Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

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 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) $k = (612)_7$, $n = 10$

b) $k = (59)_{10}$, $n = 2$

c) $k = (\mathrm{C3})_{16}$, $n = 2$

d) $k = (417)_8$, $n = 2$

e) $k = (54)_6$, $n = 2$

f) $k = (1101101)_2$, $n = 16$

Soluzione

a) $(612)_7 = 6 \cdot 7^2 + 1 \cdot 7^1 + 2 \cdot 7^0 = 6 \cdot 49 + 1 \cdot 7 + 2 \cdot 1 = 294 + 7 + 2 = 303$

$(612)_7 = (303)_{10}$

b)

quoziente	resto
59	
29	1
14	1
7	0
3	1
1	1
0	1

$(59)_{10} = (111011)_2$

c)

base 16	C	3
base 2	1100	0011

$(\mathrm{C3})_{16} = (11000011)_2$

d)

base 8	4	1	7
base 2	100	001	111

$(417)_8 = (100001111)_2$

e) $(54)_6 = 5 \cdot 6^1 + 4 \cdot 6^0 = 5 \cdot 6 + 4 \cdot 1 = 30 + 4 = 34$

quoziente	resto
34	
17	0
8	1
4	0
2	0
1	0
0	1

$(54)_6 = (100010)_2$

f)

base 2	0110	1101
base 16	6	D

$(1101101)_2 = (\mathrm{6D})_{16}$

Esercizio 2

Dati $a = -10$, $b = 18$ 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. $2^n + a = 2^5 - 10 = 22$. Codificando 22 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 10110$.

   Poiché $-16 \leq -10 \leq 15$, 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 10110 e 10010, troncata a 5 bit è: $s_a + s_b = 01000$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 01000, 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	+	$-s_b$
10110	=	s_a
100100		si devono considerare solo gli ultimi 5 bit
00100		$s_a - s_b$

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

Esercizio 3

Un negozio di bigiotteria assembla collane utilizzando perline con differenti caratteristiche:

- materiale: pietra, plastica, legno;
- colore: rosso, bianco, verde, giallo, blu;
- forma: circolare, quadrata, triangolare, sferica.

Le collane vengono assemblate inserendo da ciascuna estremità del filo due perline identiche, ripetendo questa operazione quattro volte.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica delle perline (materiale, colore, forma);

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

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

Soluzione

a)
- 3 materiali: $\lceil \log_2 3 \rceil = 2$ bit.
- 5 colori: $\lceil \log_2 5 \rceil = 3$ bit;
- 4 forme: $\lceil \log_2 4 \rceil = 2$ bit;

b) Per la regola moltiplicativa, ci sono $3 \times 5 \times 4 = 60$ possibili perline, quindi servono $\lceil \log_2 60 \rceil = 6$ bit.

c) Ogni collana è composta da quattro coppie di perline disposte simmetricamente. Questo fatto evita di dover considerare diversi orientamenti della collana: se si infilasse una pietra alla volta, la collana formata, nell'ordine, da una pietra circolare rossa, una bianca, una verde, e una gialla, potrebbe essere anche ottenuta infilando le stesse pietre ma nell'ordine inverso e poi girando la collana. Quindi, sembra ragionevole pensare che l'ordine delle perline abbia importanza e che possano esserci ripetizioni (nessuna specifica a riguardo). Pertanto, il numero di configurazioni che possono essere assunte da una collana è dato dalle disposizioni con ripetizione di 60 elementi (le perline) su 4 posti (le coppie):

$$D_r(60,\, 4) = 60^4 = (2^2 \cdot 3 \cdot 5)^4 = 2^8 \cdot 50625$$

Poiché la prima potenza di 2 che supera 50625 è 2^{16}, per codificare le possibili collane serviranno $\lceil \log_2(2^8 \cdot 50625) \rceil = \lceil \log_2 2^8 + \log_2 50625 \rceil = \lceil 8 + \log_2 50625 \rceil = 8 + \lceil \log_2 50625 \rceil = 8 + 16 = 24$ bit.

Esercizio 4

Sia data la seguente formula, F:

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

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 lava, stiri, e viceversa):

a) Bice e Antonio non lavano;

b) se Bice o Carlo lavano, Antonio stira;

c) Antonio stira solo se anche Carlo fa lo stesso;

d) Carlo o Bice lavano, Antonio stira;

e) Bice lava se e solo se Antonio stira.

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

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

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio lava
$\neg a$	Antonio stira
b	Bice lava
$\neg b$	Bice stira
c	Carlo lava
$\neg c$	Carlo stira

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

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

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

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

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

e) $b \leftrightarrow \neg a$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

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

b)

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

c)

(1)	$b \rightarrow (c \wedge a)$	Ip2
(2)	$(b \rightarrow c) \wedge (b \rightarrow a)$	Distrib. delle conseg. (1)
(3)	$b \rightarrow c$	Elim. congiunzione (2)
(4)	b	Ip1
(5)	$\neg a \vee b$	Introd. disgiunzione (4)
(6)	$a \rightarrow b$	Def. implicazione (5)
(7)	$(a \rightarrow b) \wedge (b \rightarrow c)$	Congiunzione di (6) e (3)
(8)	$a \rightarrow c$	Sillogismo ipotetico (7)