Corso di Laurea in Informatica Applicata

# Linguaggio e Metodi della Matematica

Prova scritta del 20 Dicembre 2005

[**Esercizio 1**]
Data la teoria $\Gamma = \{\forall x.(P(x) \vee Q(x))\ ,\ P(a) \rightarrow R(a)\ ,\ \neg R(a) \rightarrow \neg Q(a)\}$.
Si dica se le seguenti formule sono conseguenza logica di $\Gamma$:

1. $\exists z.R(z)$
2. $\forall z.R(z)$

In caso positivo fornire una dimostrazione formale, in caso negativo dare un'opportuna interpretazione come controesempio.

**Svolgimento**

La formula $\exists z.R(z)$ è conseguenza logica di $\Gamma$, come dimostrato dalla seguente prova formale:

| | | |
|---|---|---|
| 1. | $[\ \neg\exists z.R(z)\ ]$ | (Ipotesi aggiuntiva) |
| 2. | $\forall z.\neg R(z)$ | (**EQ**. da 1) |
| 3. | $\neg R(a)$ | ($\forall$**I** da 2) |
| 4. | $\neg R(a) \rightarrow \neg Q(a)$ | (Ipotesi in $\Gamma$) |
| 5. | $\neg Q(a)$ | (**M.P**. da 3 e 4) |
| 6. | $\forall x.(P(x) \vee Q(x))$ | (Ipotesi in $\Gamma$) |
| 7. | $P(a) \vee Q(a)$ | ($\forall$**I** da 6) |
| 8. | $P(a)$ | (**D.S**. da 5 e 7) |
| 9. | $P(a) \rightarrow R(a)$ | (Ipotesi in $\Gamma$) |
| 10. | $R(a)$ | (**M.P**. da 8 e 9) |
| 11. | $\perp$ | (**C**. da 3 e 10) |
| 12. | $\exists z.R(z)$ | (**Abs** da $\frac{[1]}{11}$) |

La formula $\forall z.R(z)$ invece non è conseguenza logica di $\Gamma$, come dimostrato dalla seguente interpretazione $\mathcal{I}$ che soddisfa tutte le formule in $\Gamma$ ma rende falsa $\forall z.R(z)$.
Prendiamo $D_{\mathcal{I}} = \{a, b\}$, con $TS_{\mathcal{I}}(P) = \{a, b\}$, $TS_{\mathcal{I}}(Q) = \emptyset$ e $TS_{\mathcal{I}}(R) = \{a\}$.
Banalmente, si ha:

- $\mathcal{I} \models \forall x.(P(x) \vee Q(x))$ perché $\mathcal{I} \models P(a)$ e $\mathcal{I} \models P(b)$;
- $\mathcal{I} \models P(a) \rightarrow R(a)$ perché $\mathcal{I} \models P(a)$ e $\mathcal{I} \models R(a)$;
- $\mathcal{I} \models \neg R(a) \rightarrow \neg Q(a)$ perché $\mathcal{I} \not\models \neg R(a)$;
- $\mathcal{I} \not\models \forall z.R(z)$ perché $\mathcal{I} \not\models R(b)$.

**[Esercizio 2]**
Si dica se le seguenti proprietà su insiemi sono valide:

1. $\forall A, B.\ ((A - B \subseteq B - A) \ \rightarrow\ (A \subseteq B))$
2. $\forall A, B.\ ((A - B \subseteq B - A) \ \rightarrow\ (B \subseteq A))$

In caso positivo fornire una dimostrazione formale, in caso negativo dare un controesempio.

**Svolgimento**

La proprietà $\forall A, B.\ ((A - B \subseteq B - A) \ \rightarrow\ (A \subseteq B))$ è valida, come dimostrato dalla seguente prova formale:

| | | |
|---|---|---|
| 1. | $A - B \subseteq B - A$ | (Ipotesi aggiuntiva) |
| 2. | $\quad x \in A$ | (Ipotesi aggiuntiva) |
| 3. | $\quad\quad x \in \overline{B}$ | (Ipotesi aggiuntiva) |
| 4. | $\quad\quad\quad x \in A \cap \overline{B}$ | (**A**.**I**.$_\cap$ da 2 e 3) |
| 5. | $\quad\quad\quad x \in A - B$ | (**EQ**. da 4) |
| 6. | $\quad\quad\quad x \in B - A$ | (**M**.**P**.$_\subseteq$ da 1 e 5) |
| 7. | $\quad\quad\quad x \in B \cap \overline{A}$ | (**EQ**. da 6) |
| 8. | $\quad\quad\quad x \in \overline{A}$ | (**A**.**E**.$_\cap$ da 7) |
| 9. | $\quad\quad\quad \perp$ | (**C**. da 2 e 8) |
| 10. | $\quad\quad x \in B$ | (**Abs**. da $\frac{[3]}{9}$) |
| 11. | $\quad x \in A \rightarrow x \in B$ | (**Imp**. da $\frac{[2]}{10}$) |
| 12. | $\quad A \subseteq B$ | ($\forall$**G**$_\subseteq$ da 11) |
| 13. | $(A - B \subseteq B - A) \rightarrow (A \subseteq B)$ | (**Imp**. da $\frac{[1]}{12}$) |
| 14. | $\forall A, B.\ (A - B \subseteq B - A) \rightarrow (A \subseteq B)$ | ($\forall$**G** per due volte da 13) |

La proprietà $\forall A, B.\ ((A - B \subseteq B - A) \ \rightarrow\ (B \subseteq A))$ non è valida, come dimostrato dal seguente semplice controesempio.
Prendiamo $A = \{a\}$, $B = \{a, b\}$. Ovviamente $A - B = \emptyset$ e $B - A = \{b\}$, quindi:

- $A - B \subseteq B - A$;
- $B \not\subseteq A$.

**[Esercizio 3]**
Dimostrare per induzione che: $\forall n.\ 3|(7^n - 1)$.
Giustificare con commenti precisi tutti i passaggi della dimostrazione.

**Svolgimento**

Procediamo per induzione.

**[CASO BASE]** Dobbiamo far vedere che la proprietà vale per $n = 0$. Infatti

$$7^0 - 1 = 1 - 1 = 0$$

e ovviamente $3|0$.

**[CASO INDUTTIVO]** Prendiamo un $n$ generico e assumendo che $7^n - 1$ sia multiplo di 3 vogliamo far vedere che anche $7^{n+1} - 1$ è multiplo di 3.

| | |
|---|---|
| $7^{n+1} - 1 = 7 \cdot 7^n - 1$ | (per note proprietà degli esponenti) |
| $7 \cdot 7^n - 1 = 7 \cdot 7^n - 7 + 7 - 1$ | (per note proprietà aritmetiche) |
| $7 \cdot 7^n - 7 + 7 - 1 = 7 \cdot (7^n - 1) + (7 - 1)$ | (per note proprietà del prodotto) |
| $7 \cdot (7^n - 1) + (7 - 1) = 7 \cdot (7^n - 1) + 6$ | (per note proprietà aritmetiche) |

Riassumendo la catena di uguaglianze riportata sopra abbiamo:

$$7^{n+1} - 1 = 7 \cdot (7^n - 1) + 6$$

Per ipotesi induttiva abbiamo che $3|7^n - 1$ e quindi per il lemma di divisibilità #2 abbiamo anche $3|7 \cdot (7^n - 1)$.

Inoltre $3|6$ e quindi per il lemma di divisibilità #1 abbiamo $3|7 \cdot (7^n - 1) + 6$ e quindi $3|7^{n+1} - 1$ per l'uguaglianza di cui sopra.

**[Esercizio 4]**
Si considerino le seguenti relazioni:

1. $R_1 = \{(n,m) \mid n,m \in \mathbb{Z} \wedge \exists x \in \mathbb{N}. n = m \cdot 10^x\}$
2. $R_2 = \{(n,m) \mid n,m \in \mathbb{Z} \wedge \exists y,k \in \mathbb{N}. n = m \cdot k \cdot 2^y\}$
3. $R_3 = \{(n,m) \mid n,m \in \mathbb{Z} \wedge \exists z,h \in \mathbb{N}. n = m \cdot h \cdot 5^z\}$

Si risponda alle seguenti domande, giustificando la risposta:

1. $R_1$ è riflessiva? Irriflessiva? Simmetrica? Transitiva?
2. $R_2$ è riflessiva? Irriflessiva? Simmetrica? Transitiva?
3. $R_3$ è riflessiva? Irriflessiva? Simmetrica? Transitiva?
4. l'insieme $R_1$ include, è incluso o è uguale a $R_2 \cap R_3$?

**Svolgimento**

La relazione $R_1$ è riflessiva perché prendendo $x = 0$ si ha $10^0 = 1$ e quindi $n = n \cdot 10^0$ per un qualsiasi intero $n$. È anche transitiva perché se $n = m \cdot 10^{x_0}$ e $m = r \cdot 10^{x_1}$ per opportuni $x_0$ e $x_1$, allora $n = r \cdot 10^{x_0+x_1}$. Si noti invece che non è irriflessiva perché come detto $(n,n) \in R_1$ per ogni $n$. Non è simmetrica perché ad esempio $(10,1) \in R_1$ mentre $(1,10) \notin R_1$.

La relazione $R_2$ è riflessiva perché prendendo $z = 0$ e $k = 1$ si ha $5^0 \cdot 1 = 1$ e quindi $n = n \cdot 1 \cdot 5^0$ per un qualsiasi intero $n$. È anche transitiva perché se $n = m \cdot k_0 \cdot 5^{z_0}$ e $m = r \cdot k_1 \cdot 5^{z_1}$ per opportuni $z_0$, $z_1$, $k_0$ e $k_1$, allora $n = r \cdot (k_0 \cdot k_1) \cdot 5^{z_0+z_1}$. Si noti invece che non è irriflessiva perché come detto $(n,n) \in R_2$ per ogni $n$. Non è simmetrica perché ad esempio $(10,1) \in R_2$ mentre $(1,10) \notin R_2$.

Per la relazione $R_3$ valgono considerazioni del tutto analoghe a quelle di $R_2$.

La tabella sottostante riassume le proprietà di $R_1$, $R_2$ e $R_3$.

| | rif. | irr. | sim. | trans. |
|---|---|---|---|---|
| $R_1$ | **si** | no<br>$n = 1$ | no<br>$n = 10, m = 1$ | **si** |
| $R_2$ | **si** | no<br>$n = 1$ | no<br>$n = 10, m = 1$ | **si** |
| $R_3$ | **si** | no<br>$n = 1$ | no<br>$n = 10, m = 1$ | **si** |

La relazione $R_1$ è inclusa strettamente in $R_2 \cap R_3$.
Per vedere che $R_1 \subseteq R_2 \cap R_3$ facciamo vedere che ogni coppia $(n,m) \in R_1$ è contenuta anche in $R_2$ e $R_3$. Se $(n,m) \in R_1$ vuol dire che esiste un $x \in \mathbb{N}$ tale che $n = m \cdot 10^x$ e quindi $n = m \cdot 5^x \cdot 2^x$. Ma allora $(n,m) \in R_2$ (prendendo $y = x$ e $k = 2^x$) e $(n,m) \in R_3$ (prendendo $z = x$ e $h = 5^x$).
Per vedere che $R_2 \cap R_3 \not\subseteq R_1$ basta trovare una coppia di valori $(n,m) \in R_2 \cap R_3$ tali che $(n,m) \notin R_1$. Prendiamo la coppia $(20,1)$. Con $y = 1$ e $k = 4$ si ha $20 = 1 \cdot 4 \cdot 5^1$ e dunque $(20,1) \in R_2$. Con $z = 2$ e $k = 5$ si ha $20 = 1 \cdot 5 \cdot 2^2$ e dunque $(20,1) \in R_3$. Invece non è possibile trovare $x \in \mathbb{N}$ tale che $20 = 1 \cdot 10^x$ e dunque $(20,1) \notin R_1$.