Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2004–2005

docente: Stefano Ferrari

09.11.2005 — 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) $k = (362)_7$, $n = 10$

b) $k = (70)_{10}$, $n = 2$

c) $k = (\mathrm{D7})_{16}$, $n = 2$

d) $k = (126)_8$, $n = 2$

e) $k = (1202)_3$, $n = 2$

f) $k = (1001100)_2$, $n = 16$

Soluzione

a) $(362)_7 = 3 \cdot 7^2 + 6 \cdot 7^1 + 2 \cdot 7^0 = 3 \cdot 49 + 6 \cdot 7 + 2 \cdot 1 = 147 + 42 + 2 = 191$

$(362)_7 = (191)_{10}$

b)

quoziente	resto
70	
35	0
17	1
8	1
4	0
2	0
1	0
0	1

$(70)_{10} = (1000110)_2$

c)

base 16	D	7
base 2	1101	0111

$(\mathrm{D7})_{16} = (11010111)_2$

d)

base 8	1	2	6
base 2	001	010	110

$(126)_8 = (1010110)_2$

e) $(1202)_3 = 1 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3^1 + 2 \cdot 3^0 = 1 \cdot 27 + 2 \cdot 9 + 0 \cdot 3 + 2 \cdot 1 = 27 + 18 + 0 + 2 = 47$

quoziente	resto
47	
23	1
11	1
5	1
2	1
1	0
0	1

$(1202)_3 = (101111)_2$

f)

base 2	0100	1100
base 16	4	C

$(1001100)_2 = (\mathrm{4C})_{16}$

Esercizio 2

Dati $a = 22$, $b = 3$ 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. $2^n + a = 2^5 + 22 = 54$. Codificando 54 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 10110$.

Poiché $a = 22 > 15$, 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 10110 e 00011, troncata a 5 bit è: $s_a + s_b = 11001$.

   Poiché s_a e s_b hanno il primo bit diverso, non 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	+	$-s_b$
10110	=	s_a
110011		si devono considerare solo gli ultimi 5 bit
10011		$s_a - s_b$

   Poiché s_a e s_b hanno il primo bit diverso, e il primo bit della loro differenza, 10011, è uguale al primo bit di s_a, non si è verificato un overflow.

Esercizio 3

Un programma di grafica consente di formare loghi utilizzando figure con le seguenti caratteristiche:

- colore: nero, rosso, giallo, verde, blu, azzurro;
- forma: quadrato, triangolo, cerchio, esagono;
- dimensione: piccolo, medio, grande.

Ogni logo viene formato allineando 4 figure.
Si calcoli:

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

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

c) il numero di bit necessari per codificare i possibili loghi.

Soluzione

a)
- 6 colori: $\lceil \log_2 6 \rceil = 3$ bit;
- 4 forme: $\lceil \log_2 4 \rceil = 2$ bit;
- 3 dimensioni: $\lceil \log_2 3 \rceil = 2$ bit.

b) Ci sono $6 \times 4 \times 3 = 72$ differenti figure, quindi servono $\lceil \log_2 72 \rceil = 7$ bit.

c) I loghi vengono composti allineando 4 figure. Sembra ragionevole ammettere le ripetizioni, e considerare importante l'ordine con cui le figure appaiono nel logo. Quindi, si potranno avere un numero di loghi pari al numero di disposizioni con ripetizione di 72 oggetti (6 colori $\times$ 4 forme $\times$ 3 dimensioni) su 4 posti.

$$\begin{aligned} D_r(72, 4) &= 72^4 = (2^3 \cdot 3^2)^4 \\ &= 2^{12} \cdot 3^8 = 2^{12} \cdot 6561 \end{aligned}$$

In totale si avranno quindi $2^{12} \cdot 6561$ possibili loghi. Poiché la prima potenza di 2 che supera 6561 è 2^{13}, per codificare i possibili loghi serviranno $\lceil \log_2(2^{12} \cdot 6561) \rceil = \lceil \log_2 2^{12} + \log_2 6561 \rceil = \lceil 12 + \log_2 6561 \rceil = 12 + \lceil \log_2 6561 \rceil = 12 + 13 = 25$ bit.

Nota: Per un refuso, nella versione originale del testo dell'esercizio era riportato "Ogni logo viene formato allineando 4 forme" invece di "Ogni logo viene formato allineando 4 figure". Tale frase poteva essere interpretata in almeno quattro modi:

(i) "Ogni logo viene formato allineando 4 figure aventi forme qualsiasi";

(ii) "Ogni logo viene formato allineando 4 figure aventi la stessa forma";

(iii) "Ogni logo viene formato allineando 4 figure aventi forme differenti";

(iv) "Ogni logo viene formato allineando 4 figure aventi forme differenti, ma identico colore e dimensione".

(v) "Ogni logo viene formato allineando 4 figure aventi forme qualsiasi, ma identico colore e dimensione".

Il caso (i) coincide con quello della risoluzione sopra riportata.

Il caso (ii), logo composto da figure con la stessa forma, richiede di calcolare le disposizioni con ripetizione di 18 oggetti (6 colori $\times$ 3 dimensioni) su 4 posti, ottenendo così $D_r(18, 4) = 18^4 = 2^4 \cdot 3^8 = 2^4 \cdot 6561$ configurazioni differenti per ogni forma, per un totale di $4 \times 2^4 \cdot 6561 = 2^6 \cdot 6561$ loghi differenti (rappresentabili con 19 bit).

Il caso (iii), logo composto da figure con forme differenti, il numero di differenti loghi può essere calcolato come segue. Al primo posto possono essere messi $6 \times 3 \times 4$ figure differenti. Al secondo posto possono essere messe tutte le figure che hanno una forma differente da quella messa al primo posto: esse sono $6 \times 3 \times 3$. Al terzo posto possono essere messe tutte le figure che hanno una forma differente da quelle messe ai primi due posti: esse sono $6 \times 3 \times 2$. Al

quarto posto possono essere messe solo le figure con una forma che già non compare nei primi tre posti: esse sono 6×3. Quindi, si hanno $(6 \cdot 3)^4 \cdot 4 \cdot 3 \cdot 2 = 2^7 \cdot 3^9 = 2^7 \cdot 19683$ configurazioni differenti, che necessitano di $7 + 15 = 22$ bit.

Nel caso (iv), logo composto da figure con lo stesso colore e dimensione, ma con forma differente, il numero di differenti loghi per ogni combinazione di colore e dimensione è dato dalle disposizioni di 4 elementi (caratterizzati per la forma) su 4 posti. Poiché il numero di combinazioni di colore e dimensione è 18 (6 colori e 3 dimensioni), quindi si hanno $18 \times D(4, 4) = 18 \cdot 4 \cdot 3 \cdot 2 = 2^4 \cdot 3^3 = 2^4 \cdot 27$ differenti configurazioni, le quali richiedono 9 bit per essere rappresentate.

Similmente, nel caso (v), logo composto da figure con lo stesso colore e dimensione, ma con forma qualsiasi, il numero di differenti loghi per ogni combinazione di colore e dimensione è dato dalle disposizioni con ripetizione di 4 elementi (caratterizzati per la forma) su 4 posti. Poiché il numero di combinazioni di colore e dimensione è 18 (6 colori e 3 dimensioni), quindi si hanno $18 \times D_r(4, 4) = 18 \cdot 4^4 = 2^9 \cdot 3^2 = 2^9 \cdot 9$ differenti configurazioni, le quali richiedono 13 bit per essere rappresentate.

Esercizio 4

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

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

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 paga, incassi, e viceversa):

a) se Bice paga, Antonio e Carlo incassano;

b) Carlo incassa, Antonio o Bice no;

c) Antonio paga solo se anche Bice fa lo stesso;

d) Carlo e Bice incassano;

e) Carlo incassa se e solo se Antonio paga;

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio paga
$\neg a$	Antonio incassa
b	Bice paga
$\neg b$	Bice incassa
c	Carlo paga
$\neg c$	Carlo incassa

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

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

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

c) $a \rightarrow b$

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

e) $\neg c \leftrightarrow a$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

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

b)

La dimostrazione della parte b) è riportata in figura 2.

c)

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

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

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

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

Figura 2: Soluzione della parte b) dell'esercizio 6.