Fondamenti di informatica per la sicurezza

UNIVERSITÀ DEGLI STUDI DI MILANO

anno accademico 2006–2007 docente: Stefano FERRARI

31.10.2006 — Soluzione del primo compitino — 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) $k = (503)_7$, $n = 10$

b) $k = (41)_{10}$, $n = 2$

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

d) $k = (235)_8$, $n = 2$

e) $k = (140)_5$, $n = 2$

f) $k = (1010011)_2$, $n = 16$

Soluzione

a) $(503)_7 = 5{\cdot}7^2{+}0{\cdot}7^1{+}3{\cdot}7^0 = 5{\cdot}49{+}0{\cdot}7{+}3{\cdot}1 = 245 + 0 + 3 = 248$

$(503)_7 = (248)_{10}$

b)

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

$(41)_{10} = (101001)_2$

c)

base 16	2	A
base 2	0010	1010

$(2\text{A})_{16} = (101010)_2$

d)

base 8	2	3	5
base 2	010	011	101

$(235)_8 = (10011101)_2$

e) $(140)_5 = 1{\cdot}5^2{+}4{\cdot}5^1{+}0{\cdot}5^0 = 1{\cdot}25{+}4{\cdot}5{+}0{\cdot}1 = 25 + 20 + 0 = 45$

quoziente	resto
45	
22	1
11	0
5	1
2	1
1	0
0	1

$(140)_5 = (101101)_2$

f)

base 2	0101	0011
base 16	5	3

$(1010011)_2 = (53)_{16}$

Esercizio 2

Dati $a = -18$, $b = 4$ 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. $2^n{+}a = 2^5{-}18 = 14$. Codificando 14 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 01110$.

Poiché $a = -18 < -16$, si è verificato un overflow.

$2^n + b = 2^5 + 4 = 36$. Codificando 36 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 00100$.

Poiché $-16 \leq 4 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 01110 e 00100, troncata a 5 bit è: $s_a + s_b = 10010$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 10010, si è verificato un overflow.

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

00100		sottraendo, s_b
11011	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
11100	+	$-s_b$
01110	=	s_a
101010		si devono considerare solo gli ultimi 5 bit
01010		$s_a - s_b$

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

Esercizio 3

Una azienda tessile confeziona maglie a strisce orizzontali assemblando strisce di tessuto aventi le seguenti caratteristiche:

- colore: verde, rosso, giallo, blu, bianco, nero;
- tono: chiaro, scuro, brillante;
- materiale: lana, cotone.

Considerando che ogni maglia è composta da tre strisce dello stesso materiale, ma di colore e tono differente, si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (colore, tono e materiale);

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

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

Soluzione

a)
- 6 colori: $\lceil \log_2 6 \rceil = 3$ bit;
- 3 toni: $\lceil \log_2 3 \rceil = 2$ bit;
- 2 materiali: $\lceil \log_2 2 \rceil = 1$ bit.

b) Per la regola moltiplicativa, ci sono $6 \times 3 \times 2 = 36$ possibili strisce, quindi servono $\lceil \log_2 36 \rceil = 6$ bit.

c) Ogni maglia è composta da tre strisce dello stesso materiale, ma che si differenziano tra loro sia per colore, sia per tono. Poiché appare ragionevole pensare che una maglia formata rispettivamente da una striscia blu, una bianca e una rossa appaia differente da una maglia formata da una striscia bianca, una blu e una rossa, si può ritenere che l'ordine degli oggetti abbia importanza. Inoltre, le specifiche del problema richiedono che, all'interno delle strisce dello stesso materiale usate per confezionare una maglia, non possano esserci ripetizioni. Pertanto, per ogni materiale, il numero di configurazioni che possono essere assunte da una maglia è dato dalle disposizioni semplici di 18 elementi (6 colori $\times$ 3 toni) su 3 posti (le strisce):

$$D(18,\,3) = 18 \cdot 17 \cdot 16 = 9 \cdot 2 \cdot 17 \cdot 2^4$$
$$= 2^5 \cdot 153$$

Si potranno quindi avere $2 \cdot 2^5 \cdot 153 = 2^6 \cdot 105$ possibili maglie (perché per ogni materiale si potranno avere $2^5 \cdot 153$ maglie differenti). Poiché la prima potenza di 2 che supera 153 è 2^8, per codificare le possibili maglie serviranno $\lceil \log_2(2^6 \cdot 153) \rceil = \lceil \log_2 2^6 + \log_2 153 \rceil = \lceil 6 + \log_2 153 \rceil = 6 + \lceil \log_2 153 \rceil = 6 + 8 = 14$ bit.

Esercizio 4

Sia data la seguente formula, F:

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

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.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non disegna, scriva, e viceversa):

a) se Antonio disegna, Bice e Carlo scrivono;

b) Carlo non scrive, Bice o Antonio sì;

c) Carlo oppure Bice scrivono;

d) Antonio disegna solo se anche Bice fa lo stesso;

e) Bice scrive se e solo se Antonio e Carlo disegnano.

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

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

Soluzione

Dati i seguenti simboli proposizionali:

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

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

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

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

c) $\neg c \vee \neg b$

d) $a \to b$

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

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$\neg c \vee (a \wedge b)$	Ip2
(2)	$(\neg c \vee a) \wedge (\neg c \vee b)$	Distributività (1)
(3)	$\neg c \vee a$	Elim. congiunzione (2)
(4)	$c \to a$	Def. implicazione (3)
(5)	$\neg a$	Ip1
(6)	$\neg c$	Modus Tollens (4) e (5)

b)

(1)	$\neg(a \wedge (b \vee c))$	Ip2
(2)	$\neg a \vee \neg(b \vee c)$	Legge di De Morgan (1)
(3)	$\neg(b \vee c) \vee \neg a$	Commutatività (2)
(4)	$(b \vee c) \to \neg a$	Def. implicazione (3)
(5)	$\neg(c \vee b) \to \neg a$	Ip1
(6)	$\neg a$	Dim. per casi (4) e (5)

c)

(1)	$c \to (a \vee \neg b)$	Ip2
(2)	$\neg c \vee (a \vee \neg b)$	Def. implicazione (1)
(3)	$\neg c \vee a \vee \neg b$	Associatività (2)
(4)	$\neg c \vee \neg b \vee a$	Commutatività (3)
(5)	$(\neg c \vee \neg b) \vee a$	Associatività (4)
(6)	$\neg(\neg c \vee \neg b) \to a$	Def. implicazione (5)
(7)	$(c \wedge b) \to a$	Legge di De Morgan (6)
(8)	$(b \wedge c) \to a$	Associatività (7)
(9)	$a \vee (b \wedge c)$	Ip1
(10)	$(b \wedge c) \vee a$	Commutatività (9)
(11)	$\neg(b \wedge c) \to a$	Def. implicazione (10)
(12)	a	Dim. per casi (8) e (11)