Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006

docente: Stefano Ferrari

08.02.2006 — 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) $k = (531)_7$, $n = 10$

b) $k = (29)_{10}$, $n = 2$

c) $k = (2C)_{16}$, $n = 2$

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

e) $k = (312)_5$, $n = 2$

f) $k = (10111011)_2$, $n = 16$

Soluzione

a) $(531)_7 = 5 \cdot 7^2 + 3 \cdot 7^1 + 1 \cdot 7^0 = 5 \cdot 49 + 3 \cdot 7 + 1 \cdot 1 = 245 + 21 + 1 = 267$

$(531)_7 = (267)_{10}$

b)

quoziente	resto
29	
14	1
7	0
3	1
1	1
0	1

$(29)_{10} = (11101)_2$

c)

base 16	2	C
base 2	0010	1100

$(2C)_{16} = (101100)_2$

d)

base 8	1	7	0
base 2	001	111	000

$(170)_8 = (1111000)_2$

e) $(312)_5 = 3 \cdot 5^2 + 1 \cdot 5^1 + 2 \cdot 5^0 = 3 \cdot 25 + 1 \cdot 5 + 2 \cdot 1 = 75 + 5 + 2 = 82$

quoziente	resto
82	
41	0
20	1
10	0
5	0
2	1
1	0
0	1

$(312)_5 = (1010010)_2$

f)

base 2	1011	1011
base 16	B	B

$(10111011)_2 = (BB)_{16}$

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. $2^n + a = 2^5 + 17 = 49$. Codificando 49 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 10001$.

Poiché $a = 17 > 15$, si è verificato un overflow.

$2^n + b = 2^5 - 3 = 29$. Codificando 29 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 11101$.

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

2. La somma binaria di 10001 e 11101, troncata a 5 bit è: $s_a + s_b = 01110$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 01110, si è verificato un overflow.

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

11101		sottraendo, s_b
00010	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
00011	+	$-s_b$
10001	=	s_a
10100		$s_a - s_b$

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

Esercizio 3

Una azienda produce cartoncini con le seguenti caratteristiche:

- colore: bianco, rosso, giallo, verde;
- superficie: liscia, ruvida;
- dimensione: A4, A5, A6.

I cartoncini vengono venduti confezionati in una busta che ne contiene 5, tutti della stessa dimensione, ma con almeno una delle altre caratteristiche diversa.

Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (colore, superficie, dimensione);

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

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

Soluzione

a)
- 4 colori: $\lceil \log_2 4 \rceil = 2$ bit;
- 2 tipi di superficie: $\lceil \log_2 2 \rceil = 1$ bit;
- 3 dimensioni: $\lceil \log_2 3 \rceil = 2$ bit.

b) Ci sono $4 \times 2 \times 3 = 24$ varianti di cartoncino, quindi servono $\lceil \log_2 24 \rceil = 5$ bit.

c) Le confezioni sono sono composte da 5 cartoncini della stessa dimensione. Le ripetizioni non sono ammesse in quanto tutte le altre caratteristiche (superficie e colore) devono essere diverse. Non vi sono specifiche esplicite riguardo all'importanza dell'ordine dei cartoncini nella stessa confezione, ma il tipo di materiale e di confezione fa pensare che l'ordine sia da tenere in considerazione (una volta imbustati, i cartoncini non possono mischiarsi). Quindi, per ogni dimensione, si potranno avere un numero di buste pari al numero di disposizioni semplici di 8 oggetti (4 colori $\times$ 2 tipi di superficie) su 5 posti.

$$\begin{aligned} D(8,5) &= \frac{8!}{(8-5)!} = \\ &= 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 2^6 \cdot 7 \cdot 5 \cdot 3 = \\ &= 2^6 \cdot 105 \end{aligned}$$

Poiché si hanno 3 differenti dimensioni, in totale si avranno quindi $3 \cdot 2^6 \cdot 105 = 2^6 \cdot 315$ possibili confezioni. Poiché la prima potenza di 2 che supera 315 è 2^9, per codificare le possibili confezioni serviranno $\lceil \log_2(2^6 \cdot 315) \rceil = \lceil \log_2 2^6 + \log_2 315 \rceil = \lceil 6 + \log_2 315 \rceil = 6 + \lceil \log_2 315 \rceil = 6 + 9 = 15$ bit.

Se invece si fosse considerato l'ordine come non importante, per ogni dimensione, si sarebbero dovute considerare le combinazioni semplici di 8 oggetti su 5 posti:

$$\begin{aligned} C(8,5) &= \frac{8!}{(8-5)!5!} = \\ &= \frac{8 \cdot 7 \cdot 6}{3 \cdot 2} = 2^3 \cdot 7 \end{aligned}$$

Ciò avrebbe portato quindi ad un numero di bit richiesti paria a $\lceil \log_2(2^3 \cdot 21) \rceil = \lceil 3 + \log_2 21 \rceil = 3 + \lceil \log_2 21 \rceil = 3 + 5 = 8$ bit.

Esercizio 4

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

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

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 sporca, pulisca, e viceversa):

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

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

a) se Antonio sporca, Bice e Carlo puliscono;

b) Bice pulisce se e solo se Antonio sporca;

c) Carlo non sporca, Bice e Antonio sì;

d) Carlo o Bice puliscono;

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

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio sporca
$\neg a$	Antonio pulisce
b	Bice sporca
$\neg b$	Bice pulisce
c	Carlo sporca
$\neg c$	Carlo pulisce

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

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

b) $\neg b \leftrightarrow a$

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

d) $\neg c \vee \neg b$

e) $\neg a \rightarrow \neg b$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a) Una possible soluzione è riportata in figura 2.

b)

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

c) Una possible soluzione è riportata in figura 3.

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

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

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

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