Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006

docente: Stefano Ferrari

03.02.2006 — 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) $k = (630)_7$, $n = 10$

b) $k = (92)_{10}$, $n = 2$

c) $k = (\mathrm{A3})_{16}$, $n = 2$

d) $k = (216)_8$, $n = 2$

e) $k = (140)_5$, $n = 2$

f) $k = (10101011)_2$, $n = 16$

Soluzione

a) $(630)_7 = 6 \cdot 7^2 + 3 \cdot 7^1 + 0 \cdot 7^0 = 6 \cdot 49 + 3 \cdot 7 + 0 \cdot 1 = 294 + 21 + 0 = 315$

$(630)_7 = (315)_{10}$

b)

quoziente	resto
92	
46	0
23	0
11	1
5	1
2	1
1	0
0	1

$(92)_{10} = (1011100)_2$

c)

base 16	A	3
base 2	1010	0011

$(\mathrm{A3})_{16} = (10100011)_2$

d)

base 8	2	1	6
base 2	010	001	110

$(216)_8 = (10001110)_2$

e) $(140)_5 = 1 \cdot 5^2 + 4 \cdot 5^1 + 0 \cdot 5^0 = 1 \cdot 25 + 4 \cdot 5 + 0 \cdot 1 = 25 + 20 + 0 = 45$

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

$(140)_5 = (101101)_2$

f)

base 2	1010	1011
base 16	A	B

$(10101011)_2 = (\mathrm{AB})_{16}$

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 dolciaria produce torroncini con le seguenti caratteristiche:

- copertura: tradizionale, cioccolato, crema al limone, caramello;
- ingredienti: nocciole, pistacchi, mandorle, anacardi, cocco;
- dimensione: mini, standard, maxi.

I torroncini vengono venduti in una sacchetto in cui sono contenuti 4 torroncini della stessa dimensione.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (copertura, ingredienti, dimensione);

b) il numero di bit necessari per codificare un torroncino;

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

Soluzione

a)
- 4 tipi di copertura: $\lceil \log_2 4 \rceil = 2$ bit;
- 5 ingredienti: $\lceil \log_2 5 \rceil = 3$ bit;
- 3 dimensioni: $\lceil \log_2 3 \rceil = 2$ bit.

b) Ci sono $4 \times 5 \times 3 = 60$ varianti di torroncino, quindi servono $\lceil \log_2 60 \rceil = 6$ bit.

c) Le confezioni sono sono composte da 4 torroncini della stessa dimensione. Sembra ragionevole ammettere le ripetizioni, senza considerare l'ordine dei torroncini nel sacchetto. Quindi, per ogni dimensione, si potranno avere un numero di sacchetti pari al numero di combinazioni con ripetizione di 20 oggetti (4 tipi di copertura $\times$ 5 ingredienti) su 4 posti.

$$\begin{aligned} C_r(20, 4) &= C(20 + 4 - 1, 4) = C(23, 4) = \\ &= \binom{23}{4} = \frac{23!}{19! \cdot 4!} = \\ &= \frac{23 \cdot 22 \cdot 21 \cdot 20}{4 \cdot 3 \cdot 2} = \\ &= 23 \cdot 11 \cdot 7 \cdot 5 = 8855 \end{aligned}$$

Poiché si hanno 3 differenti dimensioni, in totale si avranno quindi $3 \cdot 8855 = 26565$ possibili confezioni. Poiché la prima potenza di 2 che supera 26565 è 2^{15}, per codificare le possibili confezioni serviranno $\lceil \log_2 26565 \rceil = 15$ bit.

Esercizio 4

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

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

Soluzione

La tabella di verità è riportata in figura 1. Poiché alcune interpretazioni rendono falsa la proposizione data, essa non è una tautologia.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non cucina, lavi, e viceversa):

a) se Antonio cucina, Bice e Carlo lavano;

b) Carlo non lava, Bice e Antonio sì;

c) Bice lava se e solo se Antonio cucina;

d) Carlo e Bice lavano;

e) Antonio cucina solo se anche Bice fa lo stesso;

Soluzione

Dati i seguenti simboli proposizionali:

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

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

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

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

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

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

c) $\neg b \leftrightarrow a$

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

e) $a \rightarrow b$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a) Una possible soluzione è riportata in figura 2.

b) Una possible soluzione è riportata in figura 3.

c)

(1)	$a \vee c$	Ip2
(2)	$\neg a \rightarrow c$	Def. implicazione (1)
(3)	$\neg(b \rightarrow c)$	Ip1
(4)	$\neg(\neg b \vee c)$	Def. Implicazione (3)
(5)	$b \wedge \neg c$	Leggi di De Morgan (4)
(6)	$\neg c$	Elim. congiunzione (5)
(7)	a	Modus Tollens (2) e (6)

(1)	$(c \to b) \leftrightarrow a$	Ip1
(2)	$((c \to b) \to a) \land (a \to (c \to b))$	Def. biimplicazione (1)
(3)	$(c \to b) \to a$	Elim. congiunzione (2)
(4)	$\neg a \to \neg(c \to b)$	Contrapposizione (3)
(5)	$\neg a \to \neg(\neg c \lor b)$	Def. implicazione (4)
(6)	$\neg a \to (\neg\neg c \land \neg b)$	Leggi di De Morgan (5)
(7)	$(\neg a \to \neg\neg c) \land (\neg a \to \neg b)$	Distrib. dell'implicazione (6)
(8)	$\neg a \to \neg b$	Elim. congiunzione (7)
(9)	$\neg a$	Ip2
(10)	$\neg b$	Modus Ponens da (8) e (9)

Figura 2: Una possibile soluzione dell'esercizio 6a.

(1)	$(b \land a) \lor c$	Ip1
(2)	$\neg(b \land a) \to c$	Def. implicazione (1)
(3)	$a \to (c \lor \neg b)$	Ip2
(4)	$\neg a \lor (c \lor \neg b)$	Def. implicazione (3)
(5)	$\neg a \lor (\neg b \lor c)$	Commutatività (4)
(6)	$(\neg a \lor \neg b) \lor c$	Associatività (5)
(7)	$\neg(\neg a \lor \neg b) \to c$	Def. implicazione (6)
(8)	$(a \land b) \to c$	Leggi di De Morgan (7)
(9)	$(b \land a) \to c$	Commutatività (8)
(10)	$(\neg(b \land a) \to c) \land ((b \land a) \to c)$	Congiunzione di (2) e (9)
(11)	$((\neg(b \land a) \to c) \land ((b \land a) \to c)) \to c$	Dim. per casi
(12)	c	Modus Ponens da (10) e (11)

Figura 3: Una possibile soluzione dell'esercizio 6b.