Fondamenti di informatica per la sicurezza

anno accademico 2003–2004

docente: Stefano Ferrari

03.02.2004 — Soluzione della prima parte — versione A

Esercizio 1

Effettuare i seguenti cambi di base:

a) $(742)_8 = (???)_{10}$

b) $(89)_{10} = (???)_2$

c) $(E9)_{16} = (???)_2$

d) $(74)_8 = (???)_2$

e) $(60)_7 = (???)_2$

Soluzione

a) $(742)_8 = 7 \cdot 8^2 + 4 \cdot 8^1 + 2 \cdot 8^0 = 7 \cdot 64 + 32 + 2 = 448 + 34 = (482)_{10}$

b) $(89)_{10}$

quoziente	resto
89	
44	1
22	0
11	0
5	1
2	1
1	0
0	1

$(89)_{10} = (1011001)_2$

c) $(E9)_{16}$

E	9
1110	1001

$(E9)_{16} = (11101001)_2$

d) $(74)_8$

7	4
111	100

$(74)_8 = (111100)_2$

e) $(60)_7 = 6 \cdot 7^1 + 0 \cdot 7^0 = 42 + 0 = (42)_{10}$

quoziente	resto
42	
21	0
10	1
5	0
2	1
1	0
0	1

$(60)_7 = (101010)_2$

Esercizio 2

Una banca offre ai propri clienti la possibilità di aprire un conto con diverse caratteristiche:

- tasso di interesse (2%, 2,5%, 3%, 3,5%)
- deposito titoli (SI/NO)
- carta di credito (Visa, Mastercard, American Express)

Si calcoli:

a) il numero di bit necessari per codificare ciascuna delle tre offerte (tasso di interesse, deposito titoli e carta di credito);

b) il numero di bit necessari per codificare la configurazione di un conto corrente.

Soluzione

a)

tasso di interesse	$\lceil \log_2(4) \rceil = 2$
deposito	$\lceil \log_2(2) \rceil = 1$
carta di credito	$\lceil \log_2(3) \rceil = 2$

b) $\lceil \log_2(4 \times 2 \times 3) \rceil = \lceil \log_2(24) \rceil = 5$

Nota: $\lceil x \rceil$ indica il numero intero uguale o immediatamente superiore a x.

Esercizio 3

Dimostrare, tramite tavola di verità se le seguenti formule sono tautologie:

a) $\neg(\neg(q \to q) \vee (\neg(p \wedge r) \vee \neg p))$

b) $\neg r \to \neg(((s \to \neg q) \wedge \neg s) \wedge r)$

Soluzione

a) Non è una tautologia. La tabella di verità è riportata in fig. 1

b) È una tautologia. La tabella di verità è riportata in fig. 2

Esercizio 4

Dimostrare, che le seguenti inferenze sono valide:

a) **Ip1** $\neg(b \rightarrow \neg c)$
   Ip2 $c \rightarrow a$
   Tesi a

b) **Ip1** $\neg(a \rightarrow (b \wedge \neg c))$
   Ip2 b
   Tesi c

c) **Ip1** $\neg(c \vee (a \leftrightarrow b))$
   Ip2 b
   Tesi $\neg a$

Soluzione

a) La soluzione è riportata in fig. 3.

b) La soluzione è riportata in fig. 4.

c) La soluzione è riportata in fig. 5.

Esercizio 5

Formalizzare le seguenti proposizioni:

a) se Bruno corre, Cocchi lo insegue

b) Cocchi è fermo e Aldo non guarda

c) Bruno non corre

d) Aldo guarda se e solo se Bruno corre

e) Cocchi corre e Bruno no

Soluzione

Dati i seguenti simboli proposizionali:

a : Aldo guarda

b : Bruno corre

c : Cocchi corre

le frasi dell'esercizio possono essere formalizzate come:

a) $b \rightarrow c$

b) $\neg c \wedge \neg a$

c) $\neg b$

d) $a \leftrightarrow b$

e) $c \wedge \neg b$

Esercizio 6

Dimostrare che è valida l'inferenza ottenuta prendendo come ipotesi i punti a) e b) dell'esercizio 5 e come tesi il punto c).

Soluzione

Ip1 $b \rightarrow c$

Ip2 $\neg c \wedge \neg a$

Tesi $\neg b$

La dimostrazione è riportata in fig. 6.

p	q	r	$q \to q$	$\neg(q \to q)$	$p \wedge r$	$\neg(p \wedge r)$	$\neg p$	$\neg(p \wedge r) \vee \neg p$	$\alpha \vee \beta$	$\neg(\alpha \vee \beta)$
F	F	F	V	F	F	V	V	V	V	F
F	F	V	V	F	F	V	V	V	V	F
F	V	F	V	F	F	V	V	V	V	F
F	V	V	V	F	F	V	V	V	V	F
V	F	F	V	F	F	V	F	V	V	F
V	F	V	V	F	V	F	F	F	F	V
V	V	F	V	F	F	V	F	V	V	F
V	V	V	V	F	V	F	F	F	F	V
				α				β		

Figura 1: Soluzione dell'esercizio 3a.

q	r	s	$\neg r$	$\neg q$	$s \to \neg q$	$\neg s$	$(s \to \neg q) \wedge \neg s$	$\alpha \wedge r$	$\neg(\alpha \wedge r)$	$\neg r \to \neg(\alpha \wedge r)$
F	F	F	V	V	V	V	V	F	V	V
F	F	V	V	V	V	F	F	F	V	V
F	V	F	F	V	V	V	V	V	F	V
F	V	V	F	V	V	F	F	F	V	V
V	F	F	V	F	V	V	V	F	V	V
V	F	V	V	F	F	F	F	F	V	V
V	V	F	F	F	V	V	V	V	F	V
V	V	V	F	F	F	F	F	F	V	V
							α			

Figura 2: Soluzione dell'esercizio 3b.

(1)	$\neg(\neg b \vee \neg c)$	equivalenza logica a Ip1
(2)	$b \wedge c$	leggi di De Morgan appl. a (1)
(3)	c	elemento di cong. di (2)
(4)	a	*modus ponens* da Ip2 e (3)

Figura 3: Soluzione dell'esercizio 4a.

(1)	$\neg(\neg a \vee (b \wedge \neg c))$	equivalenza logica a Ip1
(2)	$a \wedge \neg(b \wedge \neg c)$	equivalenza logica a (1)
(3)	$\neg(b \wedge \neg c)$	elemento di cong. di (2)
(4)	$\neg b \vee c$	leggi di De Morgan appl. a (3)
(5)	$b \to c$	equivalenza logica a (4)
(6)	c	*modus ponens* da (5) e Ip2

Figura 4: Soluzione dell'esercizio 4b.

(1)	$\neg c \wedge \neg(a \leftrightarrow b)$	equivalenza logica a Ip1
(2)	$\neg(a \leftrightarrow b)$	elemento di cong. di (1)
(3)	$\neg a \leftrightarrow b$	equivalenza logica a (2)
(4)	$(\neg a \to b) \wedge (b \to \neg a)$	equivalenza logica a (3)
(5)	$b \to \neg a$	elemento di cong. di (4)
(6)	$\neg a$	*modus ponens* da (5) e Ip2

Figura 5: Soluzione dell'esercizio 4c.

(1)	$\neg c \to \neg b$	contrapposizione di Ip1
(2)	$\neg c$	elemento di cong. Ip2
(3)	$\neg b$	*modus pones* da (1) e (2)

Figura 6: Soluzione dell'esercizio 6.