Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2004–2005

docente: Stefano Ferrari

25.01.2005 — 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) $k = (314)_7$, $n = 10$

b) $k = (71)_{10}$, $n = 2$

c) $k = (\mathrm{F3})_{16}$, $n = 2$

d) $k = (164)_8$, $n = 2$

e) $k = (312)_6$, $n = 2$

f) $k = (101101)_2$, $n = 16$

Soluzione

a) $(314)_7 = 3\cdot 7^2 + 1\cdot 7^1 + 4\cdot 7^0 = 3\cdot 49 + 1\cdot 7 + 4\cdot 1 = 147 + 7 + 4 = 158$

$(314)_7 = (158)_{10}$

b)

quoziente	resto
71	
35	1
17	1
8	1
4	0
2	0
1	0
0	1

$(71)_{10} = (1000111)_2$

c)

base 16	F	3
base 2	1111	0011

$(\mathrm{F3})_{16} = (11110011)_2$

d)

base 8	1	6	4
base 2	001	110	100

$(164)_8 = (1110100)_2$

e) $(312)_6 = 3\cdot 6^2 + 1\cdot 6^1 + 2\cdot 6^0 = 3\cdot 36 + 1\cdot 6 + 2\cdot 1 = 108 + 6 + 2 = 116$

quoziente	resto
116	
58	0
29	0
14	1
7	0
3	1
1	1
0	1

$(312)_6 = (1110100)_2$

f)

base 2	0010	1101
base 16	2	D

$(101101)_2 = (2\mathrm{D})_{16}$

Esercizio 2

Dati $a = 9$, $b = -13$ 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 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. $2^n + a = 2^5 + 9 = 41$. Codificando 41 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 01001$.

Poiché $-16 \leq 9 \leq 15$, non si è verificato un overflow.

$2^n + b = 2^5 - 13 = 19$. Codificando 19 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 10011$.

Poiché $-16 \leq -13 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 01001 e 10011, troncata a 5 bit è: $s_a + s_b = 11100$.

   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 $-s_b$.

10011		sottraendo, s_b
01100	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
01101	+	$-s_b$
01001	=	s_a
10110		$s_a - s_b$

   Poiché s_a e s_b hanno il primo bit diverso, e il primo bit della loro differenza, 10110, non è uguale al primo bit di s_a, si è verificato un overflow.

Esercizio 3

Un DJ dispone di una ricca raccolta di canzoni e musiche, che si differenziano per:

- nazionalità: italiani, europei, americani;
- periodo: '50, '60, '70, '80, e '90;
- genere: rock, altro.

Il DJ produce compilation costituite da 5 brani. Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (nazionalità, periodo, stile);

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

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

Soluzione

a)
- 3 categorie di nazionalità: $\lceil \log_2 3 \rceil = 2$ bit;
- 5 differenti periodi: $\lceil \log_2 5 \rceil = 3$ bit;
- 2 diversi generi: $\lceil \log_2 2 \rceil = 1$ bit.

b) Ci sono $3 \times 5 \times 2 = 30$ tipi di canzoni, quindi servono $\lceil \log_2 30 \rceil = 5$ bit.

c) Le compilation sono composte mettendo in sequenza 5 brani. Sembra ragionevole non ammettere le ripetizioni e considerare come diverse due raccolte costituite dalle stesse canzoni, ma in ordine differente. Quindi, si potranno avere un numero di compilation pari al numero di disposizioni semplici di 30 oggetti su 5 posti.

$$\begin{aligned} D(30,\,5) &= \frac{30!}{(30-5)!} = \\ &= 30 \cdot 29 \cdot 28 \cdot 27 \cdot 26 = \\ &= 15 \cdot 2 \cdot 29 \cdot 7 \cdot 2^2 \cdot 27 \cdot 13 \cdot 2 = \\ &= 1\,068\,795 \cdot 2^4 \end{aligned}$$

Poiché la prima potenza di 2 che supera $1\,068\,795$ è 2^{21}, per codificare le possibili compilation serviranno $\lceil \log_2(1\,068\,795 \cdot 2^4) \rceil = \lceil \log_2 1\,068\,795 \rceil + 4 = 21 + 4 = 25$ bit.

Una soluzione alternativa prevede che l'ordine non venga considerato al fine di differenziare due compilation composte dagli stessi brani. In tal caso, il numero di compilation possibili è pari alle combinazioni senza ripetizione di 30 oggetti su 5 posti.

$$\begin{aligned} C(30,\,5) &= \binom{30}{5} = \frac{30!}{(30-5)! \cdot 5!} = \\ &= \frac{30 \cdot 29 \cdot 28 \cdot 25 \cdot 26}{5 \cdot 4 \cdot 3 \cdot 2} = \\ &= 29 \cdot 7 \cdot 27 \cdot 13 \cdot 2 = 71\,253 \cdot 2 \end{aligned}$$

Poiché la prima potenza di 2 che supera 71 253 è 2^{17}, per codificare le possibili compilation serviranno, in questo caso, $\lceil \log_2(71\,253 \cdot 2) \rceil = 17 + 1 = 18$ bit.

Esercizio 4

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

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

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:

a) se Aldo corre, Berto e Carla saltano;

b) Berto riposa, così come Aldo e Carla;

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

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

c) Carla o Berto saltano;

d) Aldo riposa solo se anche Carla fa lo stesso;

e) Berto salta se e solo se Aldo corre;

Soluzione

Dati i seguenti simboli proposizionali:

a	Aldo corre
$\neg a$	Aldo riposa
b	Berto salta
$\neg b$	Berto riposa
c	Carla salta
$\neg c$	Carla riposa

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

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

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

c) $c \vee b$

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

e) $b \leftrightarrow a$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	c	Ip2
(2)	$c \rightarrow (c \vee a)$	Introd. di disg.
(3)	$c \vee a$	M. Ponens (1) e (2)
(4)	$(c \vee a) \rightarrow \neg b$	Ip1
(5)	$\neg b$	M. Ponens da (3) e (4)

b)

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

c)

(1)	$\neg c$	Ip2
(2)	$\neg c \rightarrow (c \rightarrow b)$	Ex falso seq. quod.
(3)	$c \rightarrow b$	M. Ponens da (1) e (2)
(4)	$(c \rightarrow b) \rightarrow \neg a$	Ip2
(5)	$\neg a$	M. Ponens da (3) e (4)

(1)	c	Ip2
(2)	$c \rightarrow (c \vee a)$	Introduzione di disgiunzione
(3)	$(c \vee a) \rightarrow \neg b$	Ip1
(4)	$(c \rightarrow (c \vee a)) \wedge ((c \vee a) \rightarrow \neg b)$	cong. di (2) e (3)
(5)	$((c \rightarrow (c \vee a)) \wedge ((c \vee a) \rightarrow \neg b)) \rightarrow (c \rightarrow \neg b)$	Sillogismo ipotetico
(6)	$c \rightarrow \neg b$	M. Ponens da (4) e (5)
(7)	$\neg b$	M. Ponens da (1) e (6)

Figura 2: Soluzione alternativa al teorema 6a.

(1)	$a \vee (b \wedge c)$	Ip1
(2)	$\neg a \rightarrow (b \wedge c)$	equiv. logica a (1)
(3)	$(\neg a \rightarrow b) \wedge (\neg a \rightarrow c)$	Transit. dell'implicazione (2)
(4)	$\neg a \rightarrow c$	elim. cong. (3)
(5)	$\neg c$	Ip2
(6)	a	M. Tollens da (4) e (5)

Figura 3: Soluzione alternativa al teorema 6b.