Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006

docente: Stefano Ferrari

09.11.2005 — 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) $k = (605)_7$, $n = 10$

b) $k = (42)_{10}$, $n = 2$

c) $k = (1A)_{16}$, $n = 2$

d) $k = (213)_8$, $n = 2$

e) $k = (103)_5$, $n = 2$

f) $k = (1100011)_2$, $n = 16$

Soluzione

a) $(605)_7 = 6 \cdot 7^2 + 0 \cdot 7^1 + 5 \cdot 7^0 = 6 \cdot 49 + 0 \cdot 7 + 5 \cdot 1 = 294 + 0 + 5 = 299$

$(605)_7 = (299)_{10}$

b)

quoziente	resto
42	
21	0
10	1
5	0
2	1
1	0
0	1

$(42)_{10} = (101010)_2$

c)

base 16	1	A
base 2	0001	1010

$(1A)_{16} = (11010)_2$

d)

base 8	2	1	3
base 2	010	001	011

$(213)_8 = (10001011)_2$

e) $(103)_5 = 1 \cdot 5^2 + 0 \cdot 5^1 + 3 \cdot 5^0 = 1 \cdot 25 + 0 \cdot 5 + 3 \cdot 1 = 25 + 0 + 3 = 28$

quoziente	resto
28	
14	0
7	0
3	1
1	1
0	1

$(103)_5 = (11100)_2$

f)

base 2	0110	0011
base 16	6	3

$(1100011)_2 = (63)_{16}$

Esercizio 2

Dati $a = -18$, $b = 2$ 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. $2^n + a = 2^5 - 18 = 14$. Codificando 14 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 01110$.

Poiché $a = -18 < -16$, si è verificato un overflow.

$2^n + b = 2^5 + 2 = 34$. Codificando 34 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 00010$.

Poiché $-16 \leq 2 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 01110 e 00010, troncata a 5 bit è: $s_a + s_b = 10000$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 10000, si è verificato un overflow.

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

00010		sottraendo, s_b
11101	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
11110	+	$-s_b$
01110	=	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

Un laboratorio di manipolazione genetica interviene su cellule di topo per indurre le seguenti caratteristiche:

- sesso: maschio, femmina;
- pelo: bianco, grigio, nero, marrone, glabro;
- taglia: mini, standard, maxi.

Ogni nidiata è composta da 4 topi, tutti della stessa taglia.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (sesso, pelo, taglia);

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

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

Soluzione

a)
- 2 generi: $\lceil \log_2 2 \rceil = 1$ bit;
- 5 tipi di pelo: $\lceil \log_2 5 \rceil = 3$ bit;
- 3 taglie: $\lceil \log_2 3 \rceil = 2$ bit.

b) Ci sono $2 \times 5 \times 3 = 30$ varianti di topo, quindi servono $\lceil \log_2 30 \rceil = 5$ bit.

c) Le nidiate sono sono composte da 4 topi della stessa taglia. Sembra ragionevole ammettere le ripetizioni, ma non considerare l'ordine dei topi nella nidiata. Quindi, per ogni taglia, si potranno avere un numero di nidiate pari al numero di combinazioni con ripetizione di 10 oggetti (2 generi $\times$ 5 tipi di pelo) su 4 posti.

$$\begin{aligned} C_r(10,\, 4) &= C(10+4-1,\, 4) = C(13,\, 4) = \\ &= \binom{13}{4} = \frac{13!}{9! \cdot 4!} = \\ &= \frac{13 \cdot 12 \cdot 11 \cdot 10}{4 \cdot 3 \cdot 2} = \\ &= 13 \cdot 11 \cdot 5 = 715 \end{aligned}$$

Poiché si hanno 3 taglie, in totale si avranno quindi $3 \cdot 715 = 2145$ possibili nidiate. Poiché la prima potenza di 2 che supera 2145 è 2^{12}, per codificare le possibili nidiate serviranno $\lceil \log_2 2145 \rceil = 12$ bit.

Esercizio 4

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

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

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 legga, dorma, e viceversa):

a) se Antonio legge, Bice o Carlo dormono;

b) Carlo non dorme, Bice e Antonio sì;

c) Carlo e Bice leggono;

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

e) Bice legge se e solo se Antonio dorme;

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio legge
$\neg a$	Antonio dorme
b	Bice legge
$\neg b$	Bice dorme
c	Carlo legge
$\neg c$	Carlo dorme

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

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

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

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

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

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

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

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

Soluzione

a)

(1)	$(\neg a \wedge c) \vee \neg b$	Ip2
(2)	$\neg(\neg a \wedge c) \rightarrow \neg b$	Def. implicazione (1)
(3)	$(a \vee \neg c) \rightarrow \neg b$	Leggi di De Morgan (2)
(4)	a	Ip1
(5)	$a \vee \neg c$	Introd. di disg. (4)
(6)	$\neg b$	M. Ponens da (3) e (5)

b)

(1)	$\neg(\neg a \wedge (b \vee c))$	Ip2
(2)	$\neg\neg a \vee \neg(b \vee c)$	Leggi di De Morgan (1)
(3)	$a \vee \neg(b \vee c)$	Doppia negazione (2)
(4)	$\neg(b \vee c) \vee a$	Commutatività (3)
(5)	$(b \vee c) \rightarrow a$	Def. implicazione (4)
(6)	$(c \vee b) \rightarrow a$	Commutatività (5)
(7)	$\neg a \rightarrow (c \vee b)$	Ip1
(8)	$\neg(c \vee b) \rightarrow a$	Contrapp. di (7)
(9)	$((c \vee b) \rightarrow a) \wedge (\neg(c \vee b) \rightarrow a)$	Cong. di (6) e (8)
(10)	$(((c \vee b) \rightarrow a) \wedge (\neg(c \vee b) \rightarrow a)) \rightarrow a$	Dim. per casi
(11)	a	M. Ponens da (9) e (10)

c)

(1)	$a \vee (b \wedge c)$	Ip1
(2)	$(b \wedge c) \vee a$	Commutatività (1)
(3)	$\neg(b \wedge c) \rightarrow a$	Def. Implicazione (2)
(4)	$c \rightarrow (a \vee \neg b)$	Ip2
(5)	$c \rightarrow (\neg b \vee a)$	Commutatività (4)
(6)	$c \rightarrow (b \rightarrow a)$	Def. implicazione (5)
(7)	$(c \wedge b) \rightarrow a$	Esp. delle premesse (6)
(8)	$(b \wedge c) \rightarrow a$	Commutatività (7)
(9)	a	Dim. per casi da (3) e (8)