Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2003–2004

docente: Stefano Ferrari

Soluzione del primo compitino — 03.11.2003 — versione B

Esercizio 1

Effettuare i seguenti cambi di base:

a) $(632)_8 = (???)_{10}$

b) $(68)_{10} = (???)_2$

c) $(E8)_{16} = (???)_2$

d) $(25)_8 = (???)_2$

e) $(52)_7 = (???)_2$

Soluzione

a) $(632)_8 = 6 \cdot 8^2 + 3 \cdot 8^1 + 2 \cdot 8^0 = 384 + 24 + 2 = (410)_{10}$

b) $(68)_{10}$

quoziente	resto
68	
34	0
17	0
8	1
4	0
2	0
1	0
0	1

$(68)_{10} = (1000100)_2$

c) $(E8)_{16}$

E	8
1110	1000

$(E8)_{16} = (11101000)_2$

d) $(25)_8$

2	5
010	101

$(25)_8 = (10101)_2$

e) $(52)_7 = 5 \cdot 7^1 + 2 \cdot 7^0 = 35 + 2 = (37)_{10}$

quoziente	resto
37	
18	1
9	0
4	1
2	0
1	0
0	1

$(52)_7 = (100101)_2$

Esercizio 2

Una partita di Mastermind è costituito da una sequenza di *passi* costituiti da un *tentativo* e da un *suggerimento*. Ogni tentativo è costituito da una sequenza di quattro[1] elementi scelti fra sette colori, mentre ogni suggerimento è costituito da una sequenza di quattro elementi che possono avere colore bianco, nero o essere *vuoti*.

Si calcoli:

a) il numero di bit necessari per codificare un *tentativo*;

b) il numero di bit necessari per codificare un *suggerimento*;

c) il numero di bit necessari per codificare un *passo*.

Soluzione

a) $\lceil \log_2(7^4) \rceil = \lceil \log_2(2401) \rceil = 12$

b) $\lceil \log_2(3^4) \rceil = \lceil \log_2(81) \rceil = 7$

c) $\lceil \log_2(7^4 \times 3^4) \rceil = \lceil \log_2(2401 \times 81) \rceil = \lceil \log_2(194481) \rceil = 18$

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

[1] Nel tema d'esame originale, per un errore di battitura, il numero di elementi di cui è costituito un tentativo non è stato riportato. Nella valutazione degli elaborati è stata consentita la più ampia interpretazione.

Esercizio 3

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

a) $(\neg((\neg b \leftrightarrow c) \vee \neg(a \leftrightarrow c)) \wedge \neg c) \rightarrow \neg b$

b) $(((b \vee \neg a) \rightarrow \neg(\neg a \rightarrow c)) \wedge \neg a) \rightarrow \neg c$

Soluzione

a) La soluzione è riportata in fig. 1

b) La soluzione è riportata in fig. 2

Esercizio 4

Dimostrare, che le seguenti inferenze sono valide:

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

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

c) **Ip1** $\neg(c \vee b)$
Ip2 $a \rightarrow b$
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) metto i peperoni

b) se si mettono i capperi, non si mettono mai contemporaneamente i peperoni e le alici

c) se metto i capperi, non metto le alici

d) metto i capperi o le alici

e) metto i capperi, i peperoni e le alici

Soluzione

Dati i seguenti simboli proposizionali:

a metto i peperoni

b metto i capperi

c metto le alici

le frasi dell'esercizio possono essere formalizzate come:

a) a

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

c) $b \rightarrow \neg c$

d) $b \vee c$

e) $b \wedge a \wedge c$

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 a

Ip2 $b \rightarrow \neg(a \wedge c)$

Tesi $b \rightarrow \neg c$

La dimostrazione è riportata in fig. 6

a	b	c	$\neg b$	$\neg b \leftrightarrow c$	$a \leftrightarrow c$	$\neg(a \leftrightarrow c)$	$\alpha \vee \beta$	$\neg\gamma$	$\neg c$	$\neg\gamma \wedge \neg c$	$\delta \rightarrow \neg b$
F	F	F	V	F	V	F	F	V	V	V	V
F	F	V	V	V	F	V	V	F	F	F	V
F	V	F	F	V	V	F	V	F	V	F	V
F	V	V	F	F	F	V	V	F	F	F	V
V	F	F	V	F	F	V	V	F	V	F	V
V	F	V	V	V	V	F	V	F	F	F	V
V	V	F	F	V	F	V	V	F	V	F	V
V	V	V	F	F	V	F	F	V	F	F	V
				α		β	γ			δ	

Figura 1: Soluzione dell'esercizio 3a.

a	b	c	$\neg a$	$b \vee \neg a$	$\neg a \rightarrow c$	$\neg(\neg a \rightarrow c)$	$\alpha \rightarrow \beta$	$(\alpha \rightarrow \beta) \wedge \neg a$	$\neg c$	$\gamma \rightarrow \neg c$
F	F	F	V	V	F	V	V	V	V	V
F	F	V	V	V	V	F	F	F	F	V
F	V	F	V	V	F	V	V	V	V	V
F	V	V	V	V	V	F	F	F	F	V
V	F	F	F	F	V	F	V	F	V	V
V	F	V	F	F	V	F	V	F	V	V
V	V	F	F	V	V	F	F	F	V	V
V	V	V	F	V	V	F	F	F	F	V
				α		β		γ		

Figura 2: Soluzione dell'esercizio 3b.

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

Figura 3: Soluzione dell'esercizio 4a.

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

Figura 4: Soluzione dell'esercizio 4b.

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

Figura 5: Soluzione dell'esercizio 4c.

(1)	$\neg b \vee \neg(a \wedge c)$	equivalenza logica a Ip2
(2)	$\neg b \vee \neg a \vee \neg c$	equivalenza logica a (1)
(3)	$\neg a \vee (\neg b \vee \neg c)$	equivalenza logica a (2)
(4)	$a \rightarrow (b \rightarrow \neg c)$	equivalenza logica a (3)
(5)	$b \rightarrow \neg c$	*modus ponens* da Ip1 e (4)

Figura 6: Soluzione dell'esercizio 6.