Che cos'è la logica?

Luca Motto Ros

Dipartimento di Matematica "G. Peano" — Università di Torino

Milano, 5-6 maggio 2016

Materiale: dispense del prof. Andretta reperibili all'indirizzo

`http://www.logicatorino.altervista.org/materiale/Elementi.pdf`

Esperimenti e dimostrazioni

Nella maggior parte delle discipline scientifiche (ad esempio fisica, chimica, biologia...) per stabilire la verità di un'affermazione si ricorre a misurazioni, esperimenti o simulazioni: se gli esperimenti, magari fatti più volte e da più persone, confermano l'affermazione questa viene accettata (almeno temporaneamente), altrimenti viene rifiutata.

In matematica, questo "metodo scientifico" **non funziona!!**

Ad esempio, nessun esperimento potrà mai stabilie se $\sqrt{2}$ sia un numero razionale...

Esperimenti e dimostrazioni

Controllare alcuni casi specifici (= misurazioni, esperimenti o simulazioni) può essere utile per avere indizi sulla verità o meno di un'affermazione, ma a volte questi indizi possono anche essere fuorvianti...

Esempio

Congettura: $991 \cdot n^2 + 1$ non è mai un quadrato perfetto (ovvero la sua radice quadrata non è un numero intero).

Si è dimostrato che tale congettura è falsa, anzi ci sono infiniti numeri del tipo $991 \cdot n^2 + 1$ che sono quadrati perfetti. Tuttavia, il più piccolo di tali numeri è

$$\mathbf{12055735790331359447442538767} \approx 1,2 \cdot 10^{28}$$

Quindi controllare la congettura con qualche esempio (non enorme) ci avrebbe erroneamente indotti a crederla vera...

Esperimenti e dimostrazioni

In matematica, per stabilire la verità di un'affermazione (= teorema) si deve ricorrere a una dimostrazione.

Teorema: è l'affermazione (riguardante numeri, funzioni, enti geometrici, o altri oggetti matematici) che si vuole dimostrare. Di solito è della forma

"Se valgono certe ipotesi, allora anche la tesi del teorema è vera."

Esempio: Se $f : \mathbb{R} \to \mathbb{R}$ è una funzione derivabile, allora f è continua.

Attenzione! Spesso ci sono delle assunzioni "nascoste", ovvero gli **assiomi** della teoria in cui si sta lavorando.

Dimostrazione: catena di ragionamenti che a partire dalle ipotesi ci permette di concludere che anche la tesi deve essere vera.

...ma come facciamo a essere sicuri che il ragionamento fatto sia corretto?

Esperimenti e dimostrazioni

Come facciamo a essere sicuri che il ragionamento fatto sia corretto?

La logica matematica

La logica si occupa di analizzare i ragionamenti (= dimostrazioni) e permette di garantirne la correttezza...

...ma a volte permette anche di stabilire
se una certa affermazione è dimostrabile oppure no
PRIMA che un'eventuale dimostrazione venga effettivamente scovata!

Com'è possibile?

Linguaggi del prim'ordine

Si introducono linguaggi (necessariamente artificiali) che ci permettono di studiare "matematicamente" dimostrazioni, sistemi di assiomi teorie, ecc...

Attenzione!

È importante tenere ben distinte la *sintassi* (= struttura "grammaticale" del discorso) dalla *semantica* (= "significato" dei simboli che usiamo nelle formule).

Un **linguaggio L del prim'ordine** è costituito da due gruppi di simboli:

Simboli logici: sono le parti invariabili del discorso, come congiunzioni, quantificazioni, ecc... (questi simboli sono comuni a tutti i linguaggi e non dipendono in alcun modo dall'argomentazione specifica che si sta svolgendo)

Simboli non logici: questi simboli dipendono dal tipo di oggetti matematici che si vogliono studiare (gruppi, anelli, spazi metrici, ecc...) e sono divisi in simboli di funzione, di relazione e di costante.

Simboli logici:

$x, y, z \ldots \ v_0, v_1, v_2 \ \ldots$	*variabili*
$\forall x \ \ldots$	per ogni x ...
$\exists x \ \ldots$	esiste (almeno un) x tale che ...
$\ldots \wedge \ldots$	... e ... (*congiunzione*)
$\ldots \vee \ldots$	... oppure ... (*disgiunzione*)
$\neg \ldots$	non ... (*negazione*)
$\ldots \Rightarrow \ldots$	se ... allora ... (*implicazione*)
$\ldots \iff \ldots$	... se e solo se ... (*bi-implicazione*)
$\ldots = \ldots$	*uguaglianza* tra termini

Per semplificare la lettura si usano anche altri simboli (che di per sé si potrebbero eliminare) come parentesi, virgole, ecc...

Linguaggi del prim'ordine

Simboli non logici:

- **Predicati**: $P, Q, \ldots \rightsquigarrow$ proprietà degli oggetti, relazioni tra di essi, ecc...
- **Funzioni**: $f, g, \ldots \rightsquigarrow$ operazioni, ecc...
- **Costanti**: $c, d, \ldots \rightsquigarrow$ nomi "propri" di oggetti, ecc...

Ciascun simbolo di predicato o funzione è accompagnato dalla sua arietà, un numero naturale che ne indica il numero di argomenti (funzioni/relazioni unarie, binarie, ecc...). I predicati unari si chiamano anche **proprietà**.

Di solito, un linguaggio del prim'ordine L è identificato con l'elenco dei suoi simboli non logici:

$$L = (P, Q, \ldots f, g, \ldots, c, d, \ldots)$$

Linguaggi del prim'ordine

Esempi

- **Linguaggio dei gruppi:** $L_{gp} = (\cdot, ^{-1}, 1)$, dove $\cdot$ è un simbolo di funzione binario, $^{-1}$ è un simbolo di funzione unario, e 1 è un simbolo di costante; nel caso di gruppi abeliani spesso si usa il linguaggio $L_{agp} = \{+, -, 0\}$.
- **Linguaggio di anelli/campi:** $L_{rng} = (+, -, \cdot, 0)$, dove $+$ e $\cdot$ sono simboli di funzione binari, $-$ è un simbolo di funzione unario, e 0 è un simbolo di costante.
- **Linguaggio degli ordini:** $L_{ord} = (\leq)$, dove $\leq$ è un simbolo di relazione binario.

Sintassi: termini

A partire da variabili, simboli di costante e simboli di funzione si costruiscono i **termini**.

Definizione

Un **termine** del linguaggio L è una stringa finita di simboli di L costruita utilizzando le seguenti regole di costruzione.

- Le variabili e i simboli di costante (visti come stringhe di lunghezza 1) sono termini.
- Se f è un simbolo di funzione di L di arietà $n \in \mathbb{N}$ e $t_1, \ldots, t_n$ sono termini, allora anche

$$f(t_1, \ldots, t_n)$$

è un termine.

Sintassi: termini

Termini = variabili, costanti, applicazione di funzioni ad altri termini.

Esempi

1. Sia $L = \{P, f, g, c\}$ con P relazione binaria, f funzione binaria, g funzione unaria, e c costante. Allora le seguenti stringhe sono termini:

$$x \qquad c \qquad g(c) \qquad f(x, c) \qquad f(g(c), f(x, c))$$

2. Sia $L_{urng} = (+, -, \cdot, 0, 1)$ il linguaggio degli anelli con unità: allora i termini di L_{rng} sono (essenzialmente) i polinomi a coefficienti interi. Ad esempio, il polinomio

$$2x^2 - x + 3$$

è un'abbreviazione per il termine

$$(((x \cdot x) + (x \cdot x)) + (-x)) + ((1 + 1) + 1)$$

Sintassi: formule atomiche

Le formule atomiche di un linguaggio L sono i "mattoni" con cui si costruiscono formule più complesse.

Definizione

Una **formula atomica** del linguaggio L è una stringa finita di simboli di L costruita utilizzando le seguenti regole di costruzione.

- Se P è un simbolo di relazione di L di arietà $n \in \mathbb{N}$ e $t_1, \ldots, t_n$ sono termini di L, allora

  $$P(t_1, \ldots, t_n)$$

  è una formula atomica.
- Se t_0 e t_1 sono termini di L allora

  $$t_0 = t_1$$

  è una formula atomica.

Sintassi: formule atomiche

Formule atomiche = relazioni tra termini o uguaglianza tra termini.

Esempi

1. Sia $L = \{P, f, g, c\}$ con P relazione binaria, f funzione binaria, g funzione unaria, e c costante. Allora le seguenti stringhe sono formule atomiche:

$$P(x, y) \qquad P(c, f(x)) \qquad P(f(x, c), f(g(c), f(x, c)))$$

2. Sia $L_{urng} = (+, -, \cdot, 0, 1)$ il linguaggio degli anelli con unità: le formule atomiche di L_{rng} sono (essenzialmente) le equazioni a coefficienti interi. Ad esempio, l'equazione

$$x^2 = 2x - 1$$

è un'abbreviazione per la formula atomica

$$x \cdot x = (x + x) + (-1)$$

Sintassi: formule e enunciati

Definizione

Una **formula** del linguaggio L è una stringa finita di simboli di L costruita utilizzando le seguenti regole di costruzione.

- Le formule atomiche sono formule.
- Se φ è una formula, anche $\neg\varphi$ lo è.
- Se φ e ψ sono formule e $\star$ è un connettivo binario ($\wedge, \vee, \Rightarrow, \Longleftrightarrow$), allora $(\varphi \star \psi)$ è una formula.
- Se φ è una formula, v è una variabile, e Q è un quantificatore ($\forall, \exists$), allora $Qv\,\varphi$ è una formula.

Un'occorrenza di una variabile v si dice *vincolata* se cade sotto il raggio d'azione di un quantificatore Q (ultima clausola della definizione), altrimenti si dice *libera*. La scrittura $\varphi(x_1, \ldots, x_n)$ indica che le variabili che occorrono libere in φ sono tra le $x_1, \ldots, x_n$. Una formula φ priva di variabili libere si dice **enunciato**, e spesso si denota con σ.

Sintassi: formule e enunciati

Esempi

1. Linguaggio: $L = \{P, f, g, c\}$. Le seguenti stringhe sono formule:

$$\forall x\, P(x, y) \qquad \exists y(P(c, f(y)) \Rightarrow \forall z\, P(z, y)) \qquad P(c, c) \wedge \neg P(c, f(c))$$

2. Linguaggio: $L_{urng} = (+, -, \cdot, 0, 1)$. L'enunciato

$$\exists x\, (x \cdot x = (x + x) + (-1))$$

asserisce l'esistenza di una soluzione dell'equazione polinomiale

$$x^2 = 2x - 1$$

Formalizzazione

Formalizzare una frase in un linguaggio L significa "tradurre" la frase dal linguaggio naturale ad un'opportuna formula/enunciato del linguaggio L.

Esempio

Le formalizzazione del teorema di Euclide

Esistono numeri primi arbitrariamente grandi.

nel linguaggio $L = (\leq, |, 1)$, dove $\leq$ è il simbolo binario per l'ordine, $|$ è il simbolo binario per la divisibilità ($x \mid y \rightsquigarrow$ "x divide y"), e 1 è un simbolo per l'unità è data dalla formula

$$\forall x \, \exists y \, (x \leq y \, \wedge \, \forall z \, (z \mid y \Rightarrow (z = 1 \vee z = y)))$$

(L-)Strutture

Definizione

Sia $L = (P, \dots f, \dots c, \dots)$ un linguaggio del prim'ordine. Una L-**struttura** $\mathcal{M}$ è una tupla

$$\mathcal{M} = (M, P^{\mathcal{M}}, \dots f^{\mathcal{M}}, \dots c^{\mathcal{M}}, \dots)$$

dove:

- M è un insieme, detto **dominio** (o **universo** o **supporto**) di $\mathcal{M}$;
- $P^{\mathcal{M}}$ è una relazione n-aria su M, ovvero un sottoinsieme di $M^n = \underbrace{M \times \dots \times M}_{n \text{ volte}}$, dove $n \in \mathbb{N}$ è l'arietà di P;
- $f^{\mathcal{M}}$ è una funzione da M^n in M, dove $n \in \mathbb{N}$ è l'arietà di f;
- $c^{\mathcal{M}}$ è un elemento di M.

(L-)Strutture

Esempi

- Sia $L = (f, c)$ con f simbolo di funzione binaria e c simbolo di costante. Sono L-strutture

$$(\mathbb{N}, +, 0) \qquad (\mathbb{R}, \cdot, \sqrt{2}) \qquad (\mathbb{C}, x^y, i) \qquad \dots$$

- Sia $L = (P, Q)$ con P simbolo di relazione binaria e Q simbolo di relazione unaria. Sono L-strutture

$$(\mathbb{R}, \leq, \mathbb{Q}) \qquad (\mathbb{N}, |, \mathrm{Prime}) \qquad \dots$$

dove $|$ è la relazione di divisibilità e Prime è l'insieme dei numeri primi.

Attenzione!

Una struttura è determinata sia dal suo dominio che dalle sue relazioni, funzioni e costanti: le L-strutture $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}, \cdot, 0)$ sono tutte distinte!

Esempio: spazi metrici come strutture del prim'ordine

Come si può vedere uno spazio metrico (X, d) come L-struttura in un opportuno linguaggio L?

Attenzione! Non si può semplicemente introdurre un simbolo di funzione per la distanza d: la metrica non è una funzione da X^2 in X, ma una funzione da X^2 in $\mathbb{R}$.

Una possibilità è considerare il linguaggio $L_0 = (P_r)_{r \in \mathbb{R}_{\geq 0}}$ con un simbolo di relazione binaria P_r per ogni reale non negativo r, e vedere (X, d) come la L_0-struttura $\mathcal{X} = (X, (P_r^{\mathcal{X}})_{r \in \mathbb{R}_{\geq 0}})$ dove

$$P_r^{\mathcal{X}} = \{(a, b) \in X^2 \mid d(a, b) = r\}.$$

In questo modo $d(a, b) = r$ se e solo se $(a, b) \in P_r^{\mathcal{X}}$.

Esempio: spazi metrici come strutture del prim'ordine

È possibile utilizzare un linguaggio più piccolo (ovvero numerabile)?

Consideriamo il linguaggio $L_1 = (R_q)_{q\in\mathbb{Q}_{>0}}$ dove ciascun R_q è un simbolo di relazione binaria. Allora possiamo vedere (X, d) come la L_1-struttura $\mathcal{X} = (X, (R_q^{\mathcal{X}})_{q\in\mathbb{Q}_{>0}})$ dove

$$R_q^{\mathcal{X}} = \{(a, b) \in X^2 \mid d(a, b) < q\}.$$

Ora si ha $d(a, b) = \inf\{q \in \mathbb{Q}_{>0} \mid (a, b) \in R_q^{\mathcal{X}}\}$.

(L-)Strutture

Analogamente, si può vedere uno spazio vettoriale V su un campo $\mathbb{K}$ come una L-struttura $\mathcal{V}$ nel linguaggio

$$L = (+, 0, (f_k)_{k \in \mathbb{K}})$$

dove i simboli $+$ e 0 danno la struttura di gruppo di V, e ciascuna f_k è una funzione unaria interpretata in

$$f_k^{\mathcal{V}} \colon V \to V \qquad v \mapsto kv.$$

Collettivamente, le f_k corrispondono al prodotto scalare di V.

Attenzione!

Non si può rappresentare il prodotto scalare con una singola funzione (binaria), perché esso è una mappa da $V \times \mathbb{K}$ in V.

Isomorfismi

La nozione di "isomorfismo" è una nozione di identificazione tra L-strutture.

Definizione

Siano $\mathcal{M}$ e $\mathcal{N}$ due L-strutture con linguaggio $L = (P, \dots f, \dots c, \dots)$. Un **isomorfismo** tra $\mathcal{M}$ e $\mathcal{N}$ è una mappa $F\colon M \to N$ tale che

1. F è biettiva: $F(a) \neq F(b)$ se $a \neq b$, e $\mathrm{range}(F) = N$;
2. F preserva tutte le relazioni/funzioni/costanti, ovvero per ogni $a_1, \dots, a_n, b_1, \dots, b_m \in M$

$$P^{\mathcal{M}}(a_1, \dots, a_n) \text{ se e solo se } P^{\mathcal{N}}(F(a_1), \dots, F(a_n))$$
$$F(f^{\mathcal{M}}(b_1, \dots, b_m)) = f^{\mathcal{N}}(F(b_1), \dots, F(b_m))$$
$$F(c^{\mathcal{M}}) = c^{\mathcal{N}}$$

$\mathcal{M}$ ed $\mathcal{N}$ si dicono **isomorfe** se esiste un isomorfismo tra di esse; in questo caso scriviamo $M \cong N$.

Isomorfismi

Esempi

- Isomorfismi tra strutture algebriche: gruppi, anelli, ...
- Le strutture $(\mathbb{R}, +, 0)$ e $(\mathbb{R}_{>0}, \cdot, 1)$ sono isomorfe via $x \mapsto e^x$.
- Le strutture $(\mathbb{N}, <)$ e $(\mathbb{Z}, <)$ non sono isomorfe: la prima ha un elemento minimo, la seconda no.
- Le strutture $(\mathbb{Z}, <)$ e $(\mathbb{Q}, <)$ non sono isomorfe: entrambe non hanno minimo e massimo, ma la seconda è un ordine lineare denso mentre la prima non lo è.
- Le strutture $(\mathbb{Q}, <)$ e $(\mathbb{R}, <)$ non sono isomorfe: entrambe sono ordini lineari densi senza minimo e massimo, ma la prima è una struttura numerabile mentre la seconda non lo è.

Osservazione

Spesso per dimostrare che due L-strutture **non** sono isomorfe si osserva che una soddisfa una certa proprietà (esprimibile in L) ma l'altra no.

Semantica: interpretazione di formule/enunciati

Intuitivamente, interpretare una L-formula φ in una data L-struttura $\mathcal{M}$ significa:

- sostituire i simboli non logici $P, \dots f, \dots c, \dots$ con le corrispettive interpretazioni $P^{\mathcal{M}}, \dots f^{\mathcal{M}}, \dots c^{\mathcal{M}}, \dots$ in $\mathcal{M}$;
- interpretare i simboli logici $\neg, \wedge, \vee, \Rightarrow, \iff, \forall, \exists$ con il loro significato naturale (non, e, o, se ... allora ..., se e solo se, per ogni, esiste);
- controllare se la risultante proprietà è verificata in $\mathcal{M}$ o meno.

Esempio

Sia $L = (R)$ con R simbolo di relazione binario, e sia σ l'enunciato

$$\exists x \, \forall y \, R(x, y).$$

L'interpretazione di σ nella L-struttura $\mathcal{N}_0 = (\mathbb{N}, \leq)$ asserisce l'esistenza di un elemento minimo, mentre l'interpretazione di σ nella L-struttura $\mathcal{N}_1 = (\mathbb{N}, \geq)$ asserisce l'esistenza di un elemento minimo: dunque σ è vero in $\mathcal{N}_0$ ma falso in $\mathcal{N}_1$.

Semantica: interpretazione di termini

Fissiamo un linguaggio $L = (P, \dots f, \dots c, \dots)$ e una L-struttura $\mathcal{M} = (M, P^{\mathcal{M}}, \dots f^{\mathcal{M}}, \dots c^{\mathcal{M}}, \dots)$.

Definizione

Sia t un termine di L contenente le variabili $x_1, \dots, x_n$. L'**interpretazione** di t in $\mathcal{M}$ è la funzione n-aria

$$t^{\mathcal{M}} \colon M^n \to M$$

che associa a $(a_1, \dots, a_n) \in M^n$ il valore $t^{\mathcal{M}}(a_1, \dots, a_n)$ ottenuto rimpiazzando i simboli di funzione e di costante con le corrispettive funzioni e costanti di $\mathcal{M}$.

Esempio

Il termine t dato da $x \cdot (y \cdot y) + ((x \cdot y) + 1)$ nel linguaggio degli anelli unitari definisce una funzione polinomiale $R^2 \to R$ in ogni anello unitario R, che associa ad $(a, b) \in R^2$ l'elemento $ab^2 + ab + 1_R$ di R.

Semantica: interpretazione di enunciati

Definizione

Dato un L-enunciato σ, consideriamo la pseudo-formula $\sigma^{\mathcal{M}}$ ottenuta rimpiazzando i simboli $P, \dots f, \dots c, \dots$ con le relazioni $P^{\mathcal{M}}, \dots$, funzioni $f^{\mathcal{M}}, \dots$, ed elementi $c^{\mathcal{M}} \in M$, e limitando tutti i quantificatori ad M. Diremo che $\mathcal{M}$ **soddisfa** σ, o che $\mathcal{M}$ è un **modello** di σ, in simboli

$$\mathcal{M} \models \sigma,$$

se $\sigma^{\mathcal{M}}$ afferma un fatto vero in $\mathcal{M}$. Per questa ragione $\mathcal{M} \models \sigma$ si legge spesso come: σ è vero in $\mathcal{M}$. Quanto non succede che $\mathcal{M} \models \sigma$, scriveremo $\mathcal{M} \not\models \sigma$.

Semantica: interpretazione di enunciati

Osserviamo che

la scrittura ...	equivale a dire ...
$\mathcal{M} \models \neg\sigma$	$\mathcal{M} \not\models \sigma$
$\mathcal{M} \models \sigma \wedge \tau$	$\mathcal{M} \models \sigma$ e $\mathcal{M} \models \tau$
$\mathcal{M} \models \sigma \vee \tau$	$\mathcal{M} \models \sigma$ oppure $\mathcal{M} \models \tau$
$\mathcal{M} \models \sigma \Rightarrow \tau$	se $\mathcal{M} \models \sigma$ allora $\mathcal{M} \models \tau$
$\mathcal{M} \models \sigma \iff \tau$	$\mathcal{M} \models \sigma$ se e solo se $\mathcal{M} \models \tau$

Semantica: interpretazione di enunciati

Esempio

Sia $L = (f, g, c)$ un linguaggio con f simbolo di funzione binario, g simbolo di funzione binario, e c simbolo di costante. Sia $\mathcal{M}$ una L-struttura.

- Sia σ_1 l'enunciato $\forall x \, \forall y \, \forall z \, (f(x, f(y, z)) = f(f(x, y), z))$.
  Allora $\mathcal{M} \models \sigma_1$ se e solo se $f^{\mathcal{M}}$ è un'operazione associativa.
- Sia σ_2 l'enunciato $\forall x \, (f(x, c) = x \wedge f(c, x) = x)$.
  Allora $\mathcal{M} \models \sigma_2$ se e solo se $c^{\mathcal{M}}$ è l'elemento neutro rispetto a $f^{\mathcal{M}}$.
- Sia σ_3 l'enunciato $\forall x \, (f(x, g(x)) = c \wedge f(g(x), x) = c)$.
  Allora $\mathcal{M} \models \sigma_3$ se e solo se $g^{\mathcal{M}}(a)$ è l'inverso di $a \in M$ rispetto a $f^{\mathcal{M}}$.

Dunque $\mathcal{M} \models \sigma_1 \wedge \sigma_2 \wedge \sigma_3$ se e solo se $\mathcal{M}$ è un gruppo.

$\mathcal{M}$ è un gruppo abeliano se e solo se soddisfa anche

$$\forall x \, \forall y \, (f(x, y) = f(y, x))$$

Definizione

Un enunciato σ è (**logicamente**) **valido** o una **tautologia** se $\mathcal{M} \models \sigma$ per ogni L-struttura $\mathcal{M}$, in simboli

$$\models \sigma.$$

Un enunciato σ è **insoddisfacibile** o una **contraddizione** se $\mathcal{M} \not\models \sigma$ per ogni L-struttura $\mathcal{M}$, ovvero se $\models \neg\sigma$.

Ad esempio, l'enunciato

$$\forall x\,(x = x)$$

è una tautologia. Similmente, se σ e τ sono enunciati arbitrari, allora l'enunciato

$$(\sigma \wedge (\sigma \Rightarrow \tau)) \Rightarrow \tau \qquad (\textit{Modus ponens})$$

è una tautologia.

$\mathcal{M}$ è un **modello** di un insieme di L-enunciati Σ se $\mathcal{M} \models \sigma$ per ogni $\sigma \in \Sigma$, in simboli $\mathcal{M} \models \Sigma$.

Definizione

Un enunciato τ è **conseguenza logica** di Σ, in simboli

$$\Sigma \models \tau,$$

se e solo se $\mathcal{M} \models \Sigma$ implica che $\mathcal{M} \models \tau$, per ogni L-struttura $\mathcal{M}$. Quando $\Sigma = \{\sigma\}$ diremo che τ è conseguenza logica di σ, in simboli $\sigma \models \tau$. Equivalentemente: τ è conseguenza logica di σ se $\sigma \Rightarrow \tau$ è un enunciato valido.

Due enunciati σ e τ si dicono **logicamente equivalenti** se uno è conseguenza logica dell'altro, cioè se $\sigma \models \tau$ e $\tau \models \sigma$; equivalentemente, se $\sigma \iff \tau$ è un enunciato valido.

Definizione

Un insieme di enunciati Σ è **soddisfacibile** se ha almeno un modello, cioè se c'è una L-struttura $\mathcal{M}$ tale che $\mathcal{M} \models \Sigma$. Altrimenti Σ si dice **insoddisfacibile**.

Proposizione

$$\Sigma \models \tau \quad \text{se e solo se} \quad \Sigma \cup \{\neg\tau\} \text{ è insoddisfacibile.}$$

Dimostrazione.

Supponiamo $\Sigma \cup \{\neg\tau\}$ sia insoddisfacibile. Se $\mathcal{M}$ è un modello di Σ, allora $\mathcal{M} \not\models \neg\tau$, quindi $\mathcal{M} \models \tau$. Poiché $\mathcal{M}$ è arbitrario, ne segue che $\Sigma \models \tau$.
L'altra implicazione è immediata. □

Equivalenza elementare e isomorfismi

Definizione

Due L-strutture $\mathcal{M}$ e $\mathcal{N}$ si dicono **elementarmente equivalenti**, $\mathcal{M} \equiv \mathcal{N}$ in simboli, se per ogni L-enunciato σ

$$\mathcal{M} \models \sigma \quad \text{se e solo se} \quad \mathcal{N} \models \sigma.$$

Proposizione

Se $\mathcal{M} \cong \mathcal{N}$, allora $\mathcal{M} \equiv \mathcal{N}$ (ma non viceversa).

Questo spiega il criterio che abbiamo utilizzato per dimostrare che due strutture $\mathcal{M}$ e $\mathcal{N}$ **non** sono isomorfe: se esiste una proprietà esprimibile mediante un enunciato σ che vale in $\mathcal{M}$ ma non in $\mathcal{N}$, allora $\mathcal{M}$ e $\mathcal{N}$ **non** sono logicamente equivalenti e quindi nemmeno isomorfe.

Esempio: $\mathcal{M} = (\mathbb{Q}, <)$, $\mathcal{N} = (\mathbb{Z}, <)$ e σ l'enunciato

$$\forall x \, \forall y \, (x < y \Rightarrow \exists z \, (x < z \wedge z < y)).$$

Equivalenza elementare e isomorfismi

Esempio

Le strutture $\mathcal{R} = (\mathbb{R}, +, \cdot, 0, 1)$ e $\mathcal{C} = (\mathbb{C}, +, \cdot, 0, 1)$ **non** sono isomorfe, poiché l'enunciato

$$\exists x\,(((x \cdot x) + x) + 1 = 0)$$

è vero in $\mathcal{C}$ ma non in $\mathcal{R}$ (l'equazione $x^2 + x + 1 = 0$ non ha soluzioni in $\mathbb{R}$, ma definisce una curva algebrica in $\mathbb{C}$).

Tuttavia, si dimostra ad esempio che due ordini lineari densi senza primo e ultimo elemento sono sempre elementarmente equivalenti: quindi si ha che

$$(\mathbb{Q}, \leq) \equiv (\mathbb{R}, \leq),$$

ma

$$(\mathbb{Q}, \leq) \not\cong (\mathbb{R}, \leq)$$

poiché le due strutture hanno cardinalità diversa.

Insiemi di verità

Abbiamo visto che cosa vuol dire che un enunciato è vero in una struttura, ma che dire delle formule che non sono enunciati?

In generale, una formula $\varphi(x_1, \ldots, x_n)$ definisce un insieme di n-uple di elementi della struttura che, sostituiti al posto delle variabili $x_1, \ldots, x_n$, rendono vera φ nella struttura.

Definizione

Una n-upla $(a_1, \ldots, a_n)$ di elementi di $\mathcal{M}$ soddisfa la formula $\varphi(x_1, \ldots, x_n)$, in simboli

$$\mathcal{M} \models \varphi[a_1, \ldots, a_n],$$

se sostituendo ciascuna variabile x_i con a_i (e interpretando tutti i simboli non logici in $\mathcal{M}$) si ottiene una pseudo-formula vera in $\mathcal{M}$.
L'**insieme di verità** di φ in $\mathcal{M}$ è il sottoinsieme di M^n

$$\{(a_1, \ldots, a_n) \in M^n \mid \mathcal{M} \models \varphi[a_1, \ldots, a_n]\}.$$

Insiemi di verità

Esempio

Sia $L = (f)$ un linguaggio con un solo simbolo di funzione binario. Consideriamo la L-struttura $\mathcal{N} = (\mathbb{N}, \cdot)$ e la L-formula $\varphi(x)$

$$\forall y \, \forall z \, (f(y, z) = x \Rightarrow (y = x \vee z = x)).$$

Un numero $n \in \mathbb{N}$ soddisfa $\varphi(x)$ in $\mathcal{N}$ se e solo ogni volta che n si può scrivere come prodotto di due numeri, uno di questi due risulta uguale a n. Dunque l'insieme di verità di φ in $\mathcal{N}$ è

$$\{0, 1\} \cup \{p \mid p \text{ è primo}\}.$$

Se vogliamo che l'insieme di verità sia solo l'insieme dei numeri primi, possiamo "aggiungere" a $\varphi(x)$ altre formule che escludano i casi 0 e 1, ad esempio:

$$\varphi(x) \wedge \exists y \, \neg(f(y, x) = x) \wedge \neg \forall y (f(x, y) = y).$$

Insiemi di verità

Esempio

Consideriamo ora la L-formula

$$\exists z\,(f(x,z)=y).$$

Siccome contiene le variabili libere x, y, il suo insieme di verità in $(\mathbb{N},\cdot)$ sarà un sottoinsieme di $\mathbb{N}^2$, e precisamente

$$\{(n,m)\in\mathbb{N}^2 \mid n \text{ divide } m\}.$$

Altri esempi

- L'insieme di verità di $x\cdot x<1$ in $(\mathbb{N},\cdot,<,1)$ è il singoletto $\{0\}$, mentre in $(\mathbb{R},\cdot,<,1)$ è l'intervallo aperto $(-1;1)$.
- L'insieme di verità in $\mathbb{R}$ di $y=x^2-3x+2$ è una parabola, cioè un sottoinsieme di $\mathbb{R}^2$ (più in generale, disegnare il grafo di una funzione equivale a calcolare un insieme di verità).

Definibilità

Definizione

Sia $\mathcal{M}$ una L-struttura. Un sottoinsieme A di M^n si dice **definibile** (in L) se esiste una L-formula $\varphi(x_1, \ldots, x_n)$ il cui insieme di verità in $\mathcal{M}$ coincide con A.

Gli esempi precedenti mostrano che l'insieme dei numeri primi e la relazione (binaria) di divisibilità sono definibili in $(\mathbb{N}, \cdot)$.

Esempi

- L'insieme dei reali non negativi è definibile in $(\mathbb{R}, \cdot)$, e l'ordinamento usuale su $\mathbb{R}$ è definibile in $(\mathbb{R}, +, \cdot)$.
- L'insieme dei numeri naturali e l'ordinamento usuale sono definibili in $(\mathbb{Z}, +, \cdot)$.

Tuttavia, né l'insieme dei numeri naturali né l'ordinamento sono definibili in $(\mathbb{Z}, +)$... ma come si può dimostrare che un insieme **non** è definibile?

Indefinibilità

Proposizione

Sia $F\colon \mathcal{M} \to \mathcal{N}$ un isomorfismo. Allora per ogni formula $\varphi(x_1, \ldots, x_n)$ e ogni $a_1, \ldots, a_n \in M$ si ha che

$$\mathcal{M} \models \varphi[a_1, \ldots, a_n] \quad \text{se e solo se} \quad \mathcal{N} \models \varphi[F(a_1), \ldots, F(a_n)].$$

Poiché $\mathcal{M}$ è un modello dell'enunciato $\forall x\, \varphi(x)$ (risp., $\exists x\, \varphi(x)$) se e solo se l'insieme di verità di $\varphi(x)$ è tutto M (risp., è non vuoto), si ottiene

Corollario

Se $\mathcal{M} \cong \mathcal{N}$, allora $\mathcal{M} \equiv \mathcal{N}$.

Corollario

Se F è un **automorfismo** di $\mathcal{M}$ (ovvero un isomorfismo $F\colon \mathcal{M} \to \mathcal{M}$) e $A \subseteq M^n$ è definibile, allora $F(A) = A$, dove

$$F(A) = \{(F(a_1), \ldots, F(a_n)) \in M^n \mid a_1, \ldots, a_n \in M\}.$$

Indefinibilità

Corollario

Se F è un **automorfismo** di $\mathcal{M}$, allora $F(A) = A$ per ogni insieme $A \subseteq M^n$ definibile (ovvero F **fissa** A).

Se dato $A \subseteq M^n$ riusciamo a trovare un automorfismo di $\mathcal{M}$ che **non** fissa A, allora A **non** è definibile. (Ma il viceversa non vale!)

Esempio

L'insieme $\mathbb{N}$ non è definibile in $(\mathbb{Z}, +)$ poiché l'automorfismo

$$z \mapsto -z$$

non fissa $\mathbb{N}$ (manda i numeri naturali nei numeri non positivi). Lo stesso automorfismo testimonia che $\leq$ non è definibile in $(\mathbb{Z}, +)$.

Esempio

Consideriamo il linguaggio $L = (R)$ contenente un solo simbolo di relazione binario R. Consideriamo le seguenti due relationi binarie su $\mathbb{N}$:

- **divisibilità**: $n \mid m$ se e solo se n divide m
- **coprimalità**: $n \perp m$ se e solo se $MCD(n, m) = 1$.

Allora $\perp$ è definibile nella L-struttura $(\mathbb{N}, |)$ mediante la formula

$$\forall z \left((z \mid x \wedge z \mid y) \Rightarrow \forall w \, (z \mid w) \right).$$

... continua ...

Indefinibilità

Tuttavia, $|$ non è definibile nella $\mathcal{L}$-struttura $(\mathbb{N}, \perp)$. Dato $0 \neq n \in \mathbb{N}$, sia $p_0^{m_0} p_1^{m_1} \dots p_k^{m_k}$ la sua scomposizione in fattori primi, con $p_0 < p_1 < \dots < p_k$ e $m_i \neq 0$ per ogni $1 \leq i \leq k$. Definiamo

$$F(n) = \begin{cases} n & \text{se } p_0 \neq 2 \text{ oppure } n_0 > 2 \\ p_0^2 \, p_1^{m_1} \dots p_k^{m_k} & \text{se } p_0 = 2 \text{ e } m_0 = 1 \\ p_0^1 \, p_1^{m_1} \dots p_k^{m_k} & \text{se } p_0 = 2 \text{ e } m_0 = 2. \end{cases}$$

Allora F è un automorfismo di $(\mathbb{N}, \perp)$ che non fissa $|$ poiché, ad esempio, 2 divide 4, ma $F(2) = 4$ non divide $F(4) = 2$.

Indefinibilità

Se un insieme è definibile è anche fissato da tutti gli automorfismi, ma...

Attenzione!

Non è vero che se un sottoinsieme di M^n è fissato da tutti gli automorfismi, allora è definibile!

Basta considerare una qualunque struttura **rigida** (ovvero il cui unico automorfismo sia l'identità) **infinita**, ad esempio $(\mathbb{N}, \leq)$. Allora ogni sottoinsieme della struttura è fissato da tutti gli automorfismi (rigidità!). Tuttavia, ci sono al più una quantità numerabile di formule (e quindi di insiemi definibili), ma una quantità più che numerabile di sottoinsiemi della struttura: quindi almeno uno di questi non è definibile.

Ci sono tecniche più sofisticate per dimostrare che un insieme **non** è definibile. Ad esempio, si può dimostrare che l'insieme degli elementi di torsione di un gruppo non è definibile utilizzando il **Teorema di compattezza** per la logica del prim'ordine...

Teorie e assiomi

Definizione

- Una **teoria (del prim'ordine)** è un insieme T di enunciati di un linguaggio del prim'ordine L, che si dice linguaggio di T.
- Un **sistema di assiomi** per una teoria T è un insieme Σ di enunciati del linguaggio di T tale che per ogni enunciato σ

$$\Sigma \models \sigma \quad \text{se e solo se} \quad T \models \sigma.$$

- T è **finitamente assiomatizzabile** se ammette un sistema di assiomi finito.

1. La teoria dei gruppi. Sistema di assiomi: $\Sigma_{gp} = \{\sigma_1, \sigma_2, \sigma_3\}$.
2. La teoria degli ordini lineari densi è (finitamente) assiomatizzabile.
3. Data una qualunque L-struttura $\mathcal{M}$ possiamo considerare la sua teoria

$$\mathrm{Th}(\mathcal{M}) = \{\sigma \mid \mathcal{M} \models \sigma\}.$$

Teorie complete

Definizione

Sia T una teoria nel linguaggio L.

- T si dice **soddisfacibile** (o **coerente** o **consistente**) se $\mathcal{M} \models T$ per qualche L-struttura $\mathcal{M}$.
- T si dice **completa** se è soddisfacibile e $T \models \sigma$ oppure $T \models \neg\sigma$ per ogni L-enunciato σ.
- Un L-enunciato σ è **indipendente** da T se esistono due L-strutture $\mathcal{M}_0, \mathcal{M}_1$ che soddisfano T e tali che

$$\mathcal{M}_0 \models \sigma \quad \text{e} \quad \mathcal{M}_1 \models \neg\sigma.$$

In particolare, T **non** è completa se e solo se esiste un L-enunciato σ indipendente da T.

Teorie (in)complete

Esempio

La teoria Σ_{gp} dei gruppi è incompleta. L'enunciato

$$\forall x \, \forall y \, (x \cdot y = y \cdot x)$$

è indipendente da Σ_{gp} poiché ci sono gruppi abeliani e gruppi non abeliani.

Più in generale...

Teorie (in)complete

Dato $n \in \mathbb{N}$, sia $\varepsilon_{\geq n}$ l'enunciato

$$\exists x_0 \ldots \exists x_{n-1} \Big(\bigwedge_{i<j<n} \neg(x_i = x_j) \Big)$$

che asserisce l'esistenza di almeno n elementi, e sia $\varepsilon_{=n}$ l'enunciato

$$\varepsilon_{\geq n} \wedge \neg \varepsilon_{n+1}.$$

Esempio

Se T è una teoria completa che ha un modello finito di taglia n, allora $T \models \varepsilon_{=n}$, e quindi ogni modello di T è finito di taglia n. Quindi le teorie dei gruppi (abeliani o no), degli anelli, dei campi, ... non sono complete.

Teorie (in)complete

Esempio

Sia $L_\emptyset$ il linguaggio vuoto e $T_\emptyset$ la teoria vuota (le $L_\emptyset$-strutture sono tutti gli insiemi, e tutte soddisfano $T_\emptyset$).

La teoria $T_\emptyset$ non è completa: l'enunciato $\varepsilon_{\geq n}$ è indipendete da $T_\emptyset$.

Tuttavia ciascuna teoria $T_n = \{\varepsilon_{=n}\}$ è completa.

Teorie (in)complete

Teorema

Sia L un linguaggio con una quantità numerabile di simboli non logici e sia T una L-teoria soddisfacibile che ha solo modelli infiniti. Supponiamo ci sia un modello $\mathcal{M}$ di T tale che ogni modello $\mathcal{N}$ di T di ugual taglia di $\mathcal{M}$ è isomorfo a $\mathcal{M}$. Allora T è una teoria completa.

Esempi

- La teoria $T_\infty = \{\varepsilon_{\geq n} \mid n \in \mathbb{N}\}$ che assiomatizza gli insiemi infiniti è completa.
- Per un teorema di Cantor, due ordini lineari densi numerabili senza primo e ultimo elemento sono isomorfi (infatti, sono isomorfi a $\mathbb{Q}$). Quindi la teoria T_{DLO} degli ordini lineari densi senza primo e ultimo elemento è completa.

  Nota bene. La teoria degli ordini lineari densi **non** è completa: "avere un minimo" è un enunciato indipendente da tale teoria.

Completezza e equivalenza elementare

Proposizione

Se T è una teoria soddisfacibile, le seguenti affermazioni sono equivalenti:

1. T è completa;
2. due modelli di T sono elementarmente equivalenti.

Dimostrazione.

($\Rightarrow$) Sia $\mathcal{M}$ un modello di T e sia σ un L-enunciato: dalla definizione di teoria completa segue che $T \models \sigma$ se e solo se $\mathcal{M} \models \sigma$. Sia $\mathcal{N}$ un altro modello di T. Se $\mathcal{M} \models \sigma$ allora $T \models \sigma$, da cui $\mathcal{N} \models \sigma$; viceversa, se $\mathcal{M} \not\models \sigma$ allora $\mathcal{M} \models \neg\sigma$, da cui $\mathcal{N} \models \neg\sigma$, perciò $\mathcal{N} \not\models \sigma$.

($\Leftarrow$) Se T è soddisfacibile ma $T \not\models \sigma$ e $T \not\models \neg\sigma$ allora ci sono $\mathcal{M}$ e $\mathcal{M}'$ modelli di T tali che $\mathcal{M} \models \sigma$ e $\mathcal{M}' \models \neg\sigma$. □

Completezza e equivalenza elementare

Proposizione

Se T è una teoria soddisfacibile, le seguenti affermazioni sono equivalenti:

1. T è completa;
2. due modelli di T sono elementarmente equivalenti.

Corollario

$\mathrm{Th}(\mathcal{M})$ è completa per ogni L-struttura $\mathcal{M}$.

Corollario

Due ordini lineari densi senza primo e ultimo elemento (come $(\mathbb{Q}, <)$ e $(\mathbb{R}, <)$) sono elementarmente equivalenti.

Classi di strutture (finitamente) assiomatizzabili

Data una teoria T, poniamo

$$\mathrm{Mod}(T) = \{\mathcal{M} \mid \mathcal{M} \models T\}.$$

Definizione

Una classe $\mathcal{C}$ di L-strutture si dice **assiomatizzabile** se $\mathcal{C} = \mathrm{Mod}(T)$ per qualche teoria T; se T può essere presa finita, diremo che $\mathcal{C}$ è **finitamente assiomatizzabile**.

Ad esempio, la classe dei gruppi finiti è (finitamente) assiomatizzabile? Che dire della classe dei gruppi privi di torsione?

Teorema di compattezza

Un insieme Σ di enunciati è **finitamente soddisfacibile** se ogni $\Sigma_0 \subseteq \Sigma$ finito è soddisfacibile.

Teorema di compattezza

Sia L un linguaggio del prim'ordine e sia Σ un insieme di L-enunciati. Se Σ è finitamente soddisfacibile, allora Σ è soddisfacibile.

Corollario

Sia L un linguaggio del prim'ordine, sia Σ un insieme di L-enunciati e sia τ un L-enunciato. Se $\Sigma \models \tau$, allora c'è un insieme finito $\Sigma_0 \subseteq \Sigma$ tale che $\Sigma_0 \models \tau$.

Dimostrazione.

$\Sigma \models \tau$ se e solo se $\Sigma \cup \{\neg\tau\}$ è insoddisfacibile. Per compattezza c'è un insieme finito $\Sigma_0 \subseteq \Sigma$ tale che $\Sigma_0 \cup \{\neg\tau\}$ è insoddisfacibile, il che è equivalente a dire $\Sigma_0 \models \tau$. □

Strutture finite e infinite

Teorema

Sia Σ un insieme di L-enunciati che ha modelli finiti di taglia arbitrariamente grande. Allora Σ ha un modello infinito.

Dimostrazione.

Ciascun insieme $\Sigma \cup \{\varepsilon_{\geq n} \mid n < k\}$ è soddisfacibile: per compattezza esiste un modello $\mathcal{M}$ di $\Sigma \cup \{\varepsilon_{\geq n} \mid n \in \mathbb{N}\}$. Quindi $\mathcal{M}$ è un modello di Σ infinito. □

In particolare, la classe dei gruppi (anelli, campi...) finiti **non** è assiomatizzabile.

Teorie non finitamente assiomatizzabili

Teorema

Sia T una teoria del prim'ordine in un linguaggio L e sia $\{\sigma_i \mid i \in \mathbb{N}\}$ un suo sistema di assiomi. Supponiamo che per ogni n ci sia un $m > n$ tale che $\{\sigma_0, \ldots, \sigma_n\} \not\models \sigma_m$. Allora T non è finitamente assiomatizzabile.

Dimostrazione.

Supponiamo per assurdo che $\{\tau_0, \ldots, \tau_n\}$ sia un sistema finito di assiomi per T, e sia τ l'enunciato $\bigwedge_{i \leq n} \tau_i$. Poiché $\{\sigma_i \mid i \in \mathbb{N}\} \models \tau$, per compattezza esiste $n \in \mathbb{N}$ tale che $\{\sigma_0, \ldots, \sigma_n\} \models \tau$. Sia m come nelle ipotesi del teorema: poiché $\{\sigma_0, \ldots, \sigma_n\} \models \tau$ e $\tau \models \sigma_m$ (essendo $\{\tau\}$ un sistema di assiomi per T), si avrebbe $\{\sigma_0, \ldots, \sigma_n\} \models \sigma_m$, contraddizione. □

Teorie non finitamente assiomatizzabili

Esempio

La teoria T dei gruppi infiniti è assiomatizzata da $\Sigma_{gp} \cup \{\varepsilon_{\geq i} \mid i \in \mathbb{N}\}$. Tuttavia, dato $n \in \mathbb{N}$ si ha che $\mathbb{Z}/n\mathbb{Z}$ soddisfa $\Sigma_{gp} \cup \{\varepsilon_{\geq i} \mid i \leq n\}$ ma non soddisfa $\varepsilon_{\geq n+1}$: quindi T non è finitamente assiomatizzabile.

Esempio

La teoria T dei gruppi privi di torsione non è finitamente assiomatizzabile.

Infatti, sia τ_n l'enunciato

$$\forall x\,(\neg(x = 1) \Rightarrow \neg(x^n = 1)),$$

dove x^n abbrevia $\underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ volte}}$. Allora $\Sigma_{gp} \cup \{\tau_i \mid i \in \mathbb{N}\}$ è un sistema di assiomi per T. Dato $n \in \mathbb{N}$, sia $p > n$ primo: allora $\mathbb{Z}/p\mathbb{Z}$ soddisfa $\Sigma_{gp} \cup \{\tau_i \mid i \leq n\}$ ma non soddisfa τ_p. Quindi T non è finitamente assiomatizzabile.

Classi di strutture non assiomatizzabili

Abbiamo visto che la classe dei gruppi finiti **non** è assiomatizzabile.

Esempio

La classe dei gruppi in cui tutti gli elementi hanno torsione **non** è assiomatizzabile. Per assurdo, sia T una assiomatizzazione nel linguaggio $L_{gp} = (\cdot, ^{-1}, 1)$ per tale classe. Consideriamo il linguaggio $L = L_{gp} \cup \{c\}$, e sia ρ_n l'L-enunciato $\neg(c^n \neq 1)$. Allora i gruppi $\mathbb{Z}/p\mathbb{Z}$ (per p primo sufficientemente grande) testimoniano che $T_\infty = T \cup \{\rho_n \mid n \in \mathbb{N}\}$ è finitamente soddisfacibile: basta interpretare c nella classe di resto di $p-1$. Quindi esiste un modello $\mathcal{M}$ di T_∞, che è un gruppo in cui c viene interpretato in un elemento di ordine ∞. Dunque $\mathcal{M}$, vista come L_{gp}-struttura, soddisfa T ma ha elementi di ordine ∞.

Quindi non esiste una L_{gp}-formula $\varphi(x)$ tale che il suo insieme di verità in un arbitrario gruppo è l'insieme dei suoi elementi di torsione: se esistesse, $\Sigma_{gp} \cup \{\forall x\, \varphi(x)\}$ sarebbe un'assiomatizzazione per la classe dei gruppi in cui tutti gli elementi hanno torsione.

Classi di strutture non assiomatizzabili

Un ordine lineare $(L, <)$ è **ben fondato** se non contiene catene decrescenti infinite $a_0 > a_1 > a_2 > \dots$

Esempio

Gli ordini lineari ben fondati non sono assiomatizzabili.

Supponiamo per assurdo che Σ_{WO} sia un sistema di assiomi per gli ordini lineari (stretti) ben fondati nel linguaggio $L_{LO} = \{<\}$. Espandiamo L_{LO} al linguaggio $L^*_{LO} = (\leq, (c_i)_{i\in\mathbb{N}})$, dove ciascun c_i è un simbolo di costante. Sia σ_i l'L^*_{LO}-enunciato $c_{i+1} < c_i$. Ciascun $\Sigma_{WO} \cup \{\sigma_i \mid i < n\}$ è soddisfacibile dalla struttura $\mathcal{N}_n$ di dominio $\mathbb{N}$ con l'ordine usuale e

$$c_i^{\mathcal{N}} = \begin{cases} n - i & \text{se } i \leq n \\ i & \text{se } i > n. \end{cases}$$

Per compattezza, esiste $\mathcal{M} \models \Sigma_{WO} \cup \{\sigma_i \mid i \in \mathbb{N}\}$: ma i $c_i^{\mathcal{M}}$ formano una catena discendente infinita in $\mathcal{M}$, quindi $\mathcal{M}$ (visto come ordine lineare) non è ben fondato, contraddizione.