LOGICA PER LA PROGRAMMAZIONE - a.a. 2014-2015
Prima prova di verifica intermedia - 4/11/2014 — Soluzioni Proposte

Attenzione: Le soluzioni che seguono sono considerate corrette dai docenti. Per ogni esercizio possono esistere altre soluzioni corrette, anche molto diverse da quelle proposte.

ESERCIZIO 1

Per ognuna delle seguenti formule si dica se si tratta di una tautologia oppure no. Se è una tautologia si fornisca una dimostrazione (non per casi) altrimenti si fornisca un controesempio.

1. $(Q \Rightarrow P) \Rightarrow R \equiv (P \Rightarrow R) \wedge (\neg Q \Rightarrow R)$
2. $((\neg P \Rightarrow Q) \Rightarrow \neg R) \;\vee\; \neg(P \Rightarrow R) \;\vee\; \neg(\neg R \Rightarrow \neg Q)$
3. $(Q \vee S) \wedge (Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow S)$

SOLUZIONE ESERCIZIO 1

1. $(Q \Rightarrow P) \Rightarrow R \equiv (P \Rightarrow R) \wedge (\neg Q \Rightarrow R)$

   Si tratta di una tautologica, come dimostrato di seguito. Partiamo dalla parte sinistra dell'equivalenza:

$$
\begin{array}{ll}
 & (Q \Rightarrow P) \Rightarrow R \\
\equiv & \{(\text{Elim.-}\Rightarrow) \text{ due volte}\} \\
 & \neg(\neg Q \vee P) \vee R \\
\equiv & \{(\text{De Morgan}), (\text{Doppia Negazione}), (\text{Comm.})\} \\
 & (\neg P \wedge Q) \vee R \\
\equiv & \{(\text{Distr.})\} \\
 & (\neg P \vee R) \wedge (Q \vee R) \\
\equiv & \{(\text{Elim.-}\Rightarrow) \text{ al contrario, due volte e } (\text{Doppia Negazione})\} \\
 & (P \Rightarrow R) \wedge (\neg Q \Rightarrow R)
\end{array}
$$

2. $((\neg P \Rightarrow Q) \Rightarrow \neg R) \;\vee\; \neg(P \Rightarrow R) \;\vee\; \neg(\neg R \Rightarrow \neg Q)$

   Non è una tautologia, dato che è possibile individuare valori delle variabili proposizionali che la rendono falsa. Prendendo infatti l'interpretazione $\{P \mapsto \mathbf{T}, Q \mapsto \mathbf{F}, R \mapsto \mathbf{T}\}$ si ottiene $\mathbf{F}$.

   Un modo efficace di mostrare la corretta valutazione della proposizione con l'interpretazione data è il seguente, dove riportiamo la riga della tabella di verità corrispondente all'interpretazione. I numeri nell'ultima riga mostrano l'ordine in cui sono stati valutati i connettivi logici.

P	Q	R	$((\neg$	P	$\Rightarrow$	$Q)$	$\Rightarrow$	$\neg$	$R)$	$\vee$	$\neg$	$(P$	$\Rightarrow$	$R)$	$\vee$	$\neg$	$(\neg$	R	$\Rightarrow$	$\neg$	$Q)$
T	F	T	F	T	T	F	F	F	T	F	F	T	T	T	F	F	F	T	T	T	F
			2	1	3	1	4	2	1	5	3	1	2	1	6	4	2	1	3	2	1

3. $(Q \vee S) \wedge (Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow S)$

   Si tratta di una tautologia. Vediamo diversi modi di dimostrarla: sono tutti corretti, ma sono preferibili quelli più compatti. La nostra dimostrazione preferita è la quarta.

(1) Partiamo dalla premessa:

$(Q \vee S) \wedge (Q \Rightarrow \neg P)$

$\equiv \quad \{(\text{Elim-}\Rightarrow)\}$

$(Q \vee S) \wedge (\neg Q \vee \neg P)$

$\equiv \quad \{(\text{Distributività})\}$

$(Q \wedge (\neg Q \vee \neg P)) \vee (S \wedge (\neg Q \vee \neg P))$

$\equiv \quad \{(\text{Complemento) e (Distributività})\}$

$(Q \wedge \neg P) \vee (S \wedge \neg Q) \vee (S \wedge \neg P)$

$\Rightarrow \quad \{(\text{Semp-}\wedge) \text{ tre volte}\}$

$\neg P \vee S \vee S$

$\equiv \quad \{(\text{Idempotenza})\}$

$\neg P \vee S$

$\equiv \quad \{(\text{Elim-}\Rightarrow) \text{ al contrario}\}$

$P \Rightarrow S$

(4) Dimostriamo la conseguenza usando le premesse (opportunamente trasformate) come ipotesi non tautologiche:

P

$\Rightarrow \quad \{\textbf{Ip: } Q \Rightarrow \neg P, \text{ equiv. (Contronom.) a } P \Rightarrow \neg Q\}$

$\neg Q$

$\Rightarrow \quad \{\textbf{Ip: } Q \vee S, \text{ equiv. (Elim-}\Rightarrow\text{) a } \neg Q \Rightarrow S\}$

S

(2) Partiamo dalla premessa:

$(Q \vee S) \wedge (Q \Rightarrow \neg P)$

$\equiv \quad \{(\text{Elim-}\Rightarrow)\}$

$(Q \vee S) \wedge (\neg Q \vee \neg P)$

$\Rightarrow \quad \{(\text{Risoluzione})\}$

$S \vee \neg P$

$\equiv \quad \{(\text{Elim-}\Rightarrow) \text{ al contrario}\}$

$P \Rightarrow S$

(3) Dimostriamo la conseguenza usando le premesse come ipotesi non tautologiche:

P

$\equiv \quad \{\textbf{Ip: } Q \Rightarrow \neg P\}$

$P \wedge (Q \Rightarrow \neg P)$

$\equiv \quad \{(\text{Contropositiva})\}$

$P \wedge (P \Rightarrow \neg Q)$

$\Rightarrow \quad \{(\text{Modus Ponens})\}$

$\neg Q$

$\equiv \quad \{\textbf{Ip: } (Q \vee S)\}$

$\neg Q \wedge (Q \vee S)$

$\equiv \quad \{(\text{Complemento})\}$

$\neg Q \wedge S$

$\Rightarrow \quad \{(\text{Sempl-}\wedge)\}$

S

ESERCIZIO 2

Utilizzando il principio di sostituzione dell'implicazione, si applichi l'ipotesi non tautologica $P \wedge \neg R \Rightarrow \neg Q \vee S$ alle seguenti formule, completando il passo di dimostrazione con la relativa giustificazione.

1. $(S \Rightarrow P \wedge \neg R \wedge Q) \Rightarrow S \vee R$
2. $(P \wedge \neg R) \vee Q \Rightarrow (S \Rightarrow \neg Q)$

SOLUZIONE ESERCIZIO 2

1. $(S \Rightarrow \underline{P \wedge \neg R} \wedge Q) \Rightarrow S \vee R$

$\Leftarrow \quad \{\textbf{Ip: } P \wedge \neg R \Rightarrow \neg Q \vee S, \ \underline{P \wedge \neg R} \text{ occorre neg.}\}$

$(S \Rightarrow \underline{(\neg Q \vee S)} \wedge Q) \Rightarrow S \vee R$

2. $\underline{(P \wedge \neg R)} \vee Q \Rightarrow (S \Rightarrow \neg Q)$

$\Leftarrow \quad \{\textbf{Ip: } P \wedge \neg R \Rightarrow \neg Q \vee S, \ \underline{P \wedge \neg R} \text{ occorre neg.}\}$

$\underline{\neg Q \vee S} \vee Q \Rightarrow (S \Rightarrow \neg Q)$

ESERCIZIO 3
Si formalizzi il seguente enunciato fornendo un alfabeto del primo ordine e una corrispondente interpretazione sul dominio delle persone.

"Gino e Lia sono cugini solo se hanno un nonno in comune ma non sono fratelli"

SOLUZIONE ESERCIZIO 3

- **Alfabeto**: $\mathbf{C} = \{Gino, Lia\}$, $\mathbf{F} = \emptyset$, $\mathbf{P} = \{nonno(\_,\_), fratelli(\_,\_), cugini(\_,\_)\}$
- **Interpretazione**: $\mathbf{I} = (\mathbf{D}, \alpha)$, con
  - $\mathbf{D} = \mathcal{P}$, con $\mathcal{P}$ insieme delle persone.
  - $\alpha(Gino) =$ "la persona chiamata Gino"
  - $\alpha(Lia) =$ "la persona chiamata Lia"
  - $\alpha(nonno)(d, d') \equiv \mathbf{T}$ se e solo se d è nonno di d'
  - $\alpha(fratelli)(d, d') \equiv \mathbf{T}$ se e solo se d e d' sono fratelli
  - $\alpha(cugini)(d, d') \equiv \mathbf{T}$ se e solo se d e d' sono cugini

  Ricordando che dire che P *solo se* Q, è un altro modo di dire che P implica Q, l'enunciato può essere formalizzato nel seguente modo:

$$cugini(Gino, Lia) \Rightarrow (\exists x.nonno(x, Gino) \wedge nonno(x, Lia) \wedge \neg fratelli(Gino, Lia))$$

ESERCIZIO 4
Si formalizzi il seguente enunciato utilizzando l'alfabeto del primo ordine e l'interpretazione sul dominio dei naturali che sono proposti.

"Due numeri sono *coprimi* se e solo se non hanno nessun divisore in comune diverso da 1"

- **Alfabeto**: $\mathbf{C} = \{0, 1, 2, \ldots\}$, $\mathbf{F} = \emptyset$, $\mathbf{P} = \{coprimi(\_,\_), divisore(\_,\_), = (\_,\_)\}$
- **Interpretazione**: $\mathbf{I} = (\mathbf{D}, \alpha)$, con
  - $\mathbf{D} = \mathbb{N}$, con $\mathbb{N}$ insieme dei numeri naturali
  - $\alpha(0) =$ "il numero 0", e analogamente per tutte le altre costanti
  - $\alpha(coprimi)(n, m) = \mathbf{T}$ se e solo se n e m sono coprimi
  - $\alpha(divisore)(n, m) = \mathbf{T}$ se e solo se n è un divisore di m
  - $\alpha(=)(n, m) = \mathbf{T}$ se e solo se n e m sono lo stesso numero

SOLUZIONE ESERCIZIO 4
Proponiamo due soluzioni, entrambe corrette: si possono dimostrare equivalenti usando le leggi del calcolo dei predicati.

$$(\forall x.(\forall y.coprimi(x, y) \equiv \neg(\exists z.divisore(z, x) \wedge divisore(z, y) \wedge \neg{=}(z, 1))))$$

$$(\forall x.(\forall y.coprimi(x, y) \equiv (\forall z.divisore(z, x) \wedge divisore(z, y) \Rightarrow {=}(z, 1))))$$

ESERCIZIO 5
Si calcoli, motivando la risposta, il valore di verità della formula

$$\Phi = (\forall x \, . \, R(x) \Rightarrow (\exists y \, . \, S(x,y) \wedge \neg R(y)))$$

nell'interpretazione $I = (D, \alpha)$, dove $D = \{a, b, c\}$ ed α è definita come segue

$$\alpha(R)(z) = \begin{cases} T & \text{se } z \in \{a, b\} \\ F & \text{altrimenti.} \end{cases} \qquad \alpha(S)(z,v) = \begin{cases} T & \text{se } (z,v) \in \{(a,b),(a,c),(b,c),(c,c)\} \\ F & \text{altrimenti.} \end{cases}$$

Si calcoli cioè $I_{\rho_0}(\Phi)$ usando le regole della semantica del primo ordine, dove ρ_0 è un assegnamento arbitrario.

SOLUZIONE ESERCIZIO 5

Soluzione Presentiamo una soluzione parzialmente informale.

Mostriamo che la formula $\Phi = (\forall x \, . \, R(x) \Rightarrow (\exists y \, . \, S(x,y) \wedge \neg R(y)))$ è vera nell'interpretazione data.

- La formula Φ è una **quantificazione universale**, quindi per la regola (S8) è vera se e solo se assegnando a x un qualunque valore d del dominio la formula nella portata è vera, ovvero $I_{\rho_0}(\Phi)$ è vera se, per ogni valore d del dominio, $I_{\rho_0[d/x]}(\Psi)$ è vera, con $\Psi = (R(x) \Rightarrow (\exists y \, . \, S(x,y) \wedge \neg R(y)))$.

- Per la regola (S6), visto che Ψ è un'implicazione, per ogni $d \in D$ abbiamo che $I_{\rho_0[d/x]}(\Psi)$ è falsa se e solo se la premessa $I_{\rho_0[d/x]}(R(x))$ è vera e la conseguenza $I_{\rho_0[d/x]}((\exists y \, . \, S(x,y) \wedge \neg R(y)))$ è falsa. Procediamo per casi esaminando i tre possibili valori di $d \in D$.

  ($d = c$) Per (S1) $I_{\rho_0[c/x]}(R(x))$ è falsa, perché $c \notin \alpha(R)$, quindi $I_{\rho_0[c/x]}(\Psi)$ è vera.

  ($d = a$) Per (S1) $I_{\rho_0[a/x]}(R(x))$ è vera, perché $a \in \alpha(R)$. Quindi $I_{\rho_0[a/x]}(\Psi)$ è vera solo se è vera anche ($\star$) $I_{\rho_0[a/x]}((\exists y \, . \, S(x,y) \wedge \neg R(y)))$. Per (S9), ($\star$) è vera se esiste un valore d' del dominio tale che $I_{\rho_0[a/x][d'/y]}(S(x,y) \wedge \neg R(y))$ è vera. Mostriamo che per $d' = c$ la formula è vera.

  Infatti per (S4) $I_{\rho_0[a/x][c/y]}(S(x,y) \wedge \neg R(y))$ è vera se sono vere sia (†) $I_{\rho_0[a/x][c/y]}(S(x,y))$ che (‡) $I_{\rho_0[a/x][c/y]}(\neg R(y))$. Per (S1) (†) è vera perché $(a,c) \in \alpha(S)$. Per (S3) e (S1) (‡) è vera perché $c \notin \alpha(R)$.

  ($d = b$) Del tutto analogo al caso precedente, osservando che $b \in \alpha(R)$ e $(b,c) \in \alpha(S)$.