Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2004–2005

docente: Stefano Ferrari

23.06.2005 — Soluzione della prima parte — versione A

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) $k = (450)_7$, $n = 10$

b) $k = (25)_{10}$, $n = 2$

c) $k = (\mathrm{B7})_{16}$, $n = 2$

d) $k = (246)_8$, $n = 2$

e) $k = (131)_6$, $n = 2$

f) $k = (101001)_2$, $n = 16$

Soluzione

a) $(450)_7 = 4 \cdot 7^2 + 5 \cdot 7^1 + 0 \cdot 7^0 = 4 \cdot 49 + 5 \cdot 7 + 0 \cdot 1 = 196 + 35 + 0 = 231$

$(450)_7 = (231)_{10}$

b)

quoziente	resto
25	
12	1
6	0
3	0
1	1
0	1

$(25)_{10} = (11001)_2$

c)

base 16	B	7
base 2	1011	0111

$(\mathrm{B7})_{16} = (10110111)_2$

d)

base 8	2	4	6
base 2	010	100	110

$(246)_8 = (10100110)_2$

e) $(131)_6 = 1 \cdot 6^2 + 3 \cdot 6^1 + 1 \cdot 6^0 = 1 \cdot 36 + 3 \cdot 6 + 1 \cdot 1 = 36 + 18 + 1 = 55$

quoziente	resto
55	
27	1
13	1
6	1
3	0
1	1
0	1

$(131)_6 = (110111)_2$

f)

base 2	0010	1001
base 16	2	9

$(101001)_2 = (29)_{16}$

Esercizio 2

Dati $a = -3$, $b = 9$ e $n = 4$, 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 4 possono essere rappresentati tutti i numeri interi compresi fra -2^{4-1} e $2^{4-1} - 1$. Possono pertanto essere rappresentati senza causare overflow tutti e soli i numeri x che rispettano la condizione $-8 \leq x \leq 7$.

1. $2^n + a = 2^4 - 3 = 13$. Codificando 13 in binario e troncando tale codifica a 4 bit si ottiene: $s_a = 1101$.

Poiché $-8 \leq -3 \leq 7$, non si è verificato un overflow.

$2^n + b = 2^4 + 9 = 25$. Codificando 25 in binario e troncando tale codifica a 4 bit si ottiene: $s_b = 1001$.

Poiché $b = 9 > 7$, si è verificato un overflow.

2. La somma binaria di 1101 e 1001, troncata a 4 bit è: $s_a + s_b = 0110$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 0110, si è verificato un overflow.

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

1001		sottraendo, s_b
0110	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
0111	+	$-s_b$
1101	=	s_a
10100		si devono considerare solo gli ultimi 4 bit
0100		$s_a - s_b$

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

Esercizio 3

Una azienda produce gelati confezionati con le seguenti caratteristiche:

- tipo: cono ricoperto, ghiacciolo farcito;
- gusto: fragola, limone, cioccolato, vaniglia;
- dimensione: mini, standard, maxi.

L'azienda propone una confezione speciale di 4 gelati, tutti dello stesso tipo.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (tipo, gusto, dimensione);

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

c) il numero di bit necessari per codificare le possibili confezioni a catalogo.

Soluzione

a)
- 2 tipi: $\lceil \log_2 2 \rceil = 1$ bit;
- 4 gusti: $\lceil \log_2 4 \rceil = 2$ bit;
- 3 dimensioni: $\lceil \log_2 3 \rceil = 2$ bit.

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

c) Le confezioni sono sono composte da 4 gelati dello stesso tipo. Sembra ragionevole ammettere le ripetizioni, ma non considerare l'ordine dei gelati nella confezione. Quindi, per ogni tipo, si potranno avere un numero di confezioni pari al numero di combinazioni con ripetizione di 12 oggetti (4 stili $\times$ 3 dimensioni) su 4 posti.

$$\begin{aligned} C_r(12, 4) &= C(12 + 4 - 1, 4) = C(15, 4) = \\ &= \binom{15}{4} = \frac{15!}{11! \cdot 4!} = \\ &= \frac{15 \cdot 14 \cdot 13 \cdot 12}{4 \cdot 3 \cdot 2} = \\ &= 15 \cdot \cdot 7 \cdot 13 = 1365 \end{aligned}$$

In totale si avranno quindi $2 \cdot 1365$ possibili confezioni. Poiché la prima potenza di 2 che supera 1365 è 2^{11}, per codificare le possibili confezioni serviranno $\lceil \log_2(2 \cdot 1365) \rceil = 1 + \lceil \log_2 1 \rceil = 1 + 11 = 12$ bit.

Esercizio 4

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

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

Soluzione

La tabella di verità è riportata in figura 1. Poiché esiste almeno una interpretazione che rende falsa la proposizione data, non è una tautologia.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non parla, ascolti, e viceversa):

a) se Antonio parla, Bice e Carlo ascoltano;

b) Carlo ascolta, Bice e Antonio no;

c) Carlo o Bice parlano;

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

e) Bice ascolta se e solo se Antonio parla;

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio parla
$\neg a$	Antonio ascolta
b	Bice parla
$\neg b$	Bice ascolta
c	Carlo parla
$\neg c$	Carlo ascolta

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

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

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

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

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

c) $c \vee b$

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

e) $\neg b \leftrightarrow a$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$\neg(b \rightarrow c)$	Ip1
(2)	$\neg(\neg b \vee c)$	equiv. logica a (1)
(3)	$\neg\neg b \wedge \neg c$	Leggi di De Morgan (2)
(4)	$\neg c$	Elim. di cong. (3)
(5)	$a \vee c$	Ip2
(6)	$\neg a \rightarrow c$	equiv. logica a (5)
(7)	$\neg\neg a$	M. Tollens da (4) e (6)
(8)	a	Doppia negazione (7)

b)

(1)	$(b \wedge c) \vee a$	Ip1
(2)	$(b \vee a) \wedge (c \vee a)$	equiv. logica a (1)
(3)	$b \vee a$	Elim. di cong. (2)
(4)	$\neg b \rightarrow a$	equiv. logica a (3)
(5)	$\neg b$	Ip2
(6)	a	M. Ponens da (4) e (5)

c)

(1)	$\neg(b \vee (a \leftrightarrow c))$	Ip1
(2)	$\neg b \wedge \neg(a \leftrightarrow c)$	Leggi di De Morgan (1)
(3)	$\neg(a \leftrightarrow c)$	Elim. di cong. (2)
(4)	$\neg a \leftrightarrow c$	Negazione di biimpl. (3)
(5)	$(\neg a \rightarrow c) \wedge (c \rightarrow \neg a)$	equiv. logica a (4)
(6)	$c \rightarrow \neg a$	Elim. di cong. (5)
(7)	c	Ip2
(8)	$\neg a$	M. Ponens da (6) e (7)