Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2004–2005

docente: Stefano Ferrari

22.01.2005 — Soluzione della prima parte — 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) $k = (341)_7$, $n = 10$

b) $k = (70)_{10}$, $n = 2$

c) $k = (\mathrm{F1})_{16}$, $n = 2$

d) $k = (170)_8$, $n = 2$

e) $k = (152)_6$, $n = 2$

f) $k = (101011)_2$, $n = 16$

Soluzione

a) $(341)_7 = 3\cdot 7^2 + 4\cdot 7^1 + 1\cdot 7^0 = 3\cdot 49 + 4\cdot 7 + 1\cdot 1 = 147 + 28 + 1 = 176$

$(341)_7 = (176)_{10}$

b)

quoziente	resto
70	
35	0
17	1
8	1
4	0
2	0
1	0
0	1

$(70)_{10} = (1000110)_2$

c)

base 16	F	1
base 2	1111	0001

$(\mathrm{F1})_{16} = (11110001)_2$

d)

base 8	1	7	0
base 2	001	111	000

$(170)_8 = (1111000)_2$

e) $(152)_6 = 1\cdot 6^2 + 5\cdot 6^1 + 2\cdot 6^0 = 1\cdot 36 + 5\cdot 6 + 2\cdot 1 = 36 + 30 + 2 = 68$

quoziente	resto
68	
34	0
17	0
8	1
4	0
2	0
1	0
0	1

$(152)_6 = (1000100)_2$

f)

base 2	0010	1011
base 16	2	B

$(101011)_2 = (2\mathrm{B})_{16}$

Esercizio 2

Dati $a = -9$, $b = 3$ e $n = 4$, calcolare in complemento a 2 a n bit, specificando se si verifica un overflow:

a) la codifica di a, s_a, e di b, s_b;

b) la somma delle stringhe binarie s_a e s_b;

c) la differenza delle stringhe binarie s_a e s_b.

Soluzione

Con la codifica in complemento a 2 a 4 possono essere rappresentati tutti i numeri interi compresi fra -2^{4-1} e $2^{4-1} - 1$. Possono pertanto essere rappresentati senza causare overflow tutti e soli i numeri x che rispettano la condizione $-8 \leq x \leq 7$.

1. $2^n + a = 2^4 - 9 = 7$. Codificando 7 in binario e troncando tale codifica a 4 bit si ottiene: $s_a = 0111$.

Poiché $a = -9 < -8$, si è verificato un overflow.

$2^n + b = 2^4 + 3 = 19$. Codificando 19 in binario e troncando tale codifica a 4 bit si ottiene: $s_b = 0011$.

Poiché $-8 \leq 3 \leq 7$, non si è verificato un overflow.

2. La somma binaria di 0111 e 0011, troncata a 4 bit è: $s_a + s_b = 1010$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 1010, si è verificato un overflow.

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

0011		sottraendo, s_b
1100	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
1101	+	$-s_b$
0111	=	s_a
10100		si devono considerare solo gli ultimi 4 bit
0100		$s_a - s_b$

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

Esercizio 3

Una azienda che produce materassi utilizza pannelli con le seguenti caratteristiche:

- materiale: schiuma, lattice, cocco, poliuretano;
- spessore: 1, 2, 3, 4, e 5 cm;
- lunghezza: 120, 200 cm.

L'azienda produce materassi sovrapponendo 3 pannelli con caratteristiche differenti, ovviamente della stessa lunghezza. Per ottenere un materasso simmetrico rispetto ai due lati, tale sequenza viene poi ripetuta in modo identico, ma invertito . Il grado di morbidezza e di adattabilità di un materasso dipende dal materiale, dallo spessore e dalla sequenza dei pannelli che lo compongono.

Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (materiale, spessore, lunghezza);

b) il numero di bit necessari per codificare un tipo di pannello;

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

Soluzione

a)
- 4 tipi di materiale: $\lceil \log_2 4 \rceil = 2$ bit;
- 5 differenti spessori: $\lceil \log_2 5 \rceil = 3$ bit;
- 2 diverse lunghezze: $\lceil \log_2 2 \rceil = 1$ bit.

b) Ci sono $4 \times 5 \times 2 = 40$ tipi di pannello, quindi servono $\lceil \log_2 40 \rceil = 6$ bit.

c) I materassi sono costruiti sovrapponendo 3 pannelli, di uguale lunghezza, ma che si differenziano per le altre caratteristiche: non sono pertanto ammesse le ripetizioni e l'ordine ha importanza. Escludendo la caratteristica "lunghezza", ci sono $4 \times 5 = 20$ tipi di pannello da considerare per i materassi. Per ognuna delle 2 lunghezze, si potranno avere un numero di materassi diversi pari al numero di disposizioni semplici di 20 oggetti su 3 posti.

$$\begin{aligned} D(20,\,3) &= \tfrac{20!}{(20-3)!} = 20 \cdot 19 \cdot 18 = \\ &= 5 \cdot 19 \cdot 9 \cdot 2^3 = 855 \cdot 2^3 \end{aligned}$$

Si avranno quindi $2 \times D(20,\,3) = 855 \cdot 2^4$ materassi possibili.

Poiché la prima potenza di 2 che supera 855 è 2^{10}, per codificare i possibili materassi serviranno $\lceil \log_2 855 \cdot 2^4 \rceil = 10 + 4 = 14$ bit.

Esercizio 4

Dimostrare, tramite tavola di verità, ***se*** la seguente formula è una tautologia:

a) $(\neg r \wedge \neg p) \rightarrow ((p \vee \neg r) \wedge (\neg r \vee q))$

Soluzione

La tabella di verità è riportata in figura 1. Poiché tutte le interpretazioni la rendono vera, la proposizione data è una tautologia.

Esercizio 5

Formalizzare le seguenti proposizioni:

a) se Dario parla, Elisabetta e Federico tacciono;

b) Dario tace, Elisabetta o Federico parlano;

c) Elisabetta o Dario parlano;

d) Elisabetta tace solo se anche Dario fa lo stesso;

e) Federico parla se e solo se Dario tace;

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

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

Soluzione

Dati i seguenti simboli proposizionali:

d	Dario parla
$\neg d$	Dario tace
e	Elisabetta parla
$\neg e$	Elisabetta tace
f	Federico parla
$\neg f$	Federico tace

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

a) $d \rightarrow (\neg e \wedge \neg f)$

b) $\neg d \wedge (e \vee f)$

c) $e \vee d$

d) $\neg e \rightarrow \neg d$

e) $f \leftrightarrow \neg d$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	c	Ip2
(2)	$c \rightarrow (c \vee a)$	Intr. di disg. (1)
(3)	$c \vee a$	M. Ponens da (1) e (2)
(4)	$(c \vee a) \rightarrow \neg b$	Ip1
(5)	$\neg b$	M. Ponens da (3) e (4)

b)

(1)	$a \vee (b \wedge c)$	Ip1
(2)	$(a \vee b) \wedge (a \vee c)$	equiv. logica (1)
(3)	$a \vee c$	Elim. di cong. (2)
(4)	$\neg a \rightarrow c$	equiv. logica (2)
(5)	$\neg c$	Ip2
(6)	a	M. Tollens da (4) e (5)

c)

(1)	$\neg c$	Ip2
(2)	$\neg c \rightarrow (c \rightarrow b)$	Ex falso sequ. quod. (1)
(3)	$c \rightarrow b$	M. Ponens da (1) e (2)
(4)	$(c \rightarrow b) \rightarrow \neg a$	Ip1
(5)	$\neg a$	M. Ponens da (3) e (4)