Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006

docente: Stefano Ferrari

02.12.2005 — Soluzione del primo compitino — 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) $k = (641)_7$, $n = 10$

b) $k = (90)_{10}$, $n = 2$

c) $k = (\mathrm{C8})_{16}$, $n = 2$

d) $k = (712)_8$, $n = 2$

e) $k = (401)_5$, $n = 2$

f) $k = (1101001)_2$, $n = 16$

Soluzione

a) $(641)_7 = 6\cdot 7^2 + 4\cdot 7^1 + 1\cdot 7^0 = 6\cdot 49 + 4\cdot 7 + 1\cdot 1 = 294 + 28 + 1 = 323$

$(641)_7 = (323)_{10}$

b)

quoziente	resto
90	
45	0
22	1
11	0
5	1
2	1
1	0
0	1

$(90)_{10} = (1011010)_2$

c)

base 16	C	8
base 2	1100	1000

$(\mathrm{C8})_{16} = (11001000)_2$

d)

base 8	7	1	2
base 2	111	001	010

$(712)_8 = (111001010)_2$

e) $(401)_5 = 4\cdot 5^2 + 0\cdot 5^1 + 1\cdot 5^0 = 4\cdot 25 + 0\cdot 5 + 1\cdot 1 = 100 + 0 + 1 = 101$

quoziente	resto
101	
50	1
25	0
12	1
6	0
3	0
1	1
0	1

$(401)_5 = (1100101)_2$

f)

base 2	0110	1001
base 16	6	9

$(1101001)_2 = (69)_{16}$

Esercizio 2

Dati $a = -17$, $b = 3$ 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. $2^n + a = 2^5 - 17 = 15$. Codificando 15 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 01111$.

Poiché $a = -17 < -16$, si è verificato un overflow.

$2^n + b = 2^5 + 3 = 35$. Codificando 35 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 00011$.

Poiché $-16 \leq 3 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 01111 e 00011, troncata a 5 bit è: $s_a + s_b = 10010$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 10010, si è verificato un overflow.

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

00011		sottraendo, s_b
11100	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
11101	+	$-s_b$
01111	=	s_a
101100		si devono considerare solo gli ultimi 5 bit
01100		$s_a - s_b$

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

Esercizio 3

Una azienda produce statuine di pastori per presepio con le seguenti caratteristiche:

- sesso: maschio, femmina;
- colore capelli: giallo, marrone, nero, bianco, rosso;
- posizione pecorella: senza, sulle spalle, sotto il braccio destro, sotto il braccio sinistro, vicino alla gamba destra, vicino alla gamba sinistra, in braccio.

L'azienda vende le statuine in confezioni di 4, tali che nessuna abbia la pecorella nella stessa posizione. La confezione è fatta in modo che la prima statuina sia più visibile della seconda e così via.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (sesso, capelli, posizione pecorella);

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

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

Soluzione

a)
- 2 generi: $\lceil \log_2 2 \rceil = 1$ bit;
- 5 colori dei capelli: $\lceil \log_2 5 \rceil = 3$ bit;
- 7 posizioni pecorella: $\lceil \log_2 7 \rceil = 3$ bit.

b) Ci sono $2 \times 5 \times 7 = 70$ varianti di statuina, quindi servono $\lceil \log_2 70 \rceil = 7$ bit.

c) Le confezioni sono sono composte da 4 statuine, ognuna con la pecorella in una posizione diversa. Inoltre, l'ordine delle statuine nella scatola è importante perché ogni statuina è più visibile della statuina che segue. Quindi, non sono ammesse le ripetizioni e l'ordine va considerato.

Le statuine nella confezione non hanno vincoli sul sesso e sui colori dei capelli. Pertanto, non considerando le prime due caratteristiche, si potranno avere un numero di confezioni differenti pari al numero di disposizioni semplici di 7 oggetti (le differenti posizioni della pecorella) su 4 posti.

$$\begin{aligned} D(7,4) &= \frac{7!}{(7-4)!} = \frac{7!}{3!} = 7 \cdot 6 \cdot 5 \cdot 4 = \\ &= 2^3 \cdot 7 \cdot 3 \cdot 5 = 2^3 \cdot 105 \end{aligned}$$

Poiché considerando solo le prime due caratteristiche ogni statuina può assumere 10 (2 generi $\times$ 5 colori dei capelli) configurazioni diverse, si ha che il numero di confezioni differenti sarà pari a $10^4 \times 2^3 \cdot 105 = 2^7 \cdot 65625$. Poiché la prima potenza di 2 che supera 65625 è 2^{17}, per codificare le possibili nidiate serviranno $\lceil \log_2(2^7 \cdot 65625) \rceil = \lceil \log_2 2^7 + \log_2 65625 \rceil = \lceil 7 + \log_2 65625 \rceil = 7 + \lceil \log_2 65625 \rceil = 7 + 17 = 24$ bit.

Lo stesso risultato poteva essere ottenuto usando un ragionamento simile a quello che motiva la formula delle disposizioni semplici. Per la prima posizione della confezione possono essere scelte $2 \times 5 \times 7$ statuine (cioè, una qualsiasi delle statuine disponibili). Per la seconda posizione possono essere scelte tutte le statuine tranne quelle con la pecorella nella stessa posizione della prima statuina; le possibili statuine saranno quindi $2 \times 5 \times 6$. Analogamente, per la terza e la quarta posizione potranno essere scelte rispettivamente $2 \times 5 \times 5$ e $2 \times 5 \times 4$ statuine. In totale, si potranno quindi avere $2 \cdot 5 \cdot 7 \cdot 2 \cdot 5 \cdot 6 \cdot 2 \cdot 5 \cdot 5 \cdot 2 \cdot 5 \cdot 4 = 10^4 \cdot 7 \cdot 6 \cdot 5 \cdot 4$ confezioni differenti.

Esercizio 4

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

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

Soluzione

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

Esercizio 5

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

a) Antonio non nuota, Bice o Carlo sì;

b) Carlo e Bice prendono il sole;

c) se Bice nuota, Antonio e Carlo prendono il sole;

d) Antonio prende il sole solo se anche Bice fa lo stesso;

e) Bice nuota se e solo se Antonio prende il sole;

Soluzione

Dati i seguenti simboli proposizionali:

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

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

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

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

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

d) $\neg a \rightarrow \neg b$

e) $b \leftrightarrow \neg a$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

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

b)

(1)	$\neg b \rightarrow (b \wedge a)$	Ip2
(2)	$(\neg b \rightarrow b) \wedge (\neg b \rightarrow a)$	Distr. delle cons. (1)
(3)	$\neg b \rightarrow b$	Elim. di cong. (2)
(4)	$b \vee b$	Def. implicazione (3)
(5)	b	Idempotenza (4)
(6)	$\neg(c \wedge b)$	Ip1
(7)	$\neg c \vee \neg b$	Leggi di De Morgan (6)
(8)	$c \rightarrow \neg b$	Def. implicazione (7)
(9)	$\neg c$	M. Tollens da (5) e (8)

c)

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

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

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