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 C

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) $k = (423)_7$, $n = 10$

b) $k = (61)_{10}$, $n = 2$

c) $k = (4\text{C})_{16}$, $n = 2$

d) $k = (315)_8$, $n = 2$

e) $k = (81)_9$, $n = 2$

f) $k = (1001111)_2$, $n = 16$

Soluzione

a) $(423)_7 = 4\cdot 7^2 + 2\cdot 7^1 + 3\cdot 7^0 = 4\cdot 49 + 2\cdot 7 + 3\cdot 1 = 196 + 14 + 3 = 213$

$(423)_7 = (213)_{10}$

b)

quoziente	resto
61	
30	1
15	0
7	1
3	1
1	1
0	1

$(61)_{10} = (111101)_2$

c)

base 16	4	C
base 2	0100	1100

$(4\text{C})_{16} = (1001100)_2$

d)

base 8	3	1	5
base 2	011	001	101

$(315)_8 = (11001101)_2$

e) $(81)_9 = 8\cdot 9^1 + 1\cdot 9^0 = 8\cdot 9 + 1\cdot 1 = 72 + 1 = 73$

quoziente	resto
73	
36	1
18	0
9	0
4	1
2	0
1	0
0	1

$(81)_9 = (1001001)_2$

f)

base 2	0100	1111
base 16	4	F

$(1001111)_2 = (4\text{F})_{16}$

Esercizio 2

Dati $a = -17$, $b = -5$ 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. $2^n + a = 2^5 - 17 = 15$. Codificando 15 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 01111$.

Poiché $a = -17 < -16$, si è verificato un overflow.

$2^n + b = 2^5 - 5 = 27$. Codificando 27 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 11011$.

Poiché $-16 \leq -5 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 01111 e 11011, troncata a 5 bit è: $s_a + s_b = 01010$.

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

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

$$\begin{array}{rcl} 11011 & & \text{sottraendo, } s_b \\ 00100 & + & \text{negazione delle cifre di } s_b,\ \overline{s_b} \\ 1 & = & \\ \hline 00101 & + & -s_b \\ 01111 & = & s_a \\ \hline 10100 & & s_a - s_b \end{array}$$

   Poiché s_a e s_b hanno il primo bit diverso, e il primo bit della loro differenza, 10100, non è uguale al primo bit di s_a, si è verificato un overflow.

Esercizio 3

Un videogioco di corse automobilistiche permette di personalizzare il proprio mezzo specificando le seguenti caratteristiche:

- colore: rosso, giallo, verde, blu;
- pnematici: lisci, da pioggia;
- carburante: pieno, medio, leggero.

All'inizio di ogni gara, viene predisposta una griglia di partenza formata da 5 autovetture. Le auto della stessa griglia si differenziano per colore o pneumatici, ma caricano la stessa quantità di benzina. L'ordine con cui le vetture sono disposte sulla griglia è importante.

Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (colore, pneumatici, carburante);

b) il numero di bit necessari per codificare una automobile;

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

Soluzione

a)
- 4 colori: $\lceil \log_2 4 \rceil = 2$ bit;
- 2 tipi di pneumatici: $\lceil \log_2 2 \rceil = 1$ bit;
- 3 livelli di carburante: $\lceil \log_2 3 \rceil = 2$ bit.

b) Ci sono $4 \times 2 \times 3 = 24$ varianti di autovettura, quindi servono $\lceil \log_2 24 \rceil = 5$ bit.

c) Le griglie di partenza sono sono composte da 5 autovetture con la stessa quantità di carburante. Inoltre, le autovetture si differenziano per colore o tipo di pneumatico, ed anche l'ordine di griglia è importante. Pertanto, non sono ammesse le ripetizioni e va considerato l'ordine. Quindi, per ogni livell odi carburante, si potranno avere un numero di griglie differenti pari al numero di disposizioni semplici di 8 oggetti (4 colori $\times$ 2 tipi di pneumatico) su 5 posti.

$$\begin{aligned} D(8, 5) &= \frac{8!}{3!} = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = \\ &= 2^3 \cdot 7 \cdot 2 \cdot 3 \cdot 5 \cdot 2^2 = \\ &= 2^6 \cdot 7 \cdot 3 \cdot 5 = 2^6 \cdot 105 \end{aligned}$$

In totale si avranno quindi $3 \cdot 2^6 \cdot 105 = 2^6 \cdot 315$ possibili griglie di partenza. Poiché la prima potenza di 2 che supera 315 è 2^9, per codificare le possibili confezioni serviranno $\lceil \log_2 (2^6 \cdot 315) \rceil = \lceil \log_2 2^6 + \log_2 315 \rceil = \lceil 6 + \log_2 315 \rceil = 6 + \lceil \log_2 315 \rceil = 6 + 9 = 15$ bit.

Esercizio 4

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

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

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 corra, salti, e viceversa):

a) se Antonio corre, Bice e Carlo saltano;

b) Carlo salta, Bice e Antonio no;

c) Carlo e Bice corrono;

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

e) Bice salta se e solo se Carlo corre;

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio corre
$\neg a$	Antonio salta
b	Bice corre
$\neg b$	Bice salta
c	Carlo corre
$\neg c$	Carlo salta

p	q	r	$\neg p$	$\neg p \wedge r$	$\neg\alpha$	$q \leftrightarrow \neg\alpha$	$p \vee \neg p$	$p \vee \neg p \vee \beta$	$p \rightarrow \gamma$
F	F	F	V	F	V	F	V	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	V	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	

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

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

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

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

c) $c \wedge b$

d) $c \rightarrow a$

e) $\neg b \leftrightarrow c$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$b \vee (a \wedge \neg c)$	Ip1
(2)	$(a \wedge \neg c) \vee b$	Commutatività (1)
(3)	$\neg(a \wedge \neg c) \rightarrow b$	Def. implicazione (2)
(4)	$(\neg a \vee c) \rightarrow b$	Leggi di De Morgan (3)
(5)	$\neg a$	Ip1
(6)	$\neg a \vee c$	Introd. di disg. (5)
(7)	b	M. Tollens da (4) e (6)

b)

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

c)

(1)	$a \rightarrow (c \vee \neg b)$	Ip1
(2)	$a \rightarrow (\neg b \vee c)$	Commutatività (1)
(3)	$a \rightarrow (b \rightarrow c)$	Def. Implicazione (2)
(4)	$(a \wedge b) \rightarrow c$	Esp. delle premesse (3)
(5)	$(a \wedge b) \vee c$	Ip2
(6)	$\neg(a \wedge b) \rightarrow c$	Def. implicazione (5)
(7)	c	Dim. per casi da (4) e (6)