Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

Università degli Studi di Milano

anno accademico 2007–2008 docente: Stefano Ferrari

05.11.2007 — Soluzione del primo compitino — versione C

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) $k = (514)_7$, $n = 10$

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

c) $k = (3B)_{16}$, $n = 2$

d) $k = (175)_8$, $n = 2$

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

f) $k = (1001001)_2$, $n = 16$

Soluzione

a) $(514)_7 = 5 \cdot 7^2 + 1 \cdot 7^1 + 4 \cdot 7^0 = 5 \cdot 49 + 1 \cdot 7 + 4 \cdot 1 = 245 + 7 + 4 = 256$

$(514)_7 = (256)_{10}$

b)

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

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

c)

base 16	3	B
base 2	0011	1011

$(3B)_{16} = (111011)_2$

d)

base 8	1	7	5
base 2	001	111	101

$(175)_8 = (1111101)_2$

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	1001
base 16	4	9

$(1001001)_2 = (49)_{16}$

Esercizio 2

Dati $a = -1$, $b = 18$ e $n = 5$, calcolare in complemento a 2 a n bit, specificando sempre 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. $2^n + a = 2^5 - 1 = 31$. Codificando 31 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 11111$.

Poiché $-16 \leq -1 \leq 15$, non si è verificato un overflow.

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

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

2. La somma binaria di 11111 e 10010, troncata a 5 bit è: $s_a + s_b = 10001$. Poiché s_a e s_b hanno il primo bit uguale, e uguale anche al primo bit della loro somma, 10001, non si è verificato un overflow.

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

10010		sottraendo, s_b
01101	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
01110	+	$-s_b$
11111	=	s_a
101101		si devono considerare solo gli ultimi 5 bit
01101		$s_a - s_b$

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

Esercizio 3

Una casa produttrice di automobili permette all'acquirente di scegliere le seguenti caratteristiche dell'automobile:

- verniciatura: metallizzato o non metallizzato;
- colore: bianco, nero, rosso, verde, grigio, blu;
- optional: cerchi in lega, alzacristalli elettrico, lettore MP3, navigatore satellitare, interni in radica, tettuccio apribile, interni in pelle.

Ogni automobile viene assemblata utilizzando una sola caratteristica per categoria.

Inoltre, vengono anche assemblate automobili *deluxe* che contengono tre optional differenti.

Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (vernice, colore, optional);

b) il numero di bit necessari per codificare le possibili automobili (modello base);

c) il numero di bit necessari per codificare le possibili automobili *deluxe*.

Soluzione

a)
- 2 verniciature: $\lceil \log_2 2 \rceil = 1$ bit;
- 6 colori: $\lceil \log_2 6 \rceil = 3$ bit;
- 7 optional: $\lceil \log_2 7 \rceil = 3$ bit.

b) Per la regola moltiplicativa, ci sono $2 \times 6 \times 7 = 84$ possibili automobili, quindi servono $\lceil \log_2 84 \rceil = 7$ bit.

c) Ogni automobile *deluxe* è caratterizzata da una verniciatura, un colore e tre optional differenti. Poiché l'ordine non ha importanza e non possono esserci ripetizioni, i gruppi di tre optional possono essere calcolati come le combinazioni di 7 elementi (gli optional) su 3 posti (il numero di optional per automobile *deluxe*):

$$C(7,\,3) = \frac{7!}{4!\,3!} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} 7 \cdot 5 = 35$$

Si potranno quindi avere $35 \cdot 2 \cdot 6 = 2^2 \cdot 105$ possibili automobili *deluxe* (perché per ogni gruppo di tre optional si potranno avere due di verniciature e 6 colori differenti). Poiché la prima potenza di 2 che supera 105 è 2^7, per codificare le possibili automobili *deluxe* serviranno $\lceil \log_2 (2^2 \cdot 105) \rceil = \lceil \log_2 2^2 + \log_2 105 \rceil = \lceil 2 + \log_2 105 \rceil = 2 + \lceil \log_2 105 \rceil = 2 + 7 = 9$ bit.

Esercizio 4

Sia data la seguente formula, F:

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

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 rotola, strisci, e viceversa):

a) Carlo non striscia, Bice o Antonio sì;

b) Antonio striscia solo se striscia anche Bice;

c) quando Antonio striscia, Bice e Carlo rotolano;

d) Bice rotola se e solo se Antonio e Carlo strisciano;

e) sia Carlo, sia Bice rotolano.

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

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

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio striscia
$\neg a$	Antonio rotola
b	Bice striscia
$\neg b$	Bice rotola
c	Carlo striscia
$\neg c$	Carlo rotola

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

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

b) $a \rightarrow b$

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

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

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

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

a) **Ip1** $a \rightarrow b$

Ip2 $(a \rightarrow \neg b) \wedge c$

Tesi $\neg a$

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

Ip2 c

Tesi $\neg a$

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

Ip2 c

Tesi $\neg b$

Soluzione

a)

(1)	$a \rightarrow b$	Ip1
(2)	$\neg b \rightarrow \neg a$	Contrapp. (1)
(3)	$(a \rightarrow \neg b) \wedge c$	Ip2
(4)	$a \rightarrow \neg b$	Elim. congiunzione (3)
(5)	$b \rightarrow \neg a$	Contrapp. (4)
(6)	$\neg a$	Dim. per casi (2) e (5)

b)

(1)	$\neg(b \vee (a \leftrightarrow c))$	Ip1
(2)	$\neg b \wedge \neg(a \leftrightarrow c))$	L. di 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. di biimpl. (4)
(6)	$c \rightarrow \neg a$	Elim. cong. (5)
(7)	c	Ip2
(8)	$\neg a$	M. ponens (6) e (7)

c)

(1)	$\neg((c \leftrightarrow a) \vee (b \wedge \neg a))$	Ip1
(2)	$\neg(c \leftrightarrow a) \wedge \neg(b \wedge \neg a))$	De Morgan (1)
(3)	$\neg(c \leftrightarrow a)$	Elim. cong. (2)
(4)	$\neg c \leftrightarrow a$	Neg. di biimpl. (3)
(5)	$(\neg c \rightarrow a) \wedge (a \rightarrow \neg c)$	Def. biimpl. (4)
(6)	$a \rightarrow \neg c$	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)