# Informatica

CdL in Matematica

Parte 3b

Roberto Zunino

Un esercizio svolto sull'induzione:

due definizioni bizzarre dei numeri pari

# Esempio

Sia $\mathcal{R}_X$ l'insieme di regole seguenti sui numeri naturali

$$\frac{}{0}[X0] \qquad \frac{n}{n+2}[X1]$$

e sia $X = fix(\hat{\mathcal{R}}_X)$ (il minimo punto fisso)

Analogamente, sia $\mathcal{R}_Y$ l'insieme di regole

$$\frac{}{0}[Y0] \qquad \frac{n}{n+4}[Y1] \qquad \frac{n+2}{n}[Y2]$$

e sia $Y = fix(\hat{\mathcal{R}}_Y)$.

# Esempio

$$\mathcal{R}_X : \quad \frac{}{0}[X0] \qquad \frac{n}{n+2}[X1]$$

$$\mathcal{R}_Y : \quad \frac{}{0}[Y0] \qquad \frac{n}{n+4}[Y1] \qquad \frac{n+2}{n}[Y2]$$

$$X = fix(\hat{\mathcal{R}}_X) \qquad Y = fix(\hat{\mathcal{R}}_Y)$$

Abbiamo quindi, per ogni $Z \subseteq \mathbb{N}$:

$$\hat{\mathcal{R}}_X(Z) = \{0\} \cup \{n+2 \mid n \in Z\}$$
$$\hat{\mathcal{R}}_Y(Z) = \{0\} \cup \{n+4 \mid n \in Z\} \cup \{n \mid n+2 \in Z\}$$

Svolgiamo quindi il seguente

**Esercizio.** Dimostrare che X $\subseteq Y$.

# Evitate di dire “ma è ovvio”

**Nota.** Può risultare ovvio dalle regole che

$$X = Y = \{2 \cdot n \mid n \in \mathbb{N}\} \qquad (*)$$

cioè che $X$ e $Y$ sono uguali e sono l’insieme dei naturali pari. Da questo uno può essere tentato di concludere immediatamente l’esercizio.

In questa parte del corso, tuttavia, **non** accetteremo dimostrazioni che si poggino in tal modo sull’intuizione. Ovvero, non accetteremo “è ovvia” come giustificazione per $(*)$, che invece, se la si vuole usare, va *dimostrata*.

L’enfasi è sul *come*, non sul *cosa* si dimostra.

# Dimostrazione

Per dimostrare $a \in X \implies a \in Y$, procediamo per induzione su $a \in X$. Facciamo quindi vedere che la proprietà di appartenere a $Y$ è preservata da ogni regola di $\mathcal{R}_X$. Consideriamo ambo i casi $[X0], [X1]$.

- **Caso** $[X0]$. Qui $a = 0$ e devo fare vedere che $a \in Y$. Per la regola $[Y0]$ concludo.
- **Caso** $[X1]$. Qui $a = n + 2$ per qualche $n$. Siccome $[X1]$ ha come premessa $n$, possiamo assumere come ipotesi induttiva, $n \in Y$. Per la regola $[Y1]$ si ha $n+4 \in Y$. Visto che $n+4 = (n+2)+2$, per la regola $[Y2]$ si ha $n + 2 = a \in Y$

# Dimostrazione alternativa

Data una derivazione in $\mathcal{R}_X$, posso sostituire la regola $[X0]$ con la $[Y0]$

$$\frac{}{0}[X0] \Rightarrow \frac{}{0}[Y0]$$

e la regola $[X1]$ come segue

$$\frac{n}{n+2}[X1] \Rightarrow \frac{\dfrac{n}{n+4=(n+2)+2}[Y1]}{n+2}[Y2]$$

Dopo le sostituzioni di sopra, ho una derivazione in $\hat{\mathcal{R}}_Y$.

# Un altro esercizio

**Esercizio.** Dimostrare che vale anche $Y \subseteq X$, e che quindi $X = Y$.

Questa direzione è più difficile da dimostrare.

# Svolgimento

Dimostriamo $a \in Y \implies a \in X$. Procediamo per induzione su $a \in Y$, e dimostriamo che l'appartenenza ad $X$ è preservata dalle regole in $\mathcal{R}_Y$, e quindi da $[Y0], [Y1], [Y2]$.

- Caso $[Y0]$. Qui $a = 0$, quindi $[X0]$ conclude.
- Caso $[Y1]$. Qui $a = n + 4$ per un qualche $n$. Per ipotesi induttiva ho che $n \in X$. Per la regola $[X1]$ ho che $n+2 \in X$. Ancora per $[X1]$ ottengo $(n+2)+2 = a \in X$.
- Caso $[Y2]$. Qui $a = n$ per un qualche $n$. Per ipotesi induttiva ho che $n + 2 \in X$. . . . (e ora?)

# Svolgimento

- Caso $[Y2]$. Qui $a = n$ per un qualche $n$. Per ipotesi induttiva ho che $n + 2 \in X$. Per inversione, questo deve essere conseguenza di qualche regola con premesse in $X$. Consideriamo tutte le regole possibili:
  - Caso $[X0]$. Qui si ha $n + 2 = 0$. Impossibile, visto che $n \in \mathbb{N}$.
  - Caso $[X1]$. Qui si ha $n + 2 = m + 2$ con $m \in X$. Dall'equazione si ricava $n = m$, per cui $a = n = m \in X$.

Esempio:

La “relazione” fattoriale

# Esempio: Relazione Fattoriale

Definiamo la relazione fattoriale $F \subseteq (\mathbb{N} \times \mathbb{N})$ induttivamente tramite l'insieme di regole $\mathcal{R}$

$$\frac{}{0\ F\ 1}[F0] \qquad \frac{n\ F\ m}{(n+1)\ F\ (n+1)\cdot m}[F1]$$

È facile convincersi che $nFm$ se e solo se $n! = m$, e che quindi la relazione $F$ è in realtà una *funzione* $\mathbb{N} \to \mathbb{N}$.

Andiamo ora a svolgere il seguente
**Esercizio.** Verificare che $F$ è effettivamente una funzione.

# Esistenza del Risultato

Dimostriamo prima l'esistenza del risultato della funzione. In formule:

$$\forall n \in \mathbb{N}. \exists m \in \mathbb{N}.\ nFm$$

Chiamando

$$X = \{n \mid \exists m \in \mathbb{N}.\ nFm\}$$

dimostriamo

$$\forall n \in \mathbb{N}.\ n \in X$$

cioè

$$\mathbb{N} \subseteq X$$

per induzione su $\mathbb{N}$.

# Esistenza del Risultato

Siccome $\mathbb{N}$ è definito induttivamente dalle regole $\mathcal{R}'$

$$\frac{}{0} \qquad \frac{n}{n+1}$$

dobbiamo dimostrare che $\hat{\mathcal{R}}'(X) \subseteq X$, ovvero che $X$ è preservato da tutte le regole in $\mathcal{R}'$, ovvero che

$$\begin{array}{l} 0 \in X \\ n \in X \implies n+1 \in X \end{array}$$

(che è il "solito" principio di induzione su $\mathbb{N}$).

# Esistenza del Risultato

**Caso** $0 \in X$**.** Dalla regola di $\mathcal{R}$

$$\frac{}{0\ F\ 1}[F0]$$

Si ha $0F1$, e quindi $\exists m \in \mathbb{N}.\ 0Fm$, e quindi $0 \in X$ vale.

# Esistenza del Risultato

**Caso** $n \in X \implies n+1 \in X$**.** Dall'ipotesi induttiva ricaviamo $nFm$ per qualche $m$. Usando ora la regola di $\mathcal{R}$

$$\frac{n\ F\ m}{(n+1)\ F\ (n+1)\cdot m}[F1]$$

abbiamo che $(n+1)\,F\,(n+1)\cdot m$, e di conseguenza anche $n+1 \in X$ vale.

# Unicità del Risultato

Dobbiamo ora verificare l'unicità del risultato, ovvero che

$$\forall n, m_1, m_2 \in \mathbb{N}.\ nFm_1 \wedge nFm_2 \implies m_1 = m_2$$

Anche se potremmo procedere per induzione su $n \in \mathbb{N}$, procediamo invece per induzione su $nFm_1$. Definiamo una relazione $p \subseteq \mathbb{N} \times \mathbb{N}$ come segue:

$$p(n, m) = \text{“}\forall m_2 \in \mathbb{N}.\ nFm_2 \implies m = m_2\text{”}$$

e osserviamo che la proprietà di unicità si può riscrivere come

$$F \subseteq p$$

# Unicità del Risultato

Per dimostrare

$$F \subseteq p$$

per il principio d'induzione basta fare vedere che $\hat{\mathcal{R}}(p) \subseteq p$, ovvero che $p$ è preservata da ogni regola di $\mathcal{R}$.

In concreto, dobbiamo dimostrare:

1) $p(0, 1)$
2) $\forall n, m \in \mathbb{N}.\ p(n, m) \implies p(n + 1, (n + 1) \cdot m)$

# Unicità del Risultato

**Caso 1.** Per dimostrare $p(0,1)$, dobbiamo fare vedere che

$$0Fm_2 \implies m_2 = 1$$

Assumiamo $IP1$: $0Fm_2$, e procediamo per inversione. Osserviamo che $IP1$ non può essere conseguenza di $[F1]$, visto che da questa si ricava $(n+1)F(\ldots)$ e chiaramente $0 \neq n+1$. Quindi $IP1$ si deve ricavare con $[F0]$, e deve essere:

$$\frac{}{0F1 = m_2}[F0]$$

da cui la tesi.

# Unicità del Risultato

**Caso 2.** Per dimostrare $p(n,m) \implies p(n+1,(n+1)\cdot m)$, possiamo assumere che:

$$\begin{aligned} IP1: &\quad p(n,m) \\ IP2: &\quad (n+1)Fm_2 \end{aligned}$$

da cui dobbiamo derivare $m_2 = (n+1)\cdot m$.
Invertiamo $IP2$. Non è ricavabile dalla regola $[F0]$, visto che da questa si ricava $0F(\ldots)$ e $0 \neq n+1$. Quindi deve ricavarsi da $[F1]$:

$$\frac{nFm'}{(n+1)F(n+1)\cdot m' = m_2}[F1]$$

dove $nFm'$ vale.

# Unicità del Risultato

**Caso 2 (continua).**

$$IP3: \ nFm'$$

Ricodiamo che $IP1 : p(n, m)$ ci dice che

$$\forall k \in \mathbb{N}.\ nFk \implies k = m$$

Scegliamo $k = m'$:

$$nFm' \implies m' = m$$

ma l'antecedente vale per $IP3$, quindi abbiamo $m' = m$, da cui la tesi $m_2 = (n + 1) \cdot m' = (n + 1) \cdot m$.

# Sull'inversione

Nell'esempio appena fatto, dopo avere ricavato

$$(n+1)Fm_2$$

siamo andati a "invertire" tale ipotesi.

Questo richiede di andare a considerare **tutte** le regole e capire quali potrebbero avere come conseguenza quell'ipotesi.

Nell'esempio visto, solo $[F1]$ poteva farlo. In generale, potrebbero esserci più regole, ognuna delle quali genera un sottocaso da trattare.

# Inversione non unica

Nell'esempio appena fatto, quando $nFm$ vale, esiste una sola regola che può derivarlo. Non è sempre quello il caso: per esempio

$$\frac{}{0I0}[I0] \qquad \frac{nIm}{(n+2)I(m+2)}[I1] \qquad \frac{(n+1)I(m+1)}{nIm}[I2]$$

definisce la funzione identità $\mathsf{id}(n) = n$, ma ci sono molti (infiniti) modi diversi per ricavare $nIn$. Per esempio:

$$\frac{}{0I0}[I0] \qquad \frac{\dfrac{\dfrac{}{0I0}[I0]}{2I2}[I1]}{1I1}[I2]}{0I0}[I2]$$

# Conclusioni

La dimostrazione appena vista non si applica solo al caso del fattoriale ma a tutte le relazioni/funzioni definite induttivamente da regole della forma

$$\frac{}{0Fc} \qquad \frac{nFm}{(n+1)Fg(n,m)}$$

per una qualche funzione $g$.

Sappiamo quindi che: esiste ed è unica la "relazione" $F$ (per Knaster-Tarski), ed essa è effettivamente una funzione (per l'esercizio svolto prima).

# Conclusioni

Di solito, definire una funzione per induzione è fatto con una scrittura simile a:

$$f(0) = c \qquad f(n+1) = g(n, f(n))$$

Nell'esercizio appena svolto abbiamo dimostrato che le definizioni come quella di sopra sono sempre *ben poste*: esiste un'unica $f$ che soddisfa quanto sopra.

# Altri esempi

# Esercizio

**Esercizio.** Considerate la relazione $I$ sui naturali definita induttivamente da:

$$\frac{}{0I0}[I0] \qquad \frac{nIm}{(n+2)I(m+2)}[I1] \qquad \frac{(n+1)I(m+1)}{nIm}[I2]$$

Dimostrate che $I$ implica l'identità, cioè che:

$$\forall n, m \in \mathbb{N}.\ nIm \implies n = m$$

Provate prima a farlo per induzione su $n \in \mathbb{N}$ e notate che non si ci riesce (perché?).

Poi procedete per induzione su $nIm$.

# Esercizio

**Esercizio.** Ricordate la definizione delle sequenze finite di naturali:

$$\frac{}{\epsilon} \qquad \frac{s}{n : s}$$

Definite una relazione (funzione) $s\ \Sigma\ n$ che valga quando $n$ è la somma di tutta la sequenza $s$.

# Esercizio

**Esercizio.**
Sia $S$ l'insieme delle sequenze finite definite da

$$\frac{}{\epsilon} \qquad \frac{s}{n : n : s}$$

Dimostrate che

$$\forall n, s.\ s \in S \wedge s\ \Sigma\ n \implies n \text{ pari}$$

# Esercizio

**Esercizio.**
Sia $R$ la relazione tra sequenze di naturali data da

$$\frac{}{\epsilon \; R \; \epsilon} \qquad \frac{s \; R \; s'}{n : m : s \; R \; m : n : s'}$$

Dimostrate che

$$\forall s, s', a, a'. \qquad s \; R \; s' \wedge s \; \Sigma \; a \wedge s' \; \Sigma \; a' \implies a = a'$$

# Esercizio

**Esercizio.** (avanzato)
Definite con un insieme di regole la relazione $s \; R \; s'$ che vale quando $s$ è una permutazione (un riordinamento) di $s'$.