Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

Università degli Studi di Milano — anno accademico 2008–2009 — docente: Stefano Ferrari

29.11.2008 — Soluzione del primo compitino — versione D

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) $k = (523)_7$, $n = 10$

b) $k = (57)_{10}$, $n = 2$

c) $k = (7\mathrm{C})_{16}$, $n = 2$

d) $k = (512)_8$, $n = 2$

e) $k = (410)_5$, $n = 2$

f) $k = (1000111)_2$, $n = 16$

Soluzione

a) $(523)_7 = 5\cdot7^2+2\cdot7^1+3\cdot7^0 = 5\cdot49+2\cdot7+3\cdot1 = 245+14+3 = 262$

$(523)_7 = (262)_{10}$

b)

quoziente	resto
57	
28	1
14	0
7	0
3	1
1	1
0	1

$(57)_{10} = (111001)_2$

c)

base 16	7	C
base 2	0111	1100

$(7\mathrm{C})_{16} = (1111100)_2$

d)

base 8	5	1	2
base 2	101	001	010

$(512)_8 = (101001010)_2$

e) $(410)_5 = 4\cdot5^2+1\cdot5^1+0\cdot5^0 = 4\cdot25+1\cdot5+0\cdot1 = 100+5+0 = 105$

quoziente	resto
105	
52	1
26	0
13	0
6	1
3	0
1	1
0	1

$(410)_5 = (1101001)_2$

f)

base 2	0100	0111
base 16	4	7

$(1000111)_2 = (47)_{16}$

Esercizio 2

Dati $a = 18$, $b = -6$ 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. $2^n+a = 2^5+18 = 50$. Codificando 50 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 10010$.

Poiché $a = 18 > 15$, si è verificato un overflow.

$2^n + b = 2^5 - 6 = 26$. Codificando 26 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 11010$.

Poiché $-16 \leq -6 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 10010 e 11010, 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 $-s_b$.

11010		sottraendo, s_b
00101	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
00110	+	$-s_b$
10010	=	s_a
11000		$s_a - s_b$

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

Esercizio 3

Una azienda editoriale produce adesivi con le seguenti caratteristiche:

- serie: calcio, spazio, orsetti, dinosauri;
- tipo: normale, metallizzato, olografico;
- dimensione: normale, mini.

L'azienda vende gli adesivi in pacchetti da cinque adesivi.

Si calcoli:

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

b) il numero di bit necessari per codificare i possibili adesivi;

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

Soluzione

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

b) Per la regola moltiplicativa, ci sono $4 \times 3 \times 2 = 24$ possibili adesivi, quindi servono $\lceil \log_2 24 \rceil = 5$ bit.

c) Ogni pacchetto è formato da 5 adesivi. E' ragionevole pensare due pacchetti con gli stessi adesivi, ma disposti in sequenza differente si possano ritenere equivalenti. Non essendo specificato se gli adesivi debbano essere diversi, si può pensare che essi debbano essere differenti: dal punto di vista del collezionista, trovare due adesivi identici nello stesso pacchetto sarebbe deludente. In tal caso, il numero di possibili pacchetti è dato dalle combinazioni semplici di 24 oggetti (gli adesivi) su 5 posti (il numero adesivi per pacchetto):

$$\begin{aligned} C(24,\,5) &= \frac{24!}{(24-5)! \cdot 5!} \\ &= \frac{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20}{5 \cdot 4 \cdot 3 \cdot 2} \\ &= 23 \cdot 22 \cdot 21 \cdot 4 = 2^3 \cdot 5313 \end{aligned}$$

Poiché la prima potenza di 2 che supera 5313 è 2^{13}, per codificare i pacchetti serviranno $\lceil \log_2(2^3 \cdot 5313) \rceil = \lceil \log_2 2^3 + \log_2 5313 \rceil = \lceil 3 + \log_2 5313 \rceil = 3 + \lceil \log_2 5313 \rceil = 3 + 13 = 16$ bit.

Una soluzione alternativa può essere ottenuta considerando un altro vincolo: che nei pacchetti ci siano solo adesivi della stessa dimensione. In tal caso, il numero di possibili pacchetti è dato dalle combinazioni semplici di 12 oggetti (gli adesivi di una data dimensione) su 5 posti (il numero adesivi per pacchetto) moltiplicato (per la regola del prodotto) per 2)(il numero di dimensioni):

$$\begin{aligned} C(12,\,5) \times 2 &= \frac{12!}{7! \cdot 5!} \times 2 \\ &= \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{5 \cdot 4 \cdot 3 \cdot 2} \times 2 \\ &= 11 \cdot 9 \cdot 8 \times 2 = 2^4 \cdot 99 \end{aligned}$$

Poiché la prima potenza di 2 che supera 99 è 2^7, per codificare i pacchetti serviranno $\lceil \log_2(2^4 \cdot 99) \rceil = \lceil \log_2 2^4 + \log_2 99 \rceil = \lceil 4 + \log_2 99 \rceil = 4 + \lceil \log_2 99 \rceil = 4 + 7 = 11$ bit.

Analoghe soluzioni alternative possono essere ottenute considerando pacchetti composti con adesivi della stessa serie o tipo.

Esercizio 4

Sia data la seguente formula, F:

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

a) Costruire la tavola di verità di F.

b) F è una tautologia? Motivare la risposta.

Soluzione

a) La tabella di verità di F è riportata in figura 1.

b) Poiché almeno una interpretazione rende falsa la proposizione F, essa non è una tautologia.

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

Figura 1: Tabella di verità dell'esercizio 4a.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non colora, disegni, e viceversa):

a) Antonio colora solo se colora anche Bice;

b) quando Antonio disegna, Bice e Carlo non colorano;

c) sia Carlo, sia Bice disegnano;

d) Bice disegna se e solo se Antonio e Carlo colorano;

e) Carlo non colora, Bice o Antonio sì.

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio colora
$\neg a$	Antonio disegna
b	Bice colora
$\neg b$	Bice disegna
c	Carlo colora
$\neg c$	Carlo disegna

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

a) $a \rightarrow b$

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

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

d) $\neg b \leftrightarrow (a \wedge c)$

e) $\neg c \wedge (b \vee a)$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$\neg(a \rightarrow \neg b)$	Ip1
(2)	$\neg(\neg a \vee \neg b)$	Def. implicazione (1)
(3)	$a \wedge b$	Legge di De Morgan (2)
(4)	a	Elim. congiunzione (3)
(5)	$a \rightarrow \neg c$	Ip2
(6)	$\neg c$	Modus ponens (4) e (5)

b)

(1)	$\neg((a \leftrightarrow c) \vee (\neg a \wedge b))$	Ip1
(2)	$\neg(a \leftrightarrow c) \wedge \neg(\neg a \wedge b))$	De Morgan (1)
(3)	$\neg(a \leftrightarrow c)$	Elim. cong. (2)
(4)	$\neg a \leftrightarrow c$	Neg. di biimpl. (3)
(5)	$(\neg a \rightarrow c) \wedge (c \rightarrow \neg a)$	Def. biimpl. (4)
(6)	$c \rightarrow \neg a$	Elim. cong. (5)
(7)	c	Ip2
(8)	$\neg a$	M. tollens (6) e (7)
(9)	$\neg(b \wedge \neg a)$	Elim. cong. (2)
(10)	$\neg b \vee a$	De Morgan (9)
(11)	$\neg b$	Sill. disg. (8) e (10)

c)

(1)	$\neg(c \rightarrow b)$	Ip2
(2)	$\neg(\neg c \vee b)$	Def. implicazione (1)
(3)	$c \wedge \neg b$	Legge di De Morgan (2)
(4)	$\neg b$	Elim. congiunzione (3)
(5)	$a \vee b$	Ip1
(6)	$\neg a \rightarrow b$	Def. implicazione (5)
(7)	a	Modus tollens (4) e (6)