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 D

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) $k = (513)_7$, $n = 10$

b) $k = (75)_{10}$, $n = 2$

c) $k = (7\mathrm{A})_{16}$, $n = 2$

d) $k = (641)_8$, $n = 2$

e) $k = (341)_5$, $n = 2$

f) $k = (1111001)_2$, $n = 16$

Soluzione

a) $(513)_7 = 5\cdot7^2+1\cdot7^1+3\cdot7^0 = 5\cdot49+1\cdot7+3\cdot1 = 245+7+3 = 255$

$(513)_7 = (255)_{10}$

b)

quoziente	resto
75	
37	1
18	1
9	0
4	1
2	0
1	0
0	1

$(75)_{10} = (1001011)_2$

c)

base 16	7	A
base 2	0111	1010

$(7\mathrm{A})_{16} = (1111010)_2$

d)

base 8	6	4	1
base 2	110	100	001

$(641)_8 = (110100001)_2$

e) $(341)_5 = 3\cdot5^2+4\cdot5^1+1\cdot5^0 = 3\cdot25+4\cdot5+1\cdot1 = 75+20+1 = 96$

quoziente	resto
96	
48	0
24	0
12	0
6	0
3	0
1	1
0	1

$(341)_5 = (1100000)_2$

f)

base 2	0111	1001
base 16	7	9

$(1111001)_2 = (79)_{16}$

Esercizio 2

Dati $a = 15$, $b = -19$ 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. $2^n+a = 2^5+15 = 47$. Codificando 47 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 01111$.

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

$2^n + b = 2^5 - 19 = 13$. Codificando 13 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 01101$.

Poiché $b = -19 < -16$, si è verificato un overflow.

2. La somma binaria di 01111 e 01101, troncata a 5 bit è: $s_a + s_b = 11100$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 11100, si è verificato un overflow.

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

01101		sottraendo, s_b
10010	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
10011	+	$-s_b$
01111	=	s_a
100010		si devono considerare solo gli ultimi 5 bit
00010		$s_a - s_b$

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

Esercizio 3

Una azienda produce spolette di filo per cucito, con le seguenti caratteristiche:

- lunghezza: 20 m, 50 m, 110 m;
- colore: bianco, grigio, nero, rosso, blu, giallo;
- diametro: sottile, normale.

L'azienda commercializza le spolette in sacchetti da 12, tutte dello stesso diametro, ma che differiscono per le altre caratteristiche.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (lunghezza, colore, diametro);

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

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

Soluzione

a)
- 3 lunghezze: $\lceil \log_2 3 \rceil = 2$ bit;
- 6 colori: $\lceil \log_2 6 \rceil = 3$ bit;
- 2 diametri: $\lceil \log_2 2 \rceil = 1$ bit.

b) Ci sono $3 \times 6 \times 2 = 36$ varianti di spoletta, quindi servono $\lceil \log_2 36 \rceil = 6$ bit.

c) I sacchetti sono sono composti da 12 spolette dello stesso diametro. Non sono quindi ammesse le ripetizioni e non bisogna considerare l'ordine delle spolette nel sacchetto. Quindi, per ogni diametro, si potranno avere un numero di sacchetti pari al numero di combinazioni semplici di 18 oggetti (3 lunghezze $\times$ 6 colori) su 12 posti.

$$\begin{aligned} C(18,\, 12) &= \binom{18}{12} = \frac{18!}{12! \cdot 6!} = \\ &= \frac{18 \cdot 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} = \\ &= 2^2 \cdot 3 \cdot 7 \cdot 13 \cdot 17 = 2^2 \cdot 4641 \end{aligned}$$

Poiché si hanno 2 diametri, in totale si avranno quindi $2 \cdot 2^2 \cdot 4621 = 2^3 \cdot 4641$ possibili sacchetti. Poiché la prima potenza di 2 che supera 4641 è 2^{13}, per codificare le possibili nidiate serviranno $\lceil \log_2(2^3 \cdot 4641) \rceil = \lceil \log_2 2^3 + \log_2 4641 \rceil = \lceil 3 + \log_2 4641 \rceil = 3 + \lceil \log_2 4641 \rceil = 3 + 13 = 16$ bit.

Esercizio 4

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

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

Soluzione

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

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non gioca, studi, e viceversa):

a) se Alberto studia, Barbara o Carlo giocano;

b) Carlo non studia, Barbara o Alberto sì;

c) Carlo e Barbara giocano;

d) Alberto studia solo se anche Barbara fa lo stesso;

e) Barbara gioca se e solo se Alberto studia;

Soluzione

Dati i seguenti simboli proposizionali:

a	Alberto gioca
$\neg a$	Alberto studia
b	Barbara gioca
$\neg b$	Barbara studia
c	Carlo gioca
$\neg c$	Carlo studia

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

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

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

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

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

c) $c \wedge b$

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

e) $b \leftrightarrow \neg a$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

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

b)

(1)	$\neg b \rightarrow (b \wedge c)$	Ip2
(2)	$(\neg b \rightarrow b) \wedge (\neg b \rightarrow c)$	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)	$\neg(a \wedge b)$	Ip1
(7)	$\neg a \vee \neg b$	Leggi di De Morgan (6)
(8)	$\neg b \vee \neg a$	Commutatività (7)
(9)	$b \rightarrow \neg a$	Def. implicazione (8)
(10)	$\neg a$	M. Ponens da (5) e (9)

c)

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