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 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) $k = (243)_7$, $n = 10$

b) $k = (53)_{10}$, $n = 2$

c) $k = (\mathrm{C4})_{16}$, $n = 2$

d) $k = (350)_8$, $n = 2$

e) $k = (83)_9$, $n = 2$

f) $k = (1111001)_2$, $n = 16$

Soluzione

a) $(243)_7 = 2\cdot 7^2 + 4\cdot 7^1 + 3\cdot 7^0 = 2\cdot 49 + 4\cdot 7 + 3\cdot 1 = 98 + 28 + 3 = 129$

$(243)_7 = (129)_{10}$

b)

quoziente	resto
53	
26	1
13	0
6	1
3	0
1	1
0	1

$(53)_{10} = (110101)_2$

c)

base 16	C	4
base 2	1100	0100

$(\mathrm{C4})_{16} = (11000100)_2$

d)

base 8	3	5	0
base 2	011	101	000

$(350)_8 = (11101000)_2$

e) $(83)_9 = 8\cdot 9^1 + 3\cdot 9^0 = 8\cdot 9 + 3\cdot 1 = 72 + 3 = 75$

quoziente	resto
75	
37	1
18	1
9	0
4	1
2	0
1	0
0	1

$(83)_9 = (1001011)_2$

f)

base 2	0111	1001
base 16	7	9

$(1111001)_2 = (79)_{16}$

Esercizio 2

Dati $a = -15$, $b = -7$ 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. $2^n + a = 2^5 - 15 = 17$. Codificando 17 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 10001$.

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

$2^n + b = 2^5 - 7 = 25$. Codificando 25 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 11001$.

Poiché $-16 \leq -7 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 10001 e 11001, troncata a 5 bit è: $s_a + s_b = 01010$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 01010, si è verificato un overflow.

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

11001		sottraendo, s_b
00110	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
00111	+	$-s_b$
10001	=	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

Un negozio di numismatica vende monete della zona euro con le seguenti caratteristiche:

- anno: 2002, 2003, 2004, 2005;
- paese: Italia, Spagna, Germania;
- valore: 1 euro, 2 euro.

Il negozio vende inoltre un pacchetto per collezionisti composto da 10 monete differenti.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (anno, paese, valore);

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

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

Soluzione

a)
- 4 anni: $\lceil \log_2 4 \rceil = 2$ bit;
- 3 paesi: $\lceil \log_2 3 \rceil = 2$ bit;
- 2 valori: $\lceil \log_2 2 \rceil = 1$ bit.

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

c) Ogni pacchetto è composto da 10 monete differenti tra loro. A meno che la particolare disposizione delle mote all'interno del pacchetto non sia un elemento per distinguere due pacchetti che contengono le stesse monete (cioè a meno che il pacchetto stesso non sia oggetto di collezione), l'ordine all'interno del pacchetto non ha importanza. Quindi, sembra ragionevole pensare che l'ordine delle monete non abbia importanza e che non possano esserci ripetizioni (per specifica del problema). Pertanto, il numero di differenti pacchetti è dato dalle combinazioni semplici di 24 elementi (le monete) su 10 posti (il numero di monete per pacchetto):

$$
\begin{aligned}
C(24,\,10) &= \frac{24!}{(24-10)!10!} \\
&= \frac{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15}{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} \\
&= 23 \cdot 22 \cdot 3 \cdot 19 \cdot 2 \cdot 17 \cdot 2 \\
&= 2^3 \cdot 3 \cdot 11 \cdot 17 \cdot 19 \cdot 23 = 2^3 \cdot 245157
\end{aligned}
$$

Poiché la prima potenza di 2 che supera 245157 è 2^{18}, per codificare i possibili pacchetti serviranno $\lceil \log_2(2^3 \cdot 245157) \rceil = \lceil \log_2 2^3 + \log_2 245157 \rceil = \lceil 3 + \log_2 245157 \rceil = 3 + \lceil \log_2 245157 \rceil = 3 + 18 = 21$ bit.

Nota: Ipotizzare che all'interno del pacchetto le monete siano disposte in un qualche ordine particolare (per esempio, in ordine di valore), non cambia il conteggio dei possibili pacchetti. Infatti, ipotizzare tale ordine significherebbe rendere irriconoscibili (cioe' riconoscere come lo stesso pacchetto) due pacchetti costituiti dalle stesse monete.

Esercizio 4

Sia data la seguente formula, F:

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

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 tutte le interpretazioni rendono vera la proposizione F, essa è una tautologia.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non cammina, corra, e viceversa):

a) se Antonio corre, Bice e Carlo camminano;

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

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

b) Carlo cammina, Bice e Antonio no;

c) Carlo e Bice corrono;

d) Carlo corre solo se anche Antonio fa lo stesso;

e) Bice o Antonio camminano se e solo se Carlo corre.

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio corre
$\neg a$	Antonio cammina
b	Bice corre
$\neg b$	Bice cammina
c	Carlo corre
$\neg c$	Carlo cammina

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

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

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

c) $c \wedge b$

d) $c \rightarrow a$

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

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$a \vee (b \wedge \neg c)$	Ip1
(2)	$(a \vee b) \wedge (a \vee \neg c)$	Distributività (1)
(3)	$a \vee b$	Elim. congiunzione (2)
(4)	$\neg a \rightarrow b$	Def. implicazione (3)
(5)	$\neg b$	Ip2
(6)	$(\neg a \rightarrow b) \wedge \neg b$	Congiunzione di (4) e (5)
(7)	$((\neg a \rightarrow b) \wedge \neg b) \rightarrow a$	Dim. per assurdo
(8)	a	Modus Ponens (6) e (7)

b)

(1)	$\neg c \rightarrow (\neg b \wedge a)$	Ip2
(2)	$\neg c$	Ip1
(3)	$\neg b \wedge a$	Modus Ponens (1) e (2)
(4)	a	Elim. congiunzione (3)
(5)	$a \vee b$	Intr. disgiunzione (4)
(6)	$\neg a \rightarrow b$	Def. implicazione (5)

c)

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