \mid h_2(p_i)(c) = 0\}$.

Se g è un cammino in T , $h(b_i) = g(i)$ è l'isomorfismo. □

Reverse mathematics dell'unicità della chiusura algebrica

Teorema (RCA_0)

Sono equivalenti:

- 1 WKL_0 ;
- 2 ogni campo ha un'unica chiusura algebrica.

1 \rightarrow 2 appena dimostrato.

2 \rightarrow 1: si mostra in RCA_0 che se ogni campo ha un'unica chiusura algebrica allora le immagini disgiunte delle funzioni iniettive f, g sono separate da un insieme.

Si utilizzano due diverse immersioni dello stesso campo in $\overline{\mathbb{Q}(\sqrt{-1})}$.

Ricorsione transfinita e oltre

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

- 1 Il sistema ATR_0
- 2 Confrontabilità dei buoni ordini
- 3 Altri risultati
- 4 Il sistema $\Pi_1^1\text{-CA}_0$
- 5 Altri sottosistemi

Ordini

Definizione

Se $X \subseteq \mathbb{N} \times \mathbb{N}$ poniamo

$$\text{fld}(X) = \{ i \mid \exists j((i, j) \in X \vee (j, i) \in X) \},$$
$$i \leq_X j \leftrightarrow (i, j) \in X \text{ e } i <_X j \leftrightarrow i \leq_X j \wedge i \neq j.$$

$X \subseteq \mathbb{N} \times \mathbb{N}$ è **ben fondato** se non esiste $f : \mathbb{N} \rightarrow \text{fld}(X)$ tale che $\forall n f(n+1) <_X f(n)$.

$X \subseteq \mathbb{N} \times \mathbb{N}$ è un **ordine parziale** se valgono:

- $\forall i \in \text{fld}(X)(i \leq_X i)$;
- $\forall i, j \in \text{fld}(X)(i \leq_X j \wedge j \leq_X i \rightarrow i = j)$;
- $\forall i, j, k \in \text{fld}(X)(i \leq_X j \wedge j \leq_X k \rightarrow i \leq_X k)$.

X è un **ordine lineare** se vale anche:

- $\forall i, j \in \text{fld}(X)(i \leq_X j \vee j \leq_X i)$.

Un ordine lineare ben fondato è un **buon ordine**.

Il sistema
ATR₀

Gli assiomi
 ω -modelli

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 Π^1_1 -CA₀

Altri
sottosistemi

Verso la ricorsione transfinita

L'idea della ricorsione transfinita è la seguente: se $\theta(n, Y)$ è una formula e X un buon ordine, per ogni $i \in \text{fld}(X)$ vogliamo definire $Y_i = \{ n \mid \theta(n, \bigcup_{j <_X i} Y_j) \}$.

Se $Y = \{ (n, i) \mid i \in \text{fld}(X) \wedge n \in Y_i \}$,

$\bigcup_{j <_X i} Y_j$ è codificato da $Y^i = \{ (m, j) \in Y \mid j <_X i \}$.

Definizione (RCA₀)

Se $\theta(n, Y)$ è una formula, $H_\theta(X, Y)$ è la formula

$$\text{LO}(X) \wedge Y = \{ (n, i) \mid i \in \text{fld}(X) \wedge \theta(n, Y^i) \}.$$

$H_\theta(k, X, Y)$ è la formula

$$\text{LO}(X) \wedge k \in \text{fld}(X) \wedge Y = \{ (n, i) \mid i <_X k \wedge \theta(n, Y^i) \}.$$

Se $H_\theta(X, Y)$ allora $\forall k \in \text{fld}(X) H_\theta(k, X, Y^k)$.

θ può avere variabili libere diverse da n e T , e quelle variabili saranno libere in $H_\theta(X, Y)$ e $H_\theta(k, X, Y)$.

ATR₀

Siano $LO(X)$ e $WO(X)$ le formule che asseriscono che X è, rispettivamente, un ordine lineare e un buon ordine.

$LO(X)$ è Π_1^0 , mentre $WO(X)$ è Π_1^1 .

Gli assiomi di ATR_0 sono quelli di ACA_0 più lo schema di ricorsione transfinita aritmetica:
se θ è aritmetica

$$\forall X (WO(X) \rightarrow \exists Y H_\theta(X, Y))$$

ATR abbrevia Arithmetic Transfinite Recursion.

Induzione transfinita aritmetica

L'induzione corrispondente alla ricorsione transfinita aritmetica è dimostrabile in ACA_0 .

Teorema

*Se $\varphi(X)$ è una formula aritmetica ACA_0 dimostra:
per ogni X tale che $WO(X)$ vale*

$$\forall i \in \text{fld}(X) (\forall j <_X i \varphi(j) \rightarrow \varphi(i)) \rightarrow \forall i \in \text{fld}(X) \varphi(i).$$

Dimostrazione.

Sia $Y = \{i \in \text{fld}(X) \mid \neg \varphi(i)\}$. Se vale l'ipotesi dell'implicazione $\forall i \in Y \exists j \in Y j <_X i$.

Se $Y \neq \emptyset$ definiamo $f : \mathbb{N} \rightarrow \text{fld}(X)$ per ricorsione ponendo $f(0) = \min Y$, $f(n+1) = \min\{j \in Y \mid j <_X f(n)\}$ (i minimi sono rispetto a $<$, non a $<_X$).

f mostra $\neg WO(X)$. Quindi $Y = \emptyset$, cioè $\forall i \in \text{fld}(X) \varphi(i)$. \square

Unicità della ricorsione transfinita

Lemma (ACA_0)

Se $\theta(n, Y)$ è una formula e X è un buon ordine, esiste al più un Y tale che $H_\theta(X, Y)$.

Similmente, per ogni k esiste al più un Y tale che $H_\theta(k, X, Y)$.

Dimostrazione.

Se $H_\theta(X, Y)$ e $H_\theta(X, Z)$ dimostriamo per induzione transfinita aritmetica che $\forall j \in \text{fld}(X) Y^j = Z^j$.

Assumendo che $\forall i <_X j Y^i = Z^i$ si ha

$Y_i = \{n \mid \theta(n, Y^i)\} = \{n \mid \theta(n, Z^i)\} = Z_i$ per ogni $i <_X j$.

Perciò $Y^j = \{(n, i) \mid i <_X j \wedge n \in Y_i\} =$
 $= \{(n, i) \mid i <_X j \wedge n \in Z_i\} = Z^j$.

L'argomento per $H_\theta(k, X, Y)$ è lo stesso. □

Σ_1^1 -separazione

Il sistema
 ATR_0

Gli assiomi
 ω -modelli

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 Π_1^1 -CA₀

Altri
sottosistemi

Teorema (RCA₀)

Sono equivalenti:

- 1 ATR_0 ;
- 2 Σ_1^1 -separazione: se $\varphi_0(n)$ e $\varphi_1(n)$ sono formule Σ_1^1 in cui X non è libera e per cui vale $\neg \exists n(\varphi_0(n) \wedge \varphi_1(n))$ allora $\exists X \forall n((\varphi_0(n) \rightarrow n \in X) \wedge (\varphi_1(n) \rightarrow n \notin X))$.

$1 \rightarrow 2$ è dimostrato nel libro di Simpson attraverso il teorema di separazione di Lusin (teoria descrittiva degli insiemi). Noi ci arriveremo attraverso la confrontabilità dei buoni ordini.

$2 \rightarrow 1$ è il reversal.

Σ_1^1 -separazione implica ATR_0

La Σ_1^1 -separazione implica la comprensione aritmetica, quindi possiamo ragionare in ACA_0 .

Siano X un buon ordine e $\theta(n, Y)$ una formula aritmetica.

$$\begin{aligned} \text{Siano } \varphi_0(n, j) &\leftrightarrow \exists Y (H_\theta(j, X, Y) \wedge \theta(n, Y)) \\ &\text{e } \varphi_1(n, j) \leftrightarrow \exists Y (H_\theta(j, X, Y) \wedge \neg\theta(n, Y)). \end{aligned}$$

$\varphi_0(n, j)$ e $\varphi_1(n, j)$ sono entrambe Σ_1^1 e, dato che esiste al più un Y tale che $H_\theta(j, X, Y)$, si ha $\neg\exists n \exists j (\varphi_0(n, j) \wedge \varphi_1(n, j))$.

Per Σ_1^1 -separazione esiste W tale che

$$\forall n, j ((\varphi_0(n, j) \rightarrow (n, j) \in W) \wedge (\varphi_1(n, j) \rightarrow (n, j) \notin W)).$$

Per induzione transfinita aritmetica dimostriamo $H_\theta(j, X, W^j)$ e $\forall n ((n, j) \in W \leftrightarrow \theta(n, W^j))$ per ogni $j \in \text{fld}(X)$.

L'ipotesi induttiva implica subito $H_\theta(j, X, W^j)$.

Inoltre $\forall n ((\varphi_0(n, j) \leftrightarrow \theta(n, W^j)) \wedge (\varphi_1(n, j) \leftrightarrow \neg\theta(n, W^j)))$.

Perciò $\forall n ((n, j) \in W \leftrightarrow \theta(n, W^j))$.

Se $Z = \{ (n, j) \in W \mid j \in \text{fld}(X) \}$ si ha $H_\theta(X, Z)$.

ω -modelli di ATR_0

Teorema

ARITH non è un modello di ATR_0 ,
e quindi ATR_0 è strettamente più forte di ACA_0 .

Dimostrazione.

Sia $\theta(n, Y) \leftrightarrow n \in Y'$. θ è Σ_1^0 e quindi aritmetica.
Sia $X = \{ (j, i) \mid j < i \}$, l'ordine usuale di \mathbb{N} .
 RCA_0 dimostra $\text{WO}(X)$, che è quindi vero in **ARITH**.
Se Y è tale che $H_\theta(X, Y)$, per ogni i si ha $Y_i = \emptyset^{(i+1)}$.
Allora $\emptyset^{(i+1)} \leq_T Y$ per ogni i e quindi $Y \notin \text{ARITH}$. □

Non esiste il più piccolo ω -modello di ATR_0 .

HYP, l'insieme dei sottoinsiemi iperaritmetici di ω ,
è l'intersezione di tutti gli ω -modelli di ATR_0 .

Il sistema
 ATR_0

Gli assiomi
 ω -modelli

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

β -modelli di ATR_0

Il sistema
 ATR_0

Gli assiomi
 ω -modelli

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 Π_1^1 - CA_0

Altri
sottosistemi

Un β -modello è un ω -modello \mathcal{M} tale che per ogni enunciato $\Sigma_1^1 \varphi$ (con parametri da M), $\mathcal{M} \models \varphi$ se e solo se φ è vero.

[Per gli ω -modelli questo vale per φ aritmetica.]

Ogni β -modello è un modello di ATR_0 .

Non esiste il più piccolo β -modello di ATR_0
e **HYP** è l'intersezione di tutti i β -modelli di ATR_0 .

Confrontare ordini lineari

Definizione (RCA_0)

Supponiamo $LO(X)$ e $LO(Y)$.

Un **isomorfismo** tra X e Y è una $f : fld(X) \rightarrow fld(Y)$ tale che
$$\forall i, j \in fld(X) (i \leq_X j \leftrightarrow f(i) \leq_Y f(j)).$$

Scriviamo $f : X = Y$, mentre $X = Y$ (un abuso di notazione come quello per i reali) indica l'esistenza di un isomorfismo.

X è un **segmento iniziale** di Y se esiste $k \in fld(Y)$ tale che
 $X = \{ (i, j) \mid i \leq_Y j <_Y k \}$.

$f : X < Y$ indica che f è un isomorfismo tra X e un segmento iniziale di Y . $f : X > Y$ indica che f è un isomorfismo tra un segmento iniziale di X e Y .

$f : X \leq Y$, $f : X \geq Y$, $X < Y$, $X > Y$, $X \leq Y$ e $X \geq Y$ hanno i significati ovvi.

Una **mappa di confronto** tra X e Y è una f tale che
 $f : X \leq Y$ oppure $f : X \geq Y$.

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO
L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi^1_1\text{-CA}_0$

Altri
sottosistemi

Buoni ordini e ordinali

I buoni ordini sono i codici per gli ordinali numerabili.

Se $WO(X)$ e $WO(Y)$, $X < Y$, $X > Y$, $X \leq Y$ e $X \geq Y$ rappresentano le corrispondenti relazioni tra ordinali.

Mostreremo che ATR_0 è necessaria per una buona teoria degli ordinali.

Una proprietà fondamentale degli ordinali è la loro confrontabilità.

Definizione (RCA_0)

Indichiamo con **CWO** la confrontabilità dei buoni ordini: se $WO(X)$ e $WO(Y)$ esiste una mappa di confronto tra X e Y , cioè $X \leq Y$ oppure $X \geq Y$.

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1-CA_0$

Altri
sottosistemi

Unicità della mappa di confronto

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

Teorema (RCA_0)

Se $WO(X)$ e $WO(Y)$ esiste al più una mappa di confronto tra X e Y . In particolare non può essere sia $X \leq Y$ che $X > Y$.

Dimostrazione.

Se f e g sono due mappe di confronto tra X e Y sia $Z = \{i \in \text{fld}(X) \mid f(i) \neq g(i)\}$.

Si ha $\forall i \in Z \exists j \in Z j <_X i$ e, se $Z \neq \emptyset$, avremmo $\neg WO(X)$.

Perciò $Z = \emptyset$ e $f = g$. □

Esistenza della mappa di confronto

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

Teorema (ATR_0)

CWO: se $WO(X)$ e $WO(Y)$ esiste una mappa di confronto tra X e Y .

Dimostrazione.

Sia $\theta(n, f)$ la formula aritmetica che asserisce che $n \in \text{fld}(X)$ e esiste $\ell \in \text{fld}(Y)$ tale che

$$f : \{ i \in \text{fld}(X) \mid i <_X n \} = \{ j \in \text{fld}(Y) \mid j <_Y \ell \}.$$

Per ricorsione transfinita esiste f tale che $H_\theta(Y, f)$.

Per induzione transfinita aritmetica si verifica che f è una mappa di confronto tra X e Y . □

L'ordine di Kleene-Brouwer

Definizione

L'**ordine di Kleene-Brouwer KB** è un ordine lineare con $\text{fld}(\text{KB}) = \mathbb{N}^{<\mathbb{N}}$ definito ponendo $\sigma \leq_{\text{KB}} \tau$ se e solo se $\tau \subseteq \sigma \vee \exists j < \min\{|\sigma|, |\tau|\} (\forall i < j \sigma(i) = \tau(i) \wedge \sigma(j) < \tau(j))$.

$\langle \rangle$ è il massimo dell'ordine di Kleene-Brouwer, che non ha minimo ed è denso.

Studieremo soprattutto le restrizioni dell'ordine di Kleene-Brouwer: se $T \subseteq \mathbb{N}^{<\mathbb{N}}$ sia $\text{KB}(T) = \text{KB} \cap (T \times T)$.

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

L'ordine di Kleene-Brouwer e i cammini

Lemma (ACA_0)

Se T è un albero, $WO(KB(T))$ se e solo se T non ha cammini.

Dimostrazione.

Se g è un cammino in T vale $g[n+1] <_{KB} g[n]$ per ogni n , e $KB(T)$ non è un buon ordine.

Se $KB(T)$ non è un buon ordine sia $f: \mathbb{N} \rightarrow T$ tale che $f(n+1) <_{KB} f(n)$ per ogni n .

$S = \{ \sigma \in T \mid \exists n \sigma \subseteq f(n) \}$ è un albero infinito.

Dato $\sigma \in S$, se $\sigma \hat{\ } \langle i \rangle \in S$ sia $g(i) = \min \{ n \mid \sigma \hat{\ } \langle i \rangle \subseteq f(n) \}$.

Se $i < j$ allora $f(g(i)) <_{KB} f(g(j))$ e quindi $g(i) > g(j)$.

Perciò esiste solo un numero finito di i tali che $\sigma \hat{\ } \langle i \rangle \in S$.

Abbiamo mostrato che S è finitamente generato: per il lemma di König S ha un cammino, che è un cammino in T . \square

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi^1_1\text{-CA}_0$

Altri
sottosistemi

Teorema di forma normale di Kleene

Per $f : \mathbb{N} \rightarrow \mathbb{N}$ sia $f[m] = \langle f(i) : i < m \rangle$.

Un insieme X viene identificato con la sua funzione caratteristica e $X[m] = \langle \xi(i) : i < m \rangle$ dove

$$\xi(i) = \begin{cases} 0 & \text{se } i \notin X; \\ 1 & \text{se } i \in X. \end{cases}$$

Lemma

Per ogni formula $\Sigma_1^1 \varphi(X)$ esiste una formula $\Sigma_0^0 \theta(\sigma, \tau)$ tale che ACA_0 dimostra

$$\forall X (\varphi(X) \leftrightarrow \exists f \forall m \theta(X[m], f[m])).$$

φ può avere variabili libere diverse da X , e le stesse variabili saranno libere in θ .

Il lemma viene dimostrato utilizzando le funzioni di Skolem.

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici

CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

Forma normale di Kleene per formule aritmetiche

Iniziamo a dimostrare il teorema di forma normale nel caso in cui $\varphi(X)$ è aritmetica e può essere scritta come

$$\forall m_1 \exists n_1 \dots \forall m_k \exists n_k \chi(X, m_1, n_1, \dots, m_k, n_k) \text{ con } \chi \Sigma_0^0.$$

Possiamo supporre che X occorra in χ solo in formule atomiche del tipo $m_i \in X$ e $n_i \in X$: se occorre $m_i + n_j \in X$ lo sostituiamo con $\exists n_{k+1} (n_{k+1} = m_i + n_j \wedge n_{k+1} \in X)$.

ACA₀ dimostra che $\varphi(X)$ vale se e solo se esistono le funzioni di Skolem g_1, \dots, g_k tali che

$$\forall m_1 \dots \forall m_k \chi(X, m_1, g_1(m_1), \dots, m_k, g_k(m_1, \dots, m_k)).$$

Impacchettando le funzioni di Skolem in un'unica funzione f e dato che le informazioni su X necessarie a stabilire se vale

$\chi(X, m_1, g_1(m_1), \dots, m_k, g_k(m_1, \dots, m_k))$ sono l'appartenenza o meno di $m_1, g_1(m_1), \dots, m_k, g_k(m_1, \dots, m_k)$ a X , si scrive una formula $\Sigma_0^0 \theta(\sigma, \tau)$ tale che

ACA₀ dimostra $\forall X (\varphi(X) \leftrightarrow \exists f \forall m \theta(X[m], f[m]))$.

Il sistema
ATR₀

Confrontabilità
dei buoni
ordini

Le definizioni
ATR₀ dimostra
CWO

L'ordine di
Kleene-Brouwer

Insiemi analitici
CWO implica
ATR₀

Altri risultati

Il sistema
 Π_1^1 -CA₀

Altri
sottosistemi

Forma normale di Kleene per formule Σ_1^1

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

Se $\varphi(X) \leftrightarrow \exists Y \psi(X, Y)$ con ψ aritmetica il caso precedente fornisce l'esistenza di una formula $\Sigma_0^0 \eta(\sigma, \tau)$ tale che ACA_0 dimostra $\forall X \forall Y (\psi(X, Y) \leftrightarrow \exists f \forall m \eta((X \oplus Y)[m], f[m]))$.

Come al solito $X \oplus Y = \{2n \mid n \in X\} \cup \{2n + 1 \mid n \in Y\}$.

η può essere trasformata in una formula $\Sigma_0^0 \theta(\sigma, \tau)$ tale che $\forall X (\exists Y \exists f \forall m \eta((X \oplus Y)[m], f[m]) \leftrightarrow \exists h \forall m \theta(X[m], h[m]))$.

Codici analitici

Continuiamo a identificare $X \subseteq \mathbb{N}$ con la sua funzione caratteristica $X : \mathbb{N} \rightarrow \{0, 1\}$, cioè un punto dello spazio di Cantor $2^{\mathbb{N}}$. Usiamo $X \in 2^{\mathbb{N}}$ allo stesso modo di $x \in \mathbb{R}$.

Un sottoinsieme dello spazio di Cantor è analitico se è la proiezione di un sottoinsieme chiuso di $2^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$.

Definizione (RCA_0)

Un **codice analitico** è un albero $A \subseteq \mathbb{N}^{<\mathbb{N}}$ tale che ogni membro di A è della forma $\langle (\xi_i, m_i) : i < n \rangle$ con $\xi_i < 2$, cioè è ottenuto da $\langle \xi_i : i < n \rangle \in 2^{<\mathbb{N}}$ e $\langle m_i : i < n \rangle \in \mathbb{N}^{<\mathbb{N}}$. Scriviamo $A(\sigma, \tau)$ per $|\sigma| = |\tau| \wedge \langle (\sigma(i), \tau(i)) : i < |\sigma| \rangle \in A$. Per $X \in 2^{\mathbb{N}}$, **X è un punto di A** se $\exists f \forall k A(X[k], f[k])$.

Se X è un punto di A scriviamo $X \in A$, altrimenti $X \notin A$. $X \in A$ è una formula Σ_1^1 e mostreremo che vale il converso.

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer

Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

Codici analitici e formule Σ_1^1

Lemma

Per ogni formula $\Sigma_1^1 \varphi(X)$ ACA_0 dimostra l'esistenza di un codice analitico A tale che $\forall X (\varphi(X) \leftrightarrow X \in A)$.

Dimostrazione.

Esiste una formula $\Sigma_0^0 \theta(\sigma, \tau)$ tale che ACA_0 dimostra $\forall X (\varphi(X) \leftrightarrow \exists f \forall m \theta(X[m], f[m]))$.

Sia A l'insieme della successioni $\langle (\xi_i, n_i) : i < m \rangle$ con $\xi_i < 2$ tali che $\theta(\langle \xi_i : i < m' \rangle, \langle n_i : i < m' \rangle)$ per ogni $m' \leq m$.

Per ogni $X \in 2^{\mathbb{N}}$, $X \in A \leftrightarrow \exists f \forall m \theta(X[m], f[m])$. \square

Lemma

Per ogni formula $\Sigma_1^1 \varphi(n, X)$ ACA_0 dimostra $\exists \langle A_n : n \in \mathbb{N} \rangle \forall n (A_n \text{ è un c.an.} \wedge \forall X (\varphi(n, X) \leftrightarrow X \in A_n))$.

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici

CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

Formule Π_1^1 e alberi

Se A è un codice analitico e $X \in 2^{\mathbb{N}}$ sia $T_A(X)$ l'albero
 $\{\tau \in \mathbb{N}^{<\mathbb{N}} \mid A(X \upharpoonright |\tau|, \tau)\}$.

$T_A(X)$ ha un cammino se e solo se $X \in A$.

Lemma

Per ogni formula Π_1^1 $\psi(X)$ ACA_0 dimostra l'esistenza di un codice analitico A tale che

$$\forall X (\psi(X) \leftrightarrow \text{WO}(\text{KB}(T_A(X)))).$$

Dimostrazione.

Sia $\varphi = \neg\psi$, che è Σ_1^1 . Sia A un codice analitico tale che
 $\forall X (\varphi(X) \leftrightarrow X \in A)$.

Quindi $\forall X (\varphi(X) \leftrightarrow T_A(X) \text{ ha un cammino})$ e perciò
 $\forall X (\psi(X) \leftrightarrow \text{WO}(\text{KB}(T_A(X))))$. □

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer

Insiemi analitici
CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-}CA_0$

Altri
sottosistemi

Un interessante corollario

Teorema

Se $\varphi(X)$ è una formula Σ_1^1 ACA₀ dimostra
$$\neg \forall X (\varphi(X) \leftrightarrow \text{WO}(X)).$$

Dimostrazione.

Supponiamo per assurdo che $\forall X (\varphi(X) \leftrightarrow \text{WO}(X))$ e utilizziamo un procedimento diagonale.

Sia $\psi(X)$ la formula “ X è un c.an. $\wedge \neg \varphi(\text{KB}(T_X(X)))$ ”.

$\psi(X)$ è Π_1^1 ed esiste un codice analitico A tale che
$$\forall X (\psi(X) \leftrightarrow \text{WO}(\text{KB}(T_A(X))))).$$

Si ottiene $\psi(A) \leftrightarrow \neg \psi(A)$, la contraddizione cercata. □

Il sistema
ATR₀

Confrontabilità
dei buoni
ordini

Le definizioni
ATR₀ dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
ATR₀

Altri risultati

Il sistema
 Π_1^1 -CA₀

Altri
sottosistemi

CWO₀

Il sistema
ATR₀

Confrontabilità
dei buoni
ordini

Le definizioni
ATR₀ dimostra
CWO
L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
ATR₀

Altri risultati

Il sistema
 Π_1^1 -CA₀

Altri
sottosistemi

Indichiamo con **CWO₀** la teoria RCA₀ + CWO.

Sappiamo che ATR₀ implica CWO₀ e il nostro obiettivo è ottenere l'implicazione inversa.

Il primo passo è mostrare che CWO₀ implica ACA₀.

CWO₀ implica ACA₀

Teorema (CWO₀)

ACA₀.

Dimostrazione.

Mostriamo in RCA₀ che CWO implica che l'immagine di una funzione iniettiva f è un insieme.

Sia $Y = \{ (m, n) \mid f(m) \leq f(n) \}$.

LO(Y) è immediato e, usando Σ_1^0 -comprensione limitata, si verifica che ogni segmento iniziale finito di Y è finito.

Perciò WO(Y).

Confrontando l'ordine standard su \mathbb{N} e Y si ottiene una $g : \mathbb{N} \rightarrow \mathbb{N}$ tale che $\forall n, m (n \leq m \leftrightarrow f(g(n)) \leq f(g(m)))$.

Allora per ogni k vale

$$\exists n f(n) = k \leftrightarrow \exists m \leq k f(g(m)) = k.$$



Il sistema
ATR₀

Confrontabilità
dei buoni
ordini

Le definizioni
ATR₀ dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici

CWO implica
ATR₀

Altri risultati

Il sistema
 Π_1^1 -CA₀

Altri
sottosistemi

Principio di Σ_1^1 -limitatezza

Lemma (CWO_0)

Se $\varphi(X)$ è una formula Σ_1^1 tale che $\forall X(\varphi(X) \rightarrow WO(X))$ allora

$$\exists Y(WO(Y) \wedge \forall X(\varphi(X) \rightarrow X \leq Y)).$$

Dimostrazione.

Se la conclusione è falsa CWO implica che

$$\forall Y(WO(Y) \rightarrow \exists X(\varphi(X) \wedge X \geq Y)).$$

Perciò $\forall Y(WO(Y) \leftrightarrow LO(Y) \wedge \exists X(\varphi(X) \wedge X \geq Y))$.

Quindi $WO(Y)$ è equivalente ad una formula Σ_1^1 , che in ACA_0 è una contraddizione. □

Il sistema ATR_0

Confrontabilità dei buoni ordini

Le definizioni ATR_0 dimostra CWO

L'ordine di Kleene-Brouwer
Insiemi analitici
 CWO implica ATR_0

Altri risultati

Il sistema $\Pi_1^1-CA_0$

Altri sottosistemi

Sottordini

Se $LO(X)$, un sottordine di X è $X \cap (A \times A)$ per qualche $A \subseteq \text{fld}(X)$.

Lemma (CWO₀)

Se $WO(X)$, $WO(Y)$ e Y è isomorfo a un sottordine di X , allora $X \geq Y$.

Dimostrazione.

Se la conclusione è falsa CWO implica che $X < Y$.

Questo implica che X sia isomorfo ad un suo segmento iniziale. Sia $g : \text{fld}(X) \rightarrow \{i \mid i <_X k\}$ l'isomorfismo.

Definendo per ricorsione $f(0) = k$, $f(n+1) = g(f(n))$ si ha $\forall n f(n+1) <_X f(n)$, contro $WO(X)$. □

Il sistema
ATR₀

Confrontabilità
dei buoni
ordini

Le definizioni
ATR₀ dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
CWO implica
ATR₀

Altri risultati

Il sistema
 $\Pi^1_1\text{-CA}_0$

Altri
sottosistemi

L'albero a doppia discesa

Definizione (RCA_0)

Se $LO(X)$ e $LO(Y)$ l'**albero a doppia discesa** $T(X, Y)$ è l'insieme di successioni $\langle (m_i, n_i) : i < k \rangle$ tali che $m_{i+1} <_X m_i$ e $n_{i+1} <_Y n_i$ per ogni $i < k - 1$.

Scriviamo $X \star Y$ per l'ordine lineare $KB(T(X, Y))$.

Lemma (ACA_0 , e quindi CWO_0)

Se $WO(X)$ e $LO(Y)$ allora $WO(X \star Y)$.

Dimostrazione.

Se $\neg WO(X \star Y)$ l'albero $T(X, Y)$ ha un cammino e le prime componenti delle sue successioni sono una catena discendente in X , contraddicendo $WO(X)$. □

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
 CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
 CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1-CA_0$

Altri
sottosistemi

Proprietà dell'albero a doppia discesa

Lemma (CWO_0)

Se $WO(X)$, $LO(Y)$ e $\neg WO(Y)$ allora $X \leq X \star Y$.

Dimostrazione.

Sia $T(X) = \{ \sigma \mid \forall i < |\sigma| - 1 (\sigma(i+1) <_X \sigma(i)) \}$ l'albero di discesa in X . Sia g una catena discendente in Y .

Definiamo $f : fld(X) \rightarrow T(X)$ ponendo

$$f(m) = \min_{KB} \{ \sigma \in T(X) \mid \sigma(|\sigma| - 1) = m \}.$$

Se $m <_X \ell$ si ha $f(m) \leq_{KB} f(\ell) \wedge \langle m \rangle <_{KB} f(\ell)$.

Quindi f è un isomorfismo tra X e un sottordine di $KB(T(X))$, che implica $X \leq KB(T(X))$.

$\sigma \mapsto \langle (\sigma(i), g(i)) : i < |\sigma| \rangle$ è un isomorfismo tra $KB(T(X))$ e un sottordine di $X \star Y$, così che $KB(T(X)) \leq X \star Y$.

Combinando i due isomorfismi, si ha $X \leq X \star Y$. □

Somme di buoni ordini

Definizione (RCA_0)

Se $\text{LO}(X)$ e $\text{LO}(Y)$ definiamo

$$\begin{aligned} X + Y = & \{ (2m, 2n) \mid m, n \in \text{fld}(X) \wedge m \leq_X n \} \cup \\ & \cup \{ (2m + 1, 2n + 1) \mid m, n \in \text{fld}(Y) \wedge m \leq_Y n \} \cup \\ & \cup \{ (2m, 2n + 1) \mid m \in \text{fld}(X) \wedge n \in \text{fld}(Y) \}. \end{aligned}$$

Se $\langle X_i : i \in \mathbb{N} \rangle$ è una successione di ordini lineari definiamo

$$\begin{aligned} \sum_i X_i = & \{ ((m, i), (n, i)) \mid m, n \in \text{fld}(X_i) \wedge m \leq n \} \cup \\ & \cup \{ ((m, i), (n, j)) \mid m \in \text{fld}(X_i) \wedge n \in \text{fld}(X_j) \wedge i < j \}. \end{aligned}$$

Infine se $\text{LO}(X)$ poniamo $X \cdot \mathbb{N} = \sum_i X$.

In RCA_0 si ha $\text{LO}(X + Y)$, $X \leq X + Y$ (RCA_0 non dimostra $Y \leq X + Y$) e $\text{LO}(\sum_i X_i)$.

Se si parte da buoni ordini, si ottengono buoni ordini.

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici

CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

Verso la Σ_1^1 -separazione in CWO_0

Siano $\varphi_0(n)$ e $\varphi_1(n)$ formule Σ_1^1 con $\neg\exists n(\varphi_0(n) \wedge \varphi_1(n))$.

Usando gli alberi e l'ordine di Kleene-Brouwer esistono successioni $\langle X_n : n \in \mathbb{N} \rangle$ e $\langle Y_n : n \in \mathbb{N} \rangle$ di ordini lineari tali che $\forall n(\varphi_0(n) \leftrightarrow \neg\text{WO}(X_n))$ e $\forall n(\varphi_1(n) \leftrightarrow \neg\text{WO}(Y_n))$.

Quindi per ogni n vale $\text{WO}(X_n) \vee \text{WO}(Y_n)$.

$$\psi(Z) \leftrightarrow \exists X \exists n(\text{LO}(X) \wedge \neg\text{WO}(X_n) \wedge Z = X \star Y_n)$$

è Σ_1^1 e tutti gli Z che la soddisfano sono buoni ordini (perché se $\neg\text{WO}(X_n)$ allora $\text{WO}(Y_n)$ e quindi $\text{WO}(X \star Y_n)$).

Per il principio di Σ_1^1 -limitatezza sia U un buon ordine tale che $\forall Z(\psi(Z) \rightarrow Z < U)$.

Per ogni n poniamo $Z_n = (U + X_n) \star Y_n$, in modo che

$$\forall n((\neg\text{WO}(X_n) \rightarrow Z_n < U) \wedge (\neg\text{WO}(Y_n) \rightarrow U \leq Z_n)).$$

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
 CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici
 CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Altri
sottosistemi

CWO₀ dimostra Σ_1^1 -separazione

$$\forall n((\varphi_0(n) \rightarrow Z_n < U) \wedge (\varphi_1(n) \rightarrow U \leq Z_n)).$$

$Z = U \vee \exists n Z = Z_n$ è Σ_1^1 e per il principio di Σ_1^1 -limitatezza esiste un buon ordine V tale che $U < V \wedge \forall n Z_n < V$.

Identificando U con l'immagine della mappa di confronto, possiamo assumere che U sia un segmento iniziale di V .

Notiamo che $Z_n + V \cdot \mathbb{N} = V + V \cdot \mathbb{N}$ per ogni n , perché ognuno è isomorfo a un sottordine dell'altro, e poniamo

$$W_0 = \sum_n (Z_n + V \cdot \mathbb{N}) \text{ e } W_1 = \sum_n (V + V \cdot \mathbb{N}).$$

Per CWO esiste $f : W_0 = W_1$. Sia f_n la restrizione di f a $Z_n + V \cdot \mathbb{N}$, che ha immagine $V + V \cdot \mathbb{N}$.

$Z_n < U$ se e solo se l'immagine di Z_n secondo f_n è un segmento iniziale di U .

Quindi $S = \{n \mid Z_n < U\}$ esiste per ACA₀.

Allora si ha $\forall n((\varphi_0(n) \rightarrow n \in S) \wedge (\varphi_1(n) \rightarrow n \notin S))$.

Il sistema
ATR₀

Confrontabilità
dei buoni
ordini

Le definizioni
ATR₀ dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici

CWO implica
ATR₀

Altri risultati

Il sistema
 Π_1^1 -CA₀

Altri
sottosistemi

Reverse mathematics di CWO e di Σ_1^1 -limitatezza

Teorema (RCA_0)

Sono equivalenti:

- 1 ATR_0 ;
- 2 CWO;
- 3 *il principio di Σ_1^1 -limitatezza.*

Abbiamo dimostrato $1 \leftrightarrow 2$ e, nel corso della dimostrazione, anche $2 \rightarrow 3$.

$3 \rightarrow 2$: se X e Y sono buoni ordini, per Σ_1^1 -limitatezza esiste Z tale che $X < Z$ e $Y < Z$.

Combinando i due isomorfismi troviamo la mappa di confronto tra X e Y .

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Le definizioni
 ATR_0 dimostra
CWO

L'ordine di
Kleene-Brouwer
Insiemi analitici

CWO implica
 ATR_0

Altri risultati

Il sistema
 $\Pi_1^1-CA_0$

Altri
sottosistemi

Altra reverse mathematics per ATR_0

Teorema (RCA_0)

Sono equivalenti ad ATR_0 :

- 1 *il teorema dell'insieme perfetto: ogni sottoinsieme chiuso e più che numerabile di \mathbb{R} ha un sottoinsieme perfetto;*
- 2 *il teorema di separazione di Lusin: due sottoinsiemi analitici di \mathbb{R} disgiunti sono separati da un Boreliano;*
- 3 *il dominio di un sottoinsieme Boreliano di \mathbb{R}^2 con al più un valore per ogni elemento è Boreliano;*
- 4 *il teorema di Ulm: due p -gruppi abeliani ridotti numerabili che hanno gli stessi invarianti di Ulm sono isomorfi;*
- 5 *il teorema di forma normale di Cantor per buoni ordini;*
- 6 *i giochi infiniti con payoff aperto sono determinati;*
- 7 *gli insiemi aperti hanno la proprietà di Ramsey.*

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 $\Pi^1_1\text{-CA}_0$

Altri
sottosistemi

$\Pi_1^1\text{-CA}_0$

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Assiomi
 ω -modelli
Alcuni risultati

Altri
sottosistemi

Ricordiamo che le formule Π_1^1 sono quelle della forma $\forall X \psi$ dove ψ è aritmetica.

Gli assiomi di $\Pi_1^1\text{-CA}_0$ sono quelli di RCA_0 più lo schema di Π_1^1 -comprensione:
se φ è Π_1^1 e X non è libera in φ

$$\exists X \forall n (n \in X \leftrightarrow \varphi(n))$$

$\Pi_1^1\text{-CA}_0$ dimostra la comprensione per le combinazioni Booleane di Π_1^1 formule, e in particolare per le formule Σ_1^1 .

ω -modelli di $\Pi_1^1\text{-CA}_0$

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Assiomi
 ω -modelli
Alcuni risultati

Altri
sottosistemi

Teorema

Se S è un ω -modello di RCA_0 (cioè un ideale di Turing), sono equivalenti:

- 1 S è un β -modello di $\Pi_1^1\text{-CA}_0$;
- 2 S è chiuso per iperjump, cioè se $X \in S$ e Y è definibile da una formula Σ_1^1 con parametro X , allora $Y \in S$.

Questo implica che esiste il più piccolo β -modello di $\Pi_1^1\text{-CA}_0$.

Viceversa, non esiste il più piccolo ω -modello di $\Pi_1^1\text{-CA}_0$ e **HYP** è l'intersezione di tutti gli ω -modelli di $\Pi_1^1\text{-CA}_0$.

Reverse mathematics per $\Pi_1^1\text{-CA}_0$, 1

Teorema (RCA_0)

Sono equivalenti a $\Pi_1^1\text{-CA}_0$:

- 1 *il teorema di Cantor-Bendixson: ogni sottoinsieme chiuso di \mathbb{R} è unione di un insieme numerabile e di un insieme perfetto;*
- 2 *il teorema di Silver: ogni relazione di equivalenza Boreliana su \mathbb{R} che ha una quantità più che numerabile di classi di equivalenza ha un insieme perfetto di elementi non-equivalenti;*
- 3 *ogni sottoinsieme numerabile del duale di uno spazio di Banach separabile ha un più piccolo sottospazio chiuso nella topologia *debole che lo contiene;*
- 4 *Ogni sottospazio di $\ell_1 = c_0^*$ chiuso rispetto alla norma ha una chiusura nella topologia *debole.*

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 $\Pi_1^1\text{-CA}_0$

Assiomi
 ω -modelli
Alcuni risultati

Altri
sottosistemi

Reverse mathematics per Π_1^1 -CA₀, 2

Teorema (RCA₀)

Sono equivalenti a Π_1^1 -CA₀:

- 5 ogni gruppo abeliano numerabile è la somma diretta di un gruppo divisibile e di un gruppo ridotto;*
- 6 il teorema di Mal'tsev: ogni gruppo ordinato ha tipo d'ordine $\mathbb{Z}^\alpha \mathbb{Q}^\varepsilon$ dove α è un ordinale e $\varepsilon \in \{0, 1\}$;*
- 7 i giochi infiniti con payoff unione di un aperto e di un chiuso sono determinati;*
- 8 Gli insiemi G_δ (intersezioni numerabili di aperti) hanno la proprietà di Ramsey.*

Il sistema
ATR₀

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 Π_1^1 -CA₀

Assiomi
 ω -modelli

Alcuni risultati

Altri
sottosistemi

Altri sottosistemi sotto ACA_0

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 $\Pi_1^1-CA_0$

Altri
sottosistemi

$WWKL_0$ (Weak Weak König Lemma) è intermedio tra RCA_0 e WKL_0 : è equivalente a diversi enunciati in teoria della misura.

Il teorema della base di Hilbert è equivalente in RCA_0 all'asserzione che l'ordine lineare ω^ω (opportunamente definito) è un buon ordine.

Varie conseguenze di RT^2 sono state studiate e si è visto che non sono equivalenti a RT^2 , pur non essendo non dimostrabili in WKL_0 . Tra questi c'è per esempio l'enunciato "ogni ordine lineare infinito ha una catena ascendente o una catena discendente".

Altri sottosistemi sopra ACA_0

ACA_0^+ è un “piccolo” rafforzamento di ACA_0 : è equivalente all’esistenza di certi invarianti per algebre di Boole.

Alcuni teoremi combinatoriali sono dimostrabili in ACA_0^+ e implicano ACA_0 : il loro status preciso è un problema aperto.

Un teorema sugli ordini lineari indecomponibili è intermedio tra ACA_0^+ (e teorie più forti) e $\Delta_1^1-CA_0$.

Questo teorema è l’unico esempio di origine matematica di un *enunciato di analisi iperaritmetica*, cioè tale che il suo più piccolo ω -modello è **HYP**.

Un teorema di metrizzazione per spazi topologici è equivalente a $\Pi_2^1-CA_0$.

Il sistema
 ATR_0

Confrontabilità
dei buoni
ordini

Altri risultati

Il sistema
 $\Pi_1^1-CA_0$

Altri
sottosistemi