Università degli Studi di Milano

Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006 docente: Stefano Ferrari

22.06.2006 — 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) $k = (53)_9$, $n = 10$

b) $k = (17)_{10}$, $n = 2$

c) $k = (8\mathrm{B})_{16}$, $n = 2$

d) $k = (162)_8$, $n = 2$

e) $k = (124)_5$, $n = 2$

f) $k = (11101101)_2$, $n = 16$

Soluzione

a) $(53)_9 = 5 \cdot 9^1 + 3 \cdot 9^0 = 5 \cdot 9 + 3 \cdot 1 = 45 + 3 = 48$

$(53)_9 = (48)_{10}$

b)

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

$(17)_{10} = (10001)_2$

c)

base 16	8	B
base 2	1000	1011

$(8\mathrm{B})_{16} = (10001011)_2$

d)

base 8	1	6	2
base 2	001	110	010

$(162)_8 = (1110010)_2$

e) $(124)_5 = 1 \cdot 5^2 + 2 \cdot 5^1 + 4 \cdot 5^0 = 1 \cdot 25 + 2 \cdot 5 + 4 \cdot 1 = 25 + 10 + 4 = 39$

quoziente	resto
39	
19	1
9	1
4	1
2	0
1	0
0	1

$(124)_5 = (100111)_2$

f)

base 2	1110	1101
base 16	E	D

$(11101101)_2 = (\mathrm{ED})_{16}$

Esercizio 2

Dati $a = 11$, $b = -6$ e $n = 4$, 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 4 bit 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. $2^n + a = 2^4 + 11 = 27$. Codificando 27 in binario e troncando tale codifica a 4 bit si ottiene: $s_a = 1011$.

   Poiché $a = 11 > 7$, si è verificato un overflow.

$2^n + b = 2^4 - 6 = 10$. Codificando 10 in binario e troncando tale codifica a 4 bit si ottiene: $s_b = 1010$.

Poiché $-8 \leq -6 \leq 7$, non si è verificato un overflow.

2. La somma binaria di 1011 e 1010, troncata a 4 bit è: $s_a + s_b = 0101$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 0101, si è verificato un overflow.

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

1010		sottraendo, s_b
0101	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
0110	+	$-s_b$
1011	=	s_a
10001		si devono considerare solo gli ultimi 4 bit
0001		$s_a - s_b$

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

Esercizio 3

Una azienda specializzata in trucchi e travestimenti esibisce nel proprio catalogo i seguenti materiali:

- baffi: a manubrio, a spazzolino, alla Dalì;
- parrucca: a scodella, a spazzola, alla mohicana, a coda di cavallo, calvo;
- barba: pizzetto, alla Garibaldi.

L'azienda commercializza i suoi prodotti in due kit:

- kit *transform*: una confezione composta da un paio di baffi, una parrucca e una barba;
- kit *superspy*: una confezione composta da due paia di baffi, tre parrucche e una barba.

Si calcoli:

a) il numero di bit necessari per codificare ciascun tipo di materiale (baffi, parrucca e barba);

b) il numero di bit necessari per codificare i possibili kit *transform*;

c) il numero di bit necessari per codificare i possibili kit *superspy*.

Soluzione

a)
- 3 tipi di baffi: $\lceil \log_2 3 \rceil = 2$ bit;
- 5 tipi di parrucca: $\lceil \log_2 5 \rceil = 3$ bit;
- 2 tipi di barba: $\lceil \log_2 2 \rceil = 1$ bit.

b) Per la regola moltiplicativa, ci sono $3 \times 5 \times 2 = 30$ possibili kit *transform*, quindi servono $\lceil \log_2 30 \rceil = 5$ bit.

c) Nei kit *superspy* sono presenti due paia di baffi (scelti su 3), tre parrucche (scelte fra 5) e una barba (scelta fra 2). Sembra ragionevole pensare che gli elementi di travestimento non possano essere ripetuti e che l'ordine non abbia importanza. Quindi, per ogni elemento il numero di configurazioni che possono essere trovate in un kit *superspy* è dato dalle combinazioni semplici:

- per i baffi:

$$C(3,\, 2) = \frac{3!}{(3-2)!(2)!} = \frac{3}{1!} = 3$$

- per la parrucca:

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

- per la barba:

$$C(2,\, 1) = \frac{2!}{(2-1)!(1)!} = 2$$

Per la regola moltiplicativa, si potranno avere un numero di differenti kit pari al prodotto delle configurazioni di ciascun elemento. Pertanto si potranno avere $3 \cdot 5 \cdot 2 \cdot 2 = 2^2 \cdot 15$ possibili kit. Poiché la prima potenza di 2 che supera 15 è 2^4, per codificare i possibili kit serviranno $\lceil \log_2(2^2 \cdot 15) \rceil = \lceil \log_2 2^2 + \log_2 15 \rceil = \lceil 2 + \log_2 15 \rceil = 2 + \lceil \log_2 15 \rceil = 2 + 4 = 6$ bit.

Esercizio 4

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

a) $(r \to \neg p) \wedge ((\neg q \vee r) \leftrightarrow r)$

Soluzione

La tabella di verità è riportata in figura 1. Poiché almeno una interpretazione rende falsa la proposizione data, essa non è una tautologia.

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

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

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non prenda il sole, nuoti, e viceversa):

a) Carlo non nuota, Bice e Anna sì;

b) Carlo prende il sole solo se anche Anna fa lo stesso;

c) se Carlo prende il sole, Bice e Anna nuotano;

d) Bice nuota se e solo se Carlo prende il sole;

e) Anna o Bice nuotano;

Soluzione

Dati i seguenti simboli proposizionali:

a	Anna prende il sole
$\neg a$	Anna nuota
b	Bice prende il sole
$\neg b$	Bice nuota
c	Carlo prende il sole
$\neg c$	Carlo nuota

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

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

b) $c \to a$

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

d) $\neg b \leftrightarrow c$

e) $\neg a \vee \neg b$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$a \vee (c \to \neg c)$	Ip2
(2)	$a \vee (\neg c \vee \neg c)$	Def. implicazione (1)
(3)	$a \vee \neg c$	Idempotenza (2)
(4)	$\neg a \to \neg c$	Def. implicazione (3)
(5)	$c \to a$	Contrapposizione (4)
(6)	$\neg(a \vee b)$	Ip1
(7)	$\neg a \wedge \neg b)$	Leggi di De Morgan (6)
(8)	$\neg a$	Elim. congiunzione (7)
(9)	$\neg a \to (a \to c)$	Ex falso sequitur quod.
(10)	$a \to c$	Modus Ponens (8) e (9)
(11)	$(a \to c) \wedge (c \to a)$	Congiun. di (10) e (5)
(12)	$a \leftrightarrow c$	Def. biimplicazione (11)

b)

(1)	$a \to b$	Ip1
(2)	$\neg b \to \neg a$	Contrapp. (1)
(3)	$a \vee (\neg a \wedge c)$	Ip2
(4)	$(a \vee \neg a) \wedge (a \vee c)$	Distrib. (3)
(5)	$a \vee c$	Elim. congiunzione (4)
(6)	$\neg a \to c$	Def. implicazione (5)
(7)	$\neg b \to c$	Sillog. ipotetico (2) e (6)

c)

(1)	$\neg a \vee \neg(a \vee c)$	Ip2
(2)	$\neg a \vee (\neg a \wedge \neg c)$	De Morgan (1)
(3)	$(\neg a \vee \neg a) \wedge (\neg a \vee \neg c)$	Distribut. (2)
(4)	$\neg a \vee \neg a$	Elim. cong. (3)
(5)	$\neg a$	Idempotenza (4)
(6)	$a \vee (b \to a)$	Ip1
(7)	$\neg a \to (b \to a)$	Def. implicazione (6)
(8)	$b \to a$	M. Ponens (5) e (7)
(9)	$\neg b$	M. Tollens (5) e (8)