Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006

docente: Stefano Ferrari

09.11.2005 — Soluzione del primo compitino — versione B

valutazioni **1** (5) ____ **2** (5) ____ **3** (5) ____ **4** (4) ____ **5** (4) ____ **6** (9) ____

Cognome _____ **Nome** _____

Matricola _____ **Firma** _____

Esercizio 1

Per ogni numero k, calcolare il corrispondente numerale nella base n indicata:

a) $k = (514)_7$, $n = 10$

b) $k = (37)_{10}$, $n = 2$

c) $k = (\mathrm{B3})_{16}$, $n = 2$

d) $k = (507)_8$, $n = 2$

e) $k = (45)_6$, $n = 2$

f) $k = (1011101)_2$, $n = 16$

Soluzione

a) $(514)_7 = 5\cdot 7^2 + 1\cdot 7^1 + 4\cdot 7^0 = 5\cdot 49 + 1\cdot 7 + 4\cdot 1 = 245 + 7 + 4 = 256$

$(514)_7 = (256)_{10}$

b)

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

$(37)_{10} = (100101)_2$

c)

base 16	B	3
base 2	1011	0011

$(\mathrm{B3})_{16} = (10110011)_2$

d)

base 8	5	0	7
base 2	101	000	111

$(507)_8 = (101000111)_2$

e) $(45)_6 = 4\cdot 6^1 + 5\cdot 6^0 = 4\cdot 6 + 5\cdot 1 = 24 + 5 = 29$

quoziente	resto
29	
14	1
7	0
3	1
1	1
0	1

$(45)_6 = (11101)_2$

f)

base 2	0101	1101
base 16	5	D

$(1011101)_2 = (5\mathrm{D})_{16}$

Esercizio 2

Dati $a = -10$, $b = 21$ e $n = 5$, calcolare in complemento a 2 a n bit, specificando se si verifica un overflow:

1. le stringhe binarie s_a e s_b che codificano rispettivamente a e b;
2. la somma delle stringhe binarie s_a e s_b;
3. la differenza delle stringhe binarie s_a e s_b.

Soluzione

Con la codifica in complemento a 2 a 5 bit possono essere rappresentati tutti i numeri interi compresi fra -2^{5-1} e $2^{5-1} - 1$. Possono pertanto essere rappresentati senza causare overflow tutti e soli i numeri x che rispettano la condizione $-16 \leq x \leq 15$.

1. $2^n + a = 2^5 - 10 = 22$. Codificando 22 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 10110$.

   Poiché $-16 \leq -10 \leq 15$, non si è verificato un overflow.

$2^n + b = 2^5 + 21 = 53$. Codificando 53 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 10101$.

Poiché $b = 21 > 15$, si è verificato un overflow.

2. La somma binaria di 10110 e 10101, troncata a 5 bit è: $s_a + s_b = 01011$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 01011, si è verificato un overflow.

3. La differenza viene calcolata come somma di s_a e di $-s_b$.

10101		sottraendo, s_b
01010	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
01011	+	$-s_b$
10110	=	s_a
100001		si devono considerare solo gli ultimi 5 bit
00001		$s_a - s_b$

   Poiché s_a e s_b hanno il primo bit uguale, non si è verificato un overflow.

Esercizio 3

In un videogioco, l'alter ego virtuale di un giocatore possiede le seguenti caratteristiche:

- sesso: maschio, femmina;
- colore: rosso, blu, verde, giallo;
- ruolo: mago, ladro, guerriero, nano, avventuriero.

All'interno del gioco è possibile formare delle pattuglie da 4 personaggi, purché dello stesso colore, ma che differiscono tra loro per almeno una delle altre caratteristiche.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (sesso, colore, ruolo);

b) il numero di bit necessari per codificare un personaggio;

c) il numero di bit necessari per codificare le possibili pattuglie.

Soluzione

a)
- 2 generi: $\lceil \log_2 2 \rceil = 1$ bit;
- 4 colori: $\lceil \log_2 4 \rceil = 2$ bit;
- 5 ruoli: $\lceil \log_2 5 \rceil = 3$ bit.

b) Ci sono $2 \times 4 \times 5 = 40$ possibili giocatori, quindi servono $\lceil \log_2 40 \rceil = 6$ bit.

c) Le pattuglie sono sono composte da 4 personaggi dello stesso colore. Poiché devono differire per le altre caratteristiche, non sono ammesse le ripetizioni. L'ordine non appare importante. Quindi, per ogni colore, si potranno avere un numero di pattuglie pari al numero di combinazioni semplici di 10 oggetti (2 generi × 5 ruoli) su 4 posti.

$$\begin{aligned} C(10,\,4) &= \binom{10}{4} = \frac{10!}{6! \cdot 4!} = \\ &= \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2} = \\ &= 10 \cdot 3 \cdot 7 = 2 \cdot 3 \cdot 5 \cdot 7 = 2 \cdot 105 \end{aligned}$$

Poiché sono possibili 4 colori, in totale si avranno $4 \cdot 2 \cdot 105 = 2^3 \cdot 105$ possibili pattuglie. Poiché la prima potenza di 2 che supera 105 è 2^7, per codificare le possibili pattuglie serviranno $\lceil \log_2(2^3 105) \rceil = \lceil \log_2 2^3 + \log_2 105 \rceil = 3 + \lceil \log_2 105 \rceil = 3 + 7 = 10$ bit.

Esercizio 4

Dimostrare, tramite tavola di verità, ***se*** la seguente formula è una tautologia:

a) $p \vee (p \rightarrow (\neg p \rightarrow (q \leftrightarrow \neg(\neg p \wedge r))))$

Soluzione

La tabella di verità è riportata in figura 1. Poiché tutte le interpretazioni rendono vera la proposizione data, essa è una tautologia.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non guida, dorma, e viceversa):

a) se Bice dorme, Antonio o Carlo guidano;

b) Bice e Antonio non guidano;

c) Carlo e Bice dormono, Antonio guida;

d) Antonio dorme solo se anche Carlo fa lo stesso;

e) Bice dorme se e solo se Antonio guida;

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio guida
$\neg a$	Antonio dorme
b	Bice guida
$\neg b$	Bice dorme
c	Carlo guida
$\neg c$	Carlo dorme

le frasi dell'esercizio possono essere formalizzate tramite le seguenti proposizioni:

p	q	r	$\neg p$	$\neg p \wedge r$	$\neg\alpha$	$q \leftrightarrow \neg\alpha$	$\neg p \rightarrow \beta$	$p \rightarrow \gamma$	$p \vee \delta$
F	F	F	V	F	V	F	F	V	V
F	F	V	V	V	F	V	V	V	V
F	V	F	V	F	V	V	V	V	V
F	V	V	V	V	F	F	F	V	V
V	F	F	F	F	V	F	V	V	V
V	F	V	F	F	V	F	V	V	V
V	V	F	F	F	V	V	V	V	V
V	V	V	F	F	V	V	V	V	V
				α		β	γ	δ	

Figura 1: Tabella di verità della proposizione dell'esercizio 4.

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

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

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

d) $\neg a \rightarrow \neg c$

e) $\neg b \leftrightarrow a$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$b \vee (c \wedge a)$	Ip2
(2)	$(b \vee c) \wedge (b \vee a)$	Distributività (1)
(3)	$b \vee a$	Elim. cong. (2)
(4)	$\neg b \rightarrow a$	Def. implicazione (3)
(5)	$\neg a$	Ip1
(6)	b	M. Tollens da (4) e (5)

b)

(1)	$\neg(a \wedge (b \vee c))$	Ip1
(2)	$\neg a \vee \neg(b \vee c)$	Leggi di De Morgan (1)
(3)	$\neg(b \vee c) \vee \neg a$	Commutatività (2)
(4)	$(b \vee c) \rightarrow \neg a$	Def. implicazione (3)
(5)	$a \rightarrow (b \vee c)$	Ip2
(6)	$\neg(b \vee c) \rightarrow \neg a$	Contrapp. di (5)
(7)	$((b \vee c) \rightarrow \neg a) \wedge (\neg(b \vee c) \rightarrow \neg a)$	Cong. di (4) e (6)
(8)	$(((b \vee c) \rightarrow \neg a) \wedge (\neg(b \vee c) \rightarrow \neg a)) \rightarrow \neg a$	Dim. per casi
(9)	$\neg a$	M. Ponens da (7) e (8)

c)

(1)	$a \rightarrow (c \vee \neg b)$	Ip1
(2)	$\neg a \vee (c \vee \neg b)$	Def. Implicazione (1)
(3)	$\neg a \vee c \vee \neg b$	Associatività (2)
(4)	$\neg a \vee \neg b \vee c$	Commutatività (3)
(5)	$\neg(\neg a \vee \neg b) \rightarrow c$	Def. implicazione (4)
(6)	$(a \wedge b) \rightarrow c$	Leggi di De Morgan (5)
(7)	$c \vee (b \wedge a)$	Ip2
(8)	$c \vee (a \wedge b)$	Commutatività (7)
(9)	$(a \wedge b) \vee c$	Commutatività (8)
(10)	$\neg(a \wedge b) \rightarrow c$	Def. implicazione (9)
(11)	c	Dim. per casi da (6) e (10)