Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006

docente: Stefano Ferrari

02.12.2005 — 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) $k = (504)_7$, $n = 10$

b) $k = (51)_{10}$, $n = 2$

c) $k = (\mathrm{D3})_{16}$, $n = 2$

d) $k = (364)_8$, $n = 2$

e) $k = (312)_5$, $n = 2$

f) $k = (1001101)_2$, $n = 16$

Soluzione

a) $(504)_7 = 5{\cdot}7^2 + 0{\cdot}7^1 + 4{\cdot}7^0 = 5{\cdot}49 + 0{\cdot}7 + 4{\cdot}1 = 245 + 0 + 4 = 249$

$(504)_7 = (249)_{10}$

b)

quoziente	resto
51	
25	1
12	1
6	0
3	0
1	1
0	1

$(51)_{10} = (110011)_2$

c)

base 16	D	3
base 2	1101	0011

$(\mathrm{D3})_{16} = (11010011)_2$

d)

base 8	3	6	4
base 2	011	110	100

$(364)_8 = (11110100)_2$

e) $(312)_5 = 3{\cdot}5^2 + 1{\cdot}5^1 + 2{\cdot}5^0 = 3{\cdot}25 + 1{\cdot}5 + 2{\cdot}1 = 75 + 5 + 2 = 82$

quoziente	resto
82	
41	0
20	1
10	0
5	0
2	1
1	0
0	1

$(312)_5 = (1010010)_2$

f)

base 2	0100	1101
base 16	4	D

$(1001101)_2 = (\mathrm{4D})_{16}$

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. $2^n + a = 2^5 + 17 = 49$. Codificando 49 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 10001$.

Poiché $a = 17 > 15$, 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 10001 e 11011, troncata a 5 bit è: $s_a + s_b = 01100$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 01100, si è verificato un overflow.

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

11011		sottraendo, s_b
00100	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
00101	+	$-s_b$
10001	=	s_a
10110		$s_a - s_b$

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

Esercizio 3

Un azienda produce fiori di carta, aventi le seguenti caratteristiche:

- tipo: rose, margherite;
- colore: rosso, blu, bianco, giallo, verde;
- dimensione: mini, standard, maxi.

L'azienda vende i fiori in festoni di 5 fiori, tutti della stessa dimensione. I festoni terminano tutte con una composizione di foglie. Si calcoli:

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

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

c) il numero di bit necessari per codificare i possibili festoni.

Soluzione

a)
- 2 tipi: $\lceil \log_2 2 \rceil = 1$ bit;
- 5 colori: $\lceil \log_2 5 \rceil = 3$ bit;
- 3 dimensione: $\lceil \log_2 3 \rceil = 2$ bit.

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

c) I festoni sono composti da 5 topi della stessa dimensione. Un festone è una composizione ad arco, ottenuta disponendo i fiori in fila. Pertanto, l'ordine va considerato. Poiché i capi dei festoni sono ben definiti (la fine ha le foglie, l'inizio no), le simmetrie sono evitate (un singolo festone non può essere utilizzato anche al posto del festone ottenuto elecando i fiori in ordine inverso).

   All'interno dei fiori con la stessa dimensione, quindi, sono ammesse le ripetizioni e va considerato l'ordine dei fiori nel festone. Quindi, per ogni dimensione, si potranno avere un numero di festoni pari al numero di disposizioni con ripetizione di 10 oggetti (2 tipi $\times$ 5 colori) su 5 posti.

$$D_r(10,\, 5) = 10^5 = 2^5 \cdot 5^5 = 2^5 \cdot 3125$$

   Poiché i fiori possono avere 3 dimensioni diverse, in totale si avranno quindi $3 \cdot 2^5 \cdot 3125 = 2^5 \cdot 9375$ possibili festoni. Poiché la prima potenza di 2 che supera 9375 è 2^{14}, per codificare le possibili nidiate serviranno $\lceil \log_2(2^5 \cdot 9375) \rceil = \lceil \log_2 2^5 + \log_2 9375 \rceil = \lceil 5 + \log_2 9375 \rceil = 5 + \lceil \log_2 9375 \rceil = 5 + 14 = 19$ bit.

Esercizio 4

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

a) $(p \land \neg q) \to \neg((\neg q \lor \neg p) \to (\neg r \leftrightarrow r))$

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 guarda, ascolti, e viceversa):

a) Aldo non guarda, Betta e Carla sì;

b) se Aldo guarda, Betta e Carla ascoltano;

c) Carla e Betta ascoltano;

d) Aldo guarda solo se anche Betta fa lo stesso;

e) Carla ascolta se e solo se Aldo guarda;

Soluzione

Dati i seguenti simboli proposizionali:

a	Aldo guarda
$\neg a$	Aldo ascolta
b	Betta guarda
$\neg b$	Betta ascolta
c	Carla guarda
$\neg c$	Carla ascolta

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

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

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

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

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

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

d) $a \to b$

e) $\neg c \leftrightarrow a$

c)

(1)	$a \wedge (a \vee (b \to b))$	Ip1
(2)	a	Elim. di cong. (1)
(3)	$a \to (c \wedge (a \vee b))$	Ip2
(4)	$(a \to c) \wedge (a \to (a \vee b))$	Distr. delle cons. (3)
(5)	$a \to c$	Elim. di cong. (4)
(6)	c	M. Ponens da (2) e (5)

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

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

b)

(1)	$\neg b \to (b \wedge c)$	Ip2
(2)	$(\neg b \to b) \wedge (\neg b \to c)$	Distr. delle cons. (1)
(3)	$\neg b \to b$	Elim. di cong. (2)
(4)	$b \vee b$	Def. implicazione (3)
(5)	b	Idempotenza (4)
(6)	$\neg(a \wedge b)$	Ip1
(7)	$\neg a \vee \neg b$	Leggi di De Morgan (6)
(8)	$\neg b \vee \neg a$	Commutatività (7)
(9)	$b \to \neg a$	Def. implicazione (8)
(10)	$\neg a$	M. Ponens da (5) e (9)