Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

Università degli Studi di Milano

anno accademico 2006–2007 docente: Stefano Ferrari

01.12.2006 — 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) $k = (521)_7$, $n = 10$

b) $k = (73)_{10}$, $n = 2$

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

d) $k = (357)_8$, $n = 2$

e) $k = (301)_5$, $n = 2$

f) $k = (1011010)_2$, $n = 16$

Soluzione

a) $(521)_7 = 5{\cdot}7^2 + 2{\cdot}7^1 + 1{\cdot}7^0 = 5{\cdot}49 + 2{\cdot}7 + 1{\cdot}1 = 245 + 14 + 1 = 260$

$(521)_7 = (260)_{10}$

b)

quoziente	resto
73	
36	1
18	0
9	0
4	1
2	0
1	0
0	1

$(73)_{10} = (1001001)_2$

c)

base 16	8	C
base 2	1000	1100

$(8\mathrm{C})_{16} = (10001100)_2$

d)

base 8	3	5	7
base 2	011	101	111

$(357)_8 = (11101111)_2$

e) $(301)_5 = 3{\cdot}5^2 + 0{\cdot}5^1 + 1{\cdot}5^0 = 3{\cdot}25 + 0{\cdot}5 + 1{\cdot}1 = 75 + 0 + 1 = 76$

quoziente	resto
76	
38	0
19	0
9	1
4	1
2	0
1	0
0	1

$(301)_5 = (1001100)_2$

f)

base 2	0101	1010
base 16	5	A

$(1011010)_2 = (5\mathrm{A})_{16}$

Esercizio 2

Dati $a = -8$, $b = 19$ 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. $2^n + a = 2^5 - 8 = 24$. Codificando 24 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 11000$.

Poiché $-16 \leq -8 \leq 15$, non si è verificato un overflow.

$2^n + b = 2^5 + 19 = 51$. Codificando 51 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 10011$.

Poiché $b = 19 > 15$, si è verificato un overflow.

2. La somma binaria di 11000 e 10011, troncata a 5 bit è: $s_a + s_b = 01011$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 01011, si è verificato un overflow.

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

10011		sottraendo, s_b
01100	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
01101	+	$-s_b$
11000	=	s_a
100101		si devono considerare solo gli ultimi 5 bit
00101		$s_a - s_b$

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

Esercizio 3

Una azienda di giocattoli produce un *peluche* con le seguenti caratteristiche:

- forma: cavallo, orso, cane;
- taglia: *mini*, *small*, *medium*, *large*;
- colore: bianco, nero, maculato, verde, rosa.

Inoltre, l'azienda propone un'offerta speciale per chi acquista 5 peluche diversi.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (forma, taglia e colore);

b) il numero di bit necessari per codificare un modello di peluche;

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

Soluzione

a)
- 3 forme: $\lceil \log_2 3 \rceil = 2$ bit;
- 4 taglie: $\lceil \log_2 4 \rceil = 2$ bit;
- 5 colori: $\lceil \log_2 5 \rceil = 3$ bit.

b) Per la regola moltiplicativa, ci sono $3 \times 4 \times 5 = 60$ possibili *peluche*, quindi servono $\lceil \log_2 60 \rceil = 6$ bit.

c) Poiché i *peluche* dell'offerta speciale devono essere diversi, non sono ammesse le ripetizioni. L'assenza di ulteriori specifiche riguardanti l'offerta speciale fa pensare che l'ordine non sia importante.

   Pertanto il numero di offerte speciali possibili è dato dalle combianzioni semplici di 60 elementi (i possibili *peluche*) su 5 posti (il numero di *peluche* dell'offerta speciale):

$$C(60,\,5) = \frac{60!}{55!\,5!} = \frac{60 \cdot 59 \cdot 58 \cdot 57 \cdot 56}{5 \cdot 4 \cdot 3 \cdot 2} =$$
$$59 \cdot 29 \cdot 57 \cdot 56 = 2^3 \cdot 59 \cdot 29 \cdot 57 \cdot 7 =$$
$$= 2^3 \cdot 682689$$

   Poiché la prima potenza di 2 che supera 682689 è 2^{20}, per codificare le possibili maglie serviranno $\lceil \log_2(2^3 \cdot 682689) \rceil = \lceil \log_2 2^3 + \log_2 682689 \rceil = \lceil 3 + \log_2 682689 \rceil = 3 + \lceil \log_2 682689 \rceil = 3 + 20 = 23$ bit.

Esercizio 4

Sia data la seguente formula, F:

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

a) Costruire la tavola di verità di F.

b) F è una tautologia? Motivare la risposta.

Soluzione

a) La tabella di verità di F è riportata in figura 1.

b) Poiché almeno una interpretazione rende falsa la proposizione F, essa non è una tautologia.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non corre, salta, e viceversa):

a) Carlo non salta, Bice o Antonio sì;

b) se Antonio corre, Bice e Carlo saltano;

c) Carlo oppure Bice corrono;

d) Antonio salta solo se anche Bice fa lo stesso;

e) Bice salta se e solo se Antonio e Carlo corrono.

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio salta
$\neg a$	Antonio corre
b	Bice salta
$\neg b$	Bice corre
c	Carlo salta
$\neg c$	Carlo corre

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

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

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

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

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

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

d) $a \rightarrow b$

e) $b \leftrightarrow (\neg a \wedge \neg c)$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$\neg(b \vee a)$	Ip1
(2)	$\neg b \wedge \neg a$	Legge di De Morgan (1)
(3)	$\neg b$	Elim. congiunzione (2)
(4)	$b \rightarrow c$	Ex falso (3)
(5)	$b \vee (c \rightarrow \neg c)$	Ip2
(6)	$b \vee (\neg c \vee \neg c)$	Def. implicazione (5)
(7)	$b \vee \neg c$	Idempotenza (6)
(8)	$\neg b \rightarrow \neg c$	Def. implicazione (7)
(9)	$c \rightarrow b$	Contrapp. (8)
(10)	$b \leftrightarrow c$	Def. biimplicazione (4) e (9)

b)

(1)	$c \leftrightarrow b$	Ip1
(2)	$(c \rightarrow b) \wedge (b \rightarrow c)$	Def. biimplicazione (1)
(3)	$b \rightarrow c$	Elim. congiunzione (2)
(4)	$\neg c \rightarrow \neg b$	Contrapp. (3)
(5)	$\neg b \vee (\neg c \wedge a)$	Ip2
(6)	$(\neg b \vee \neg c) \wedge (\neg b \vee a)$	Distrib. (5)
(7)	$\neg b \vee \neg c$	Elim. congiunzione (6)
(8)	$\neg c \vee \neg b$	Associatività (7)
(9)	$c \rightarrow \neg b$	Def. implicazione (8)
(10)	$\neg b$	Dim. per casi (4) e (9)

c)

(1)	$\neg b \vee (a \wedge c)$	Ip2
(2)	$(\neg b \vee a) \wedge (\neg b \vee c)$	Distributività (1)
(3)	$\neg b \vee a$	Elim. congiunzione (2)
(4)	$b \rightarrow a$	Def. implicazione (3)
(5)	$\neg a$	Ip1
(6)	$\neg b$	Modus Tollens (4) e (5)