Informatica

CdL in Matematica

Parte 3

Roberto Zunino

Definizioni Ricorsive:

Esempi Intuitivi

Esempio

Una definizione informale dei numeri naturali $\mathbb{N}$

1. 0 è un naturale
2. Se n è un naturale, allora anche $n + 1$ è un naturale

Esempio

Una definizione informale dei numeri naturali pari

1. 0 è pari
2. Se n è pari, allora anche $n + 2$ è pari

Esempio

Una definizione informale delle sequenze finite di naturali

1. ϵ è una sequenza
2. Se s è una sequenza ed n è un naturale, allora anche $n : s$ è una sequenza

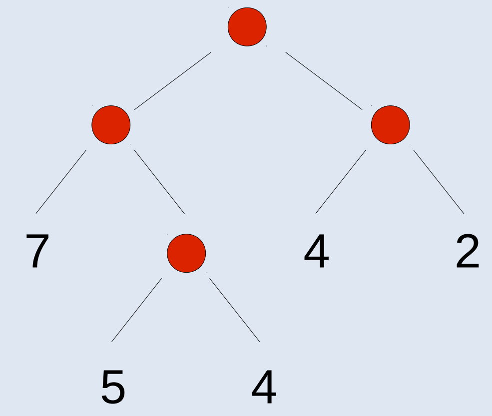
Esempio: $4 : 2 : 7 : 2 : 13 : \epsilon$ è una sequenza

Esempio

Una definizione informale degli alberi (binari) di naturali

1. I naturali sono alberi
2. Se s e d sono alberi, allora anche (s, d) è un albero

Esempio: $((7, (5, 4)), (4, 2))$ è un albero



Esempio

Una definizione informale delle espressioni aritmetiche

1. I naturali sono espressioni
2. Se e_1 e e_2 sono espressioni, allora anche $(e_1 + e_2)$ è un'espressione
3. Se e_1 e e_2 sono espressioni, allora anche $(e_1 - e_2)$ è un'espressione
4. Se e_1 e e_2 sono espressioni, allora anche $(e_1 \cdot e_2)$ è un'espressione

Esempio: $(3 + (5 \cdot 4))$ è un'espressione

Definizioni Ricorsive:

Regole di Inferenza

Regole di Inferenza

Def. Una regola di inferenza (su un insieme universo U) è un elemento di

$$\mathcal{P}^{fin}(U) \times U$$

dove $\mathcal{P}^{fin}(U)$ indica i sottoinsiemi *finiti* di U.

Notazione: una regola arbitraria $\langle \{x_1, \ldots, x_n\}, y \rangle$ viene scritta come

$$\frac{x_1 \quad \ldots \quad x_n}{y}$$

Le x_i sono chiamate *premesse* della regola, mentre y è chiamata *conclusione*.

Regole di Inferenza

Intuitivamente, se stiamo per definire un insieme A, una regola

$$\frac{x_1 \quad \ldots \quad x_n}{y}$$

formalizza il seguente requisito: se tutte le premesse x_i appartengono ad A, allora anche la conclusione y deve appartenerci.

Esempio: per definire i naturali $\mathbb{N}$ usiamo l'insieme di regole

$$\mathcal{R} = \left\{ \frac{}{0} \right\} \cup \left\{ \frac{n}{n+1} \;\middle|\; n \in U \right\}$$

Si noti che lo 0 non ha premesse (perché?)

Regole di Inferenza

Riscriviamo un poco più formalmente gli esempi visti prima:

Naturali $\quad \frac{}{0} \quad \frac{n}{n+1}$

Pari $\quad \frac{}{0} \quad \frac{n}{n+2}$

Sequenze $\quad \frac{}{\epsilon} \quad \frac{s}{n:s}(n \in \mathbb{N})$

Alberi $\quad \frac{}{n}(n \in \mathbb{N}) \quad \frac{s \quad d}{(s,d)}$

Espressioni $\quad \frac{}{n}(n \in \mathbb{N}) \quad \frac{e_1 \quad e_2}{(e_1 + e_2)} \quad \frac{e_1 \quad e_2}{(e_1 - e_2)} \quad \frac{e_1 \quad e_2}{(e_1 \cdot e_2)}$

Conseguenze Immediate

Un insieme di regole di inferenza $\mathcal{R}$ induce una funzione

$$\hat{\mathcal{R}} \in (\mathcal{P}(U) \to \mathcal{P}(U))$$

$$\hat{\mathcal{R}}(X) = \{y \mid \exists(\frac{x_1 \quad \dots \quad x_n}{y}) \in \mathcal{R}.\ x_1, \dots, x_n \in X\}$$

detta *operatore delle conseguenze immediate*.

Intuitivamente, $\hat{\mathcal{R}}(X)$ è l'insieme degli elementi che sono conseguenza di qualche regola (di $\mathcal{R}$) che ha le sue premesse in X.

Esempio

Prendendo $\mathcal{R} = \left\{ \dfrac{x}{x+2} \;\middle|\; x \in \mathbb{R} \right\}$ si ha:

$$\hat{\mathcal{R}}(X) = \{x + 2 \mid x \in X\}$$

$$\hat{\mathcal{R}}(\{1,2,5,7\}) = \{3,4,7,9\}$$
$$\hat{\mathcal{R}}(\emptyset) = \emptyset$$
$$\hat{\mathcal{R}}(\mathbb{N}) = \mathbb{N} \setminus \{0,1\}$$
$$\hat{\mathcal{R}}(\mathbb{Z}) = \mathbb{Z}$$
$$\hat{\mathcal{R}}(\mathbb{Q}) = \mathbb{Q}$$
$$\hat{\mathcal{R}}(\mathbb{R}) = \mathbb{R}$$

Esempio

Prendendo $\mathcal{R} = \left\{ \frac{x \quad y}{x+y} \;\middle|\; x, y \in \mathbb{R} \right\}$ si ha:

$$\hat{\mathcal{R}}(X) = \{x + y \mid x, y \in X\}$$

$$\hat{\mathcal{R}}(\{1,2,5\}) = \{2,3,4,6,7,10\}$$
$$\hat{\mathcal{R}}(\{1,2,3\}) = \{2,3,4,5,6\}$$
$$\hat{\mathcal{R}}(\emptyset) = \emptyset$$
$$\hat{\mathcal{R}}(\mathbb{N}) = \mathbb{N}$$
$$\hat{\mathcal{R}}(\mathbb{N} \setminus \{0\}) = \mathbb{N} \setminus \{0,1\}$$
$$\hat{\mathcal{R}}(\mathbb{Z}) = \mathbb{Z}$$

Esempio

$$\mathcal{R} = \left\{ \frac{x \qquad y}{x+y} \;\middle|\; x, y \in \mathbb{R} \right\} \cup \left\{ \frac{x \qquad y}{xy} \;\middle|\; x, y \in \mathbb{R} \right\}$$

Si ha

$$\hat{\mathcal{R}}(X) = \{x + y \mid x, y \in X\} \cup \{xy \mid x, y \in X\}$$

Esempio

$$\mathcal{R} = \left\{ \frac{}{-2}, \frac{}{3} \right\} \cup \left\{ \frac{x \qquad y}{x+y} \;\middle|\; \underbrace{xy > 0} \right\}$$

condizione a lato

Si ha:

$$\hat{\mathcal{R}}(X) = \{-2, 3\} \cup \{x + y \mid x, y \in X \wedge \overbrace{xy > 0}\}$$

Esempio

Prendendo le regole per gli alberi binari di naturali:

$$\mathcal{R} = \left\{ \frac{}{n} \;\middle|\; n \in \mathbb{N} \right\} \cup \left\{ \frac{s \quad\quad d}{(s,d)} \;\middle|\; s, d \text{ arbitrari} \right\}$$

si ha:

$$\hat{\mathcal{R}}(X) = \mathbb{N} \cup \{(x,y) \mid x, y \in X\}$$

Conseguenze e Inclusioni

La proprietà

$$\hat{\mathcal{R}}(A) \subseteq B$$

vuole dire che, se si parte da premesse in A e si applica una regola qualunque di $\mathcal{R}$, si ottiene una conclusione in B.

In particolare, $\hat{\mathcal{R}}(X) \subseteq X$ indica che X è un insieme *chiuso* sotto le regole $\mathcal{R}$: applicando una qualunque regola con premesse in X si ottiene una conclusione in X.

Esempio

Se prendiamo

$$\mathcal{R} = \left\{ \frac{x \quad y}{x - y} \middle| \, x, y \in \mathbb{R} \right\}$$

Allora, $\hat{\mathcal{R}}(\mathbb{Z}) \subseteq \mathbb{Z}$ vale: la differenza di due interi è sempre un intero.

Analogamente, vale $\hat{\mathcal{R}}(\mathbb{Q}) \subseteq \mathbb{Q}$.

Non vale invece $\hat{\mathcal{R}}(\mathbb{N}) \subseteq \mathbb{N}$: per esempio $3 - 4 \notin \mathbb{N}$ anche se $3, 4 \in \mathbb{N}$.

Conseguenze e Inclusioni

Al contrario, la proprietà

$$A \subseteq \hat{\mathcal{R}}(B)$$

vuole dire che, se si parte da un qualunque elemento di A, questo è conseguenza di una qualche regola di $\mathcal{R}$ applicata a premesse in B.

In particolare, $X \subseteq \hat{\mathcal{R}}(X)$ indica che qualunque elemento di X è ottenibile a partire da premesse in X tramite una regola di $\mathcal{R}$.

Esempio

Se prendiamo

$$\mathcal{R} = \left\{ \frac{x \quad y}{x + y + 1} \;\middle|\; x, y \in \mathbb{R} \right\}$$

Allora, $\mathbb{Z} \subseteq \hat{\mathcal{R}}(\mathbb{Z})$ vale: ogni intero a è della forma $x+y+1$ per qualche x, y interi. Infatti basta prendere $x = a$ e $y = -1$.

Analogamente, vale $\mathbb{Q} \subseteq \hat{\mathcal{R}}(\mathbb{Q})$.

Non vale invece $\mathbb{N} \subseteq \hat{\mathcal{R}}(\mathbb{N})$: infatti $0 \in \mathbb{N}$ ma non esistono x, y naturali tali che $0 = x + y + 1$.

Punti pre-/post-/fissi

Def. Sia $f \in (\mathcal{P}(U) \to \mathcal{P}(U))$.

Diciamo che X è un punto prefisso di f quando vale

$$f(X) \subseteq X$$

Diciamo che X è un punto postfisso di f quando vale

$$X \subseteq f(X)$$

Diciamo che X è un punto fisso di f quando vale

$$f(X) = X$$

Definizioni ricorsive:

Esempio di Formalizzazione

Formalizzazione

Proviamo a formalizzare ora una definizione ricorsiva. Per semplicità, prendiamo quella dei naturali pari.

1. 0 è naturale pari
2. Se n è naturale pari, allora anche $n+2$ è naturale pari

Formalizziamolo in regole:

$$\mathcal{R} = \left\{ \frac{}{0} \right\} \cup \left\{ \frac{x}{x+2} \;\middle|\; x \in U \right\}$$

Come insieme universo U prendiamo per esempio i numeri reali (o qualsiasi altro insieme "abbastanza grande").

Formalizzazione

1. 0 è naturale pari
2. Se n è naturale pari, allora anche $n+2$ è naturale pari

$$\mathcal{R} = \left\{ \frac{}{0} \right\} \cup \left\{ \frac{x}{x+2} \,\middle|\, x \in U \right\} \qquad \hat{\mathcal{R}}(X) = \{0\} \cup \{x+2 \mid x \in X\}$$

Indichiamo con X l'insieme che vogliamo definire.

Osservazione. I requisiti 1 e 2 si riscrivono come

$$\{0\} \subseteq X \qquad \{x+2 \mid x \in X\} \subseteq X$$

e cioè come

$$\hat{\mathcal{R}}(X) \subseteq X$$

In altre parole: vogliamo che X sia un punto prefisso di $\hat{\mathcal{R}}$.

Un Primo Tentativo

$$\mathcal{R} = \left\{ \frac{}{0} \right\} \cup \left\{ \frac{x}{x+2} \;\middle|\; x \in U \right\}$$

Def. (tentativo) L'insieme dei naturali pari X è l'insieme che soddisfa

$$\hat{\mathcal{R}}(X) \subseteq X$$

Purtroppo, la definizione sopra è *mal posta*: ci sono tanti insiemi X che soddisfano l'inclusione sopra.

Per esempio, oltre all'insieme dei naturali pari, abbiamo anche i punti prefissi $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$.

Definizione Corretta

Osserviamo che la soluzione X dell'inclusione $\hat{\mathcal{R}}(X) \subseteq X$ che vogliamo veramente (ovvero l'insieme dei naturali pari) è la *più piccola* tra tutte le soluzioni.

Intuitivamente, "la più piccola X" è quella che contiene solo quegli elementi che sono strettamente necessari per soddisfare i requisiti 1 e 2 da cui eravamo partiti. Quindi:

Def. L'insieme dei naturali pari X è il minimo punto prefisso di $\hat{\mathcal{R}}$.

Dimostreremo che tale insieme minimo X esiste sempre, qualunque sia l'insieme di regole $\mathcal{R}$.

Conclusione

Abbiamo visto che:

- Le definizioni ricorsive sono formalizzabili con regole di inferenza.
- L'insieme che esse vogliono definire è precisamente dato dal minimo punto prefisso dell'operatore delle conseguenze immediate $\hat{\mathcal{R}}$.
- Il minimo punto prefisso è unico (è *minimo*!)

Da dimostrare:

- Il minimo punto prefisso di $\hat{\mathcal{R}}$ esiste sempre.

Punti prefissi
e
Principio di Induzione

Monotonia

Def. Una funzione

$$f \in (\mathcal{P}(U) \to \mathcal{P}(U))$$

è *monotona* se e solo se per ogni $X, Y \in \mathcal{P}(U)$:

$$X \subseteq Y \implies f(X) \subseteq f(Y)$$

Prop. L'operatore $\hat{\mathcal{R}} \in (\mathcal{P}(U) \to \mathcal{P}(U))$ è monotono.
Dim. Sia $y \in \hat{\mathcal{R}}(X)$. Per definizione di $\hat{\mathcal{R}}$, esiste una regola

$$\frac{x_1 \quad \ldots \quad x_n}{y} \in \mathcal{R}$$

con $x_1, \ldots, x_n \in X$. Per ipotesi $X \subseteq Y$, quindi $x_1, \ldots, x_n \in Y$. Concludiamo che $y \in \hat{\mathcal{R}}(Y)$.

Knaster-Tarski

Th. (Punto prefisso di Knaster-Tarski)
Se $f \in (\mathcal{P}(U) \to \mathcal{P}(U))$ è una funzione *monotona*, allora ammette un minimo punto prefisso, cioè un X tale che

$$1)\ f(X) \subseteq X \qquad (X \text{ è punto prefisso})$$

$$2)\ f(Y) \subseteq Y \implies X \subseteq Y \qquad (X \text{ è minimo})$$

Corollario.
Siccome $\hat{\mathcal{R}}$ è monotona, ammette un minimo punto prefisso.

Knaster-Tarski: dimostrazione

Sia $\mathcal{Y}$ la famiglia dei punti prefissi $\{Y \mid f(Y) \subseteq Y\}$.

Il lemma del minimo ci suggerisce di prendere $X = \bigcap \mathcal{Y}$ e controllare che $X \in \mathcal{Y}$: in tal caso, il minimo è proprio X.

$$
\begin{array}{lll}
 & X \text{ è il minimo di } \mathcal{Y} & \\
\Leftarrow & X \in \mathcal{Y} & [\text{Lem. minimo}] \\
\Leftarrow & f(X) \subseteq X & [\text{def. } \mathcal{Y}] \\
\Leftarrow & f(X) \subseteq \bigcap \mathcal{Y} & [\text{def. } X] \\
\Leftarrow & \forall Y \in \mathcal{Y}.\ f(X) \subseteq Y & [\text{prop. } \bigcap] \\
\Leftarrow & \forall Y \in \mathcal{Y}.\ f(X) \subseteq f(Y) \wedge f(Y) \subseteq Y & [\text{transitività}] \\
\Leftarrow & \forall Y \in \mathcal{Y}.\ f(X) \subseteq f(Y) & [\text{def. } \mathcal{Y}] \\
\Leftarrow & \forall Y \in \mathcal{Y}.\ X \subseteq Y & [\text{monot. } f] \\
\Leftarrow & X \subseteq \bigcap \mathcal{Y} & [\text{prop. } \bigcap] \\
\Leftarrow & \text{vero} & [\text{def. } X]
\end{array}
$$

Minimo Punto Prefisso

Def.
Data $f \in \mathcal{P}(U) \to \mathcal{P}(U)$ monotona, indichiamo con

$$\mathsf{fix}(f)$$

il suo minimo punto prefisso.

Principio di Induzione

Questo è il risultato più importante del corso.

Th. (Principio di Induzione)
Sia $f \in \mathcal{P}(U) \to \mathcal{P}(U)$ monotona. Allora, per ogni Y:

$$f(Y) \subseteq Y \implies \mathsf{fix}(f) \subseteq Y$$

Dim. Y è prefisso, e $\mathsf{fix}(f)$ è il minimo prefisso.

Induzione: Esempio

Per esempio, nel caso di

$$\mathcal{R} = \left\{ \frac{}{0} \right\} \cup \left\{ \frac{n}{n+1} \;\middle|\; n \in U \right\}$$

il minimo punto prefisso è $\mathbb{N}$. Il suo principio di induzione è

$$\hat{\mathcal{R}}(Y) \subseteq Y \implies \mathbb{N} \subseteq Y$$

ovvero

$$\left(\begin{array}{l} 0 \in Y \\ \forall n.\ (n \in Y \implies n+1 \in Y) \end{array} \right) \implies \forall n \in \mathbb{N}.\ n \in Y$$

Induzione: Esempio

L'induzione sui pari funziona in modo simile.

$$\mathcal{R} = \left\{ \frac{}{0} \right\} \cup \left\{ \frac{n}{n+2} \;\middle|\; n \in U \right\}$$

Il minimo punto prefisso sono i pari P. Si ha:

$$\hat{\mathcal{R}}(Y) \subseteq Y \implies P \subseteq Y$$

ovvero

$$\left(\begin{array}{l} 0 \in Y \\ \forall n.\ (n \in Y \implies n+2 \in Y) \end{array} \right) \implies \forall n \in P.\ n \in Y$$

Notazione

Per semplificare la notazione, invece di scrivere

$$\mathcal{R} = \left\{ \frac{-}{0} \right\} \cup \left\{ \frac{n}{n+2} \;\middle|\; n \in U \right\}$$

a volte scriviamo solo

$$\frac{}{0} \qquad \frac{n}{n+2}$$

Induzione: Esempio

Sia X l'insieme di naturali definito ricorsivamente da:

$$\frac{}{10} \qquad \frac{n \qquad m}{n \cdot m} \qquad \frac{n \qquad m}{n + m}$$

Per dimostrare

$$\forall n \in X.\ n \text{ è pari}$$

cosa ci basta dimostrare, procedendo per induzione?

Induzione: Esempio

$$\forall n \in X.\ n \text{ è pari}$$

è equivalente a

$$X \subseteq P \qquad \text{dove } P = \{\ n \mid n \text{ pari}\}$$

e quindi, per induzione, è sufficiente che valga

$$\hat{\mathcal{R}}(P) \subseteq P$$

e cioè

$$\begin{aligned} & 10 \text{ è pari} \\ n, m \text{ pari} \implies\ & n \cdot m \text{ pari} \\ n, m \text{ pari} \implies\ & n + m \text{ pari} \end{aligned}$$

Notazione

Per semplificare, invece di

$$\mathcal{R} = \left\{ \frac{x \qquad\qquad y}{x+y} \;\middle|\; x, y \in U \wedge \underbrace{x \cdot y > 0} \right\}$$

scriviamo

$$\frac{x \qquad\qquad y}{x+y}(x \cdot y > 0)$$

o anche, abusando un po',

condizione a lato

$$\frac{x \qquad\qquad y \qquad\qquad x \cdot y > 0}{x+y}$$

Si noti che la condizione a lato non è una premessa, anche se la scriviamo come se fosse tale.

Induzione: Esempio

Sia X l'insieme di interi definito ricorsivamente da:

$$\frac{}{-4} \qquad \frac{}{5} \qquad \frac{x \qquad y}{x+y}\,(x \cdot y > 0)$$

condizione a lato

Per dimostrare

$$\forall z.\ z \in X \implies |z| > 3$$

basta dimostrare che

$$|-4| > 3$$

$$|5| > 3$$

$$|x| > 3 \ \wedge\ |y| > 3 \wedge\ x \cdot y > 0 \implies |x+y| > 3$$

ipotesi induttive

condizione a lato

Induzione: Esempio

Infatti, dalle regole

$$\frac{}{-4} \qquad \frac{}{5} \qquad \frac{x \qquad y}{x+y}(x \cdot y > 0)$$

abbiamo

$$\hat{\mathcal{R}}(Y) = \{-4, 5\} \cup \{x + y \mid x, y \in Y \ \wedge \ x \cdot y \ > 0\}$$

e chiamando $A = \{z \mid |z| > 3\}$ otteniamo per induzione

$$\hat{\mathcal{R}}(A) \subseteq A \implies X \subseteq A$$

che è equivalente a quanto detto prima.

Notazione

A volte quando si definisce un insieme per ricorsione con le regole di inferenza, si menziona l'insieme stesso nelle regole.

Per esempio, definendo i naturali pari P, potremmo scrivere

$$\frac{}{0 \in P} \qquad \frac{n \in P}{n + 2 \in P}$$

o anche, volendo definire l'associata proprietà pari:

$$\frac{}{\mathsf{pari}(0)} \qquad \frac{\mathsf{pari}(n)}{\mathsf{pari}(n + 2)}$$

Questa è solo una notazione alternativa per dire che $P = \mathsf{fix}(\hat{\mathcal{R}})$ (dove $\mathcal{R} = \ldots$) e che pari è la proprietà associata a ciò.

Operativamente

Nelle applicazioni più comuni dell'induzione, ci troviamo a dimostrare un enunciato della forma

$$\forall x.\ p(x) \implies q(x)$$

dove p, q sono proprietà. Interpretando p, q come i loro insiemi associati, possiamo riscrivere l'enunciato come

$$p \subseteq q$$

Se infine p è definito per ricorsione tramite $\mathcal{R}$, per induzione è sufficiente dimostrare che

$$\hat{\mathcal{R}}(q) \subseteq q$$

Operativamente

In termini operativi,

$$\hat{\mathcal{R}}(q) \subseteq q$$

vuole dire che "la proprietà q è preservata da tutte le regole di $\mathcal{R}$".

Concludendo, per ottere il desiderato $p \subseteq q$ è sufficiente esaminare tutte le regole che definiscono p, e per ciascuna fare vedere che, quando vale q su tutte le premesse, allora vale q anche sulla conclusione.

Punti fissi
e
Inversione

Lemma del Minimo Punto Fisso

Lemma. Sia $f \in (\mathcal{P}(U) \to \mathcal{P}(U))$ monotona, e sia $X = \mathsf{fix}(f)$ il minimo punto prefisso di f. Allora, X è anche il minimo punto fisso.

Dim. Dimostriamo che X è un punto fisso di f:

$$
\begin{array}{rll}
 & f(X) \subseteq X & [\text{ipotesi}] \\
\Rightarrow & f(f(X)) \subseteq f(X) & [\text{monotonia di } f] \\
\Rightarrow & f(X) \text{ punto prefisso di } f & [\text{definizione}] \\
\Rightarrow & X \subseteq f(X) & [X \text{ è minimo}] \\
\Rightarrow & X \subseteq f(X) \wedge f(X) \subseteq X & [\text{ipotesi}] \\
\Rightarrow & f(X) = X & [\text{doppia inclusione}]
\end{array}
$$

Infine X è anche minimo: se Y è un punto fisso, allora Y è anche punto prefisso e quindi $X \subseteq Y$ per minimalità.

Conseguenza

Per Knaster-Tarski, data una f monotona, non solo esiste il suo minimo punto prefisso X, ma tale X è anche il suo minimo punto fisso.

In altre parole, l'inclusione $f(X) \subseteq X$ è una uguaglianza quando X è minimo.

Inversione

Corollario. (Inversione)
Sia $\mathcal{R}$ un insieme di regole, e $X = \mathsf{fix}(\hat{\mathcal{R}})$.
Allora, $X \subseteq \hat{\mathcal{R}}(X)$.

Informalmente, questo ci dice che ogni elemento di X è conseguenza di una qualche regola, applicata a elementi di X.

Relazioni Definite per Ricorsione

Relazioni per Ricorsione

Siccome le relazioni sono insiemi di coppie, possiamo usare tutto quello che si è già visto per gli insiemi in generale.

Non c'è bisogno di nessuna teoria aggiuntiva.

Esempio

Una definizione ricorsiva del “minore o uguale” sui naturali

1. Ogni naturale è $\leq$ di se stesso
2. Se vale $n \leq m$, allora vale anche $n \leq (m+1)$

L'intuizione ci dice che abbiamo $5 \leq 5$ dalla 1. Quindi che $5 \leq 6$ dalla 2, da cui $5 \leq 7$, $5 \leq 8$, etc. iterando la 2. Con le regole 1 e 2 intuitivamente possiamo ricavare tutte le diseguaglianze $n \leq m$ che conosciamo.

Formalmente

$$\mathcal{R} = \left\{ \frac{}{\langle n, n\rangle} \;\middle|\; n \in \mathbb{N} \right\} \cup \left\{ \frac{\langle n, m\rangle}{\langle n, m+1\rangle} \;\middle|\; n, m \in \mathbb{N} \right\}$$

La funzione indotta dalle regole sopra è:

$$\hat{\mathcal{R}} \in (\mathcal{P}(\mathbb{N} \times \mathbb{N}) \to \mathcal{P}(\mathbb{N} \times \mathbb{N}))$$
$$\hat{\mathcal{R}}(S) = \{\langle n, n\rangle \mid n \in \mathbb{N}\} \cup \{\langle n, m+1\rangle \mid \langle n, m\rangle \in S\}$$

ed il suo minimo punto (pre-)fisso è proprio $(\leq) \in \mathcal{P}(\mathbb{N}\times\mathbb{N})$.

Notazione

Usando una notazione più succinta, scriviamo le regole

$$\mathcal{R} = \left\{ \frac{}{\langle n, n \rangle} \;\middle|\; n \in \mathbb{N} \right\} \cup \left\{ \frac{\langle n, m \rangle}{\langle n, m+1 \rangle} \;\middle|\; n, m \in \mathbb{N} \right\}$$

come segue:

$$\frac{}{n \;\leq\; n} \qquad \frac{n \;\leq\; m}{n \;\leq\; m+1}$$

Sopra, abbiamo reso esplicito che le regole sono relative alla relazione $\leq$.

“Induzione sul <=”

$$\frac{}{n \ \leq \ n} \qquad \frac{n \ \leq \ m}{n \ \leq \ m+1}$$

Per il principio di induzione abbiamo che, per ogni S:

$$\hat{\mathcal{R}}(S) \subseteq S \implies (\leq) \subseteq S$$

ovvero:

$$\text{Se} \ \left(\begin{array}{l} \forall n \in \mathbb{N}.\ n\ S\ n \\ \forall n, m \in \mathbb{N}.\ (n\ S\ m \implies n\ S\ m+1) \end{array} \right)$$

$$\text{allora} \ (\forall n, m \in \mathbb{N}.\ n \leq m \implies n\ S\ m)$$

“Induzione sul <=”

$$\text{Se} \left(\begin{array}{l} \forall n \in \mathbb{N}.\ n\ S\ n \\ \forall n, m \in \mathbb{N}.\ (n\ S\ m \implies n\ S\ m+1) \end{array} \right)$$

$$\text{allora } (\forall n, m \in \mathbb{N}.\ n \leq m \implies n\ S\ m)$$

Si noti come il principio di sopra si può applicare a tutti gli enunciati del tipo

$$\forall n, m \in \mathbb{N}.\ n \leq m \implies q(n, m)$$

Infatti, basta prendere S come la relazione associata a q.

Esercizio

Esercizio. Usando il principio di induzione su $\leq$, dimostrare che

$$n \leq m \implies \exists k \in \mathbb{N}.\ n + k = m$$

Esempio

Sia D la relazione tra naturali definita ricorsivamente da:

$$\frac{}{n\ D\ 5\cdot n} \qquad \frac{n\ D\ m \qquad n\ D\ o}{n\ D\ m+o} \qquad \frac{n\ D\ m \qquad n'\ D\ m'}{n\cdot n'\ D\ m\cdot m'}$$

Poniamo $(n \mid m) \iff n$ divide m. Per dimostrare

$$\forall n, m.\ n\ D\ m \implies (n \mid m)$$

basta dimostrare che

$$\begin{array}{rcl} & & (n \mid 5\cdot n) \\ (n \mid m) \wedge (n \mid o) & \implies & (n \mid m+o) \\ (n \mid m) \wedge (n' \mid m') & \implies & (n\cdot n' \mid m\cdot m') \end{array}$$

Derivazioni

Derivazioni

Una *derivazione* è una scrittura formale che mostra come si può "ricavare" un elemento del minimo punto fisso di $\hat{\mathcal{R}}$.

Esempio: un'altro insieme di regole per i pari

$$\mathcal{R} = \left\{ \frac{}{0} \right\} \cup \left\{ \frac{}{2} \right\} \cup \left\{ \frac{n \qquad m}{n+m} \;\middle|\; n, m \in U \right\}$$

Una possibile derivazione per 6

$$\cfrac{\cfrac{}{2} \qquad \cfrac{\cfrac{}{2} \qquad \cfrac{}{2}}{4}}{6}$$

Derivazioni

Un'altra derivazione per 6

$$\dfrac{\dfrac{\dfrac{}{2} \qquad \dfrac{}{2}}{4} \qquad \dfrac{}{2}}{6}$$

In generale, ci sono più derivazioni per lo stesso elemento.

Derivazioni

Esempio: altre regole per $(\leq) \in U = \mathcal{P}(\mathbb{N} \times \mathbb{N})$.

$$\mathcal{R} = \left\{ \frac{}{n \leq n} \;\middle|\; n \in \mathbb{N} \right\} \cup \left\{ \frac{}{n \leq n+1} \;\middle|\; n \in \mathbb{N} \right\} \cup$$
$$\left\{ \frac{n \leq m \qquad m \leq o}{n \leq o} \;\middle|\; n, m, o \in \mathbb{N} \right\}$$

Una possibile derivazione per $3 \leq 6$

$$\dfrac{\dfrac{}{3 \leq 4} \qquad \dfrac{\dfrac{}{4 \leq 5} \qquad \dfrac{}{5 \leq 6}}{4 \leq 6}}{3 \leq 6}$$

Derivazioni

Esercizio. Sempre usando

$$\mathcal{R} = \left\{ \frac{}{n \leq n} \;\middle|\; n \in \mathbb{N} \right\} \cup \left\{ \frac{}{n \leq n+1} \;\middle|\; n \in \mathbb{N} \right\} \cup$$
$$\left\{ \frac{n \leq m \qquad m \leq o}{n \leq o} \;\middle|\; n, m, o \in \mathbb{N} \right\}$$

Scrivere due derivazioni per $1 \leq 5$ che abbiano le forme seguenti

$$\dfrac{\dfrac{}{\_ \leq \_} \qquad \dfrac{\dfrac{}{\_ \leq \_} \qquad \dfrac{\dfrac{}{\_ \leq \_} \quad \dfrac{}{\_ \leq \_}}{\_ \leq \_}}{\_ \leq \_}}{\_ \leq \_} \qquad\qquad \dfrac{\dfrac{\dfrac{}{\_ \leq \_} \quad \dfrac{}{\_ \leq \_}}{\_ \leq \_} \qquad \dfrac{\dfrac{}{\_ \leq \_} \quad \dfrac{}{\_ \leq \_}}{\_ \leq \_}}{\_ \leq \_}$$

Iterate di una Funzione

Def. Data $f \in (A \to A)$ si definisce la sua i-esima iterata f^i come la funzione in $(A \to A)$

$$f^i = \underbrace{f \circ f \circ \cdots \circ f}_{i \text{ volte}}$$

ovvero

$$\begin{array}{rcl} f^0(x) & = & x \\ f^{i+1}(x) & = & f(f^i(x)) \end{array}$$

Derivazioni

Osserviamo che

- $\hat{\mathcal{R}}^0(\emptyset) = \emptyset$ coincide con con gli elementi derivabili usando le regole 0 volte.
- $\hat{\mathcal{R}}^1(\emptyset)$ coincide con con gli elementi derivabili usando le regole 1 volta (i "casi base"), ovvero ≤ 1 volte.
- $\hat{\mathcal{R}}^2(\emptyset)$ coincide con con gli elementi derivabili usando le regole ≤ 2 volte.

$\ldots$

- $\hat{\mathcal{R}}^n(\emptyset)$ coincide con con gli elementi derivabili usando le regole $\leq n$ volte.

Derivazioni

Quindi, $\hat{\mathcal{R}}^n(\emptyset)$ contiene esattamente tutti quegli elementi per i quali è possibile costruire una derivazione "alta $\leq n$ livelli".

Ergo,

$$X = \bigcup_{n \in \mathbb{N}} \hat{\mathcal{R}}^n(\emptyset)$$

contiene tutti gli elementi derivabili (usando le regole quante volte si vuole).

Derivazioni e punti fissi

Si può dimostrare che

$$X = \bigcup_{n \in \mathbb{N}} \hat{\mathcal{R}}^n(\emptyset)$$

è proprio $\mathrm{fix}(\hat{\mathcal{R}})$.

Non ne vediamo la dimostrazione, che comunque includiamo per chi vuole approfondire.

Si noti comunque che l'inclusione $\hat{\mathcal{R}}(X) \subseteq X$ è molto intuitiva: applicando una regola qualunque a premesse derivabili, si ottengono conseguenze derivabili.

FUORI ESAME

Continuità di Scott
e
Punto Fisso di Kleene

Continuità (secondo Scott)

FUORI ESAME

Def. Una funzione

$$f \in (\mathcal{P}(U) \to \mathcal{P}(U))$$

si dice *continua* se e solo se per ogni successione di insiemi

$$X_0 \subseteq X_1 \subseteq X_2 \cdots \subseteq U$$

si ha che

$$f(\bigcup_{i \in \mathbb{N}} X_i) = \bigcup_{i \in \mathbb{N}} f(X_i)$$

Prop. L'operatore $\hat{\mathcal{R}} \in (\mathcal{P}(U) \to \mathcal{P}(U))$ è *continuo*

Perché si chiama “continuità”

FUORI ESAME

Si noti la somiglianza della nozione precedente di continuità con il seguente fatto dell'*analisi matematica*.

Una $f \in (\mathbb{R} \to \mathbb{R})$ è continua se e solo se per ogni successione convergente di reali $\{x_n\}_{n\in\mathbb{N}}$ si ha

$$\lim_{n\to\infty} f(x_n) = f(\lim_{n\to\infty} x_n)$$

Nei corsi di geometria vedrete una nozione di “continuità” che generalizza sia quella usata in questo corso sia quella usuale dell'analisi.

Continuità: dimostrazione

FUORI ESAME

Prop. L'operatore $\hat{\mathcal{R}} \in (\mathcal{P}(U) \to \mathcal{P}(U))$ è *continuo*

Dobbiamo fare vedere che per ogni successione di insiemi crescente $\langle X_i \rangle_{i \in \mathbb{N}}$ si ha che

$$1) \bigcup_{i\in\mathbb{N}} \hat{\mathcal{R}}(X_i) \subseteq \hat{\mathcal{R}}(\bigcup_{i\in\mathbb{N}} X_i)$$
$$2) \hat{\mathcal{R}}(\bigcup_{i\in\mathbb{N}} X_i) \subseteq \bigcup_{i\in\mathbb{N}} \hat{\mathcal{R}}(X_i)$$

Per la 1)

$$\begin{array}{lll} & \bigcup_{i\in\mathbb{N}} \hat{\mathcal{R}}(X_i) \subseteq \hat{\mathcal{R}}(\bigcup_{i\in\mathbb{N}} X_i) & \\ \Leftarrow & \forall j \in \mathbb{N}. \quad \hat{\mathcal{R}}(X_j) \subseteq \hat{\mathcal{R}}(\bigcup_{i\in\mathbb{N}} X_i) & [\text{prop. } \bigcup] \\ \Leftarrow & \forall j \in \mathbb{N}. \quad X_j \subseteq \bigcup_{i\in\mathbb{N}} X_i & [\text{monotonia}] \\ \Leftarrow & \text{vero} & [\text{prop. } \bigcup] \end{array}$$

Continuità: dimostrazione

FUORI ESAME

Dimostriamo la 2)

$$\hat{\mathcal{R}}(\bigcup_{i \in \mathbb{N}} X_i) \subseteq \bigcup_{i \in \mathbb{N}} \hat{\mathcal{R}}(X_i)$$

Sia $y \in \hat{\mathcal{R}}(\bigcup_{i \in \mathbb{N}} X_i)$. Per definizione di $\hat{\mathcal{R}}$, esiste una regola

$$\frac{x_1 \quad \ldots x_n}{y} \in \mathcal{R} \qquad \text{dove} \qquad \forall k \in 1..n.\ x_k \in \bigcup_{i \in \mathbb{N}} X_i$$

Questo implica che $\forall k \in 1..n.\ \exists j_k \in \mathbb{N}.\ x_k \in X_{j_k}$.
Sia $m = \max(j_1, \ldots, j_n)$. Dal fatto che la successione degli X_i è crescente, ricavo che $X_{j_k} \subseteq X_m$ per ogni $k \in 1..n$.
Allora ho che $\forall k \in 1..n.\ x_k \in X_m$, da cui concludo con:

$$y \in \hat{\mathcal{R}}(X_m) \subseteq \bigcup_{i \in \mathbb{N}} \hat{\mathcal{R}}(X_i)$$

Continuità e Finitezza

FUORI ESAME

Si noti che è stato fondamentale il fatto che l'insieme delle premesse della regola $\{x_1, \dots, x_n\}$ fosse un insieme *finito*. Se fosse stato infinito, non avremmo potuto considerare $m = \max(j_1, \dots, j_n)$.

Esercizio. (avanzato) Osservate che se consentissimo alle regole di avere un insieme infinito di premesse, $\hat{\mathcal{R}}$ potrebbe essere *non* continuo.
Suggerimento: usate quanto segue.

$$\mathcal{R} = \{\frac{}{1}\ ,\ \frac{1\ 2\ 3\ 4\ 5\ \cdots}{0}\} \cup \{\frac{n}{n+1} \mid n \in \mathbb{N}\}$$

Continuità e Monotonia

FUORI ESAME

Prop. La continuità implica la monotonia.

Dim. Sia f una qualunque funzione continua

$$f \in (\mathcal{P}(U) \to \mathcal{P}(U))$$

Abbiamo quindi $f(\bigcup_{i\in\mathbb{N}} X_i) = \bigcup_{i\in\mathbb{N}} f(X_i)$ per ogni successione crescente di insiemi $\{X_i\}_{i\in\mathbb{N}}$.

Verifichiamo la monotonia. Prendiamo due arbitrari $A, B \in \mathcal{P}(U)$ tali che $A \subseteq B$. Consideriamo la successione di insiemi $X_0 = A$ e $X_{i+1} = B$ per ogni i. La successione è crescente e quindi per continuità si ha:

$$f(A) \subseteq f(A) \cup f(B) = \bigcup_{i\in\mathbb{N}} f(X_i) = f(\bigcup_{i\in\mathbb{N}} X_i) = f(A \cup B) = f(B)$$

Ancora sui punti fissi

FUORI ESAME

Per le funzioni *monotone* (come $\hat{\mathcal{R}}$), il teorema di Knaster-Tarski caratterizza il minimo punto fisso.

Per le funzioni *continue* (sempre come $\hat{\mathcal{R}}$) vale anche una caratterizzazione alternativa, che spesso risulta più comoda da usare.

Th. del Punto Fisso di Kleene

FUORI ESAME

Th. (Punto fisso di Kleene)
Sia $f \in (\mathcal{P}(U) \rightarrow \mathcal{P}(U))$ una qualunque funzione *continua*.
Sia inoltre X definito come

$$X = \bigcup_{i \in \mathbb{N}} f^i(\emptyset)$$

Allora X è il *minimo punto fisso* di f.

Th. Kleene: dimostrazione

FUORI ESAME

Verifichiamo che la successione di insiemi $\{f^i(\emptyset)\}_{i \in \mathbb{N}}$ è crescente, dimostrando $f^i(\emptyset) \subseteq f^{i+1}(\emptyset)$ per ogni $i \in \mathbb{N}$.

Per induzione su $i \in \mathbb{N}$:

- Caso base: $f^0(\emptyset) = \emptyset \subseteq f^1(\emptyset)$.
- Caso induttivo: per ipotesi induttiva ho $f^i(\emptyset) \subseteq f^{i+1}(\emptyset)$. Siccome f è continua, è anche monotona, e quindi $f(f^i(\emptyset)) \subseteq f(f^{i+1}(\emptyset))$, per cui $f^{i+1}(\emptyset) \subseteq f^{i+2}(\emptyset)$.

Th. Kleene: dimostrazione(2)

FUORI ESAME

Sia $X = \bigcup_{i\in\mathbb{N}} f^i(\emptyset)$.
Verifichiamo che X è un punto fisso:

$$
\begin{aligned}
f(X) &= f\left(\bigcup_{i\in\mathbb{N}} f^i(\emptyset)\right) && [\text{def. } X] \\
&= \bigcup_{i\in\mathbb{N}} f(f^i(\emptyset)) && [f \text{ continua}] \\
&= \bigcup_{i\in\mathbb{N}} f^{i+1}(\emptyset) && [\text{def. } f^i] \\
&= \bigcup_{i\in\mathbb{N}} f^i(\emptyset) && [f^0(\emptyset) = \emptyset] \\
&= X && [\text{def. } X]
\end{aligned}
$$

Th. Kleene: dimostrazione(3)

FUORI ESAME

Verifichiamo che X è anche minimo.

Per ogni Y tale che $Y = f(Y)$, dimostriamo $X \subseteq Y$.

$$
\begin{array}{lll}
 & X \subseteq Y & \\
\Leftarrow & \bigcup_{i \in \mathbb{N}} f^i(\emptyset) \subseteq Y & [\text{def. } X] \\
\Leftarrow & \forall i \in \mathbb{N}.\ f^i(\emptyset) \subseteq Y & [\text{prop. } \bigcup]
\end{array}
$$

L'ultima proprietà segue per induzione su $i \in \mathbb{N}$:

- Caso base: si ha $f^0(\emptyset) = \emptyset \subseteq Y$
- Caso induttivo:

$$
\begin{array}{lll}
 & f^i(\emptyset) \subseteq Y & [\text{ipotesi induttiva}] \\
\Rightarrow & f(f^i(\emptyset)) \subseteq f(Y) & [f \text{ è monotona}] \\
\Rightarrow & f^{i+1}(\emptyset) \subseteq Y & [Y \text{ è punto fisso}]
\end{array}
$$

Th. Kleene: Esempi

FUORI ESAME

Riprendiamo le regole per i numeri pari:

$$\mathcal{R} = \{\frac{\ }{0}\} \cup \{\frac{x}{x+2} \mid x \in U\}$$

Siccome $\hat{\mathcal{R}}$ è continuo, il teorema del punto fisso di Kleene ci dice che

$$\begin{aligned} Pari = & \bigcup_{i \in \mathbb{N}} \hat{\mathcal{R}}^i(\emptyset) \\ = & \emptyset \cup \\ & \{0\} \cup \\ & \{0,2\} \cup \\ & \{0,2,4\} \cup \\ & \{0,2,4,6\} \cup \ldots \end{aligned}$$

Th. Kleene: Esempi

FUORI ESAME

$$\begin{aligned} Pari = & \quad \bigcup_{i \in \mathbb{N}} \hat{\mathcal{R}}^i(\emptyset) \\ = & \quad \emptyset \ \cup \{0\} \ \cup \{0, 2\} \ \cup \{0, 2, 4\} \ \cup \{0, 2, 4, 6\} \ \cup \ldots \end{aligned}$$

Intuitivamente, gli elementi in $\hat{\mathcal{R}}^i(\emptyset)$ sono quelli che si possono "ricavare usando le regole $\leq i$ volte".