Università degli Studi di Milano

Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006 docente: Stefano Ferrari

19.07.2006 — 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) $k = (61)_7$, $n = 10$

b) $k = (33)_{10}$, $n = 2$

c) $k = (\mathrm{A3})_{16}$, $n = 2$

d) $k = (413)_8$, $n = 2$

e) $k = (124)_5$, $n = 2$

f) $k = (10111000)_2$, $n = 16$

Soluzione

a) $(61)_7 = 6 \cdot 7^1 + 1 \cdot 7^0 = 6 \cdot 7 + 1 \cdot 1 = 42 + 1 = 43$

$(61)_7 = (43)_{10}$

b)

quoziente	resto
33	
16	1
8	0
4	0
2	0
1	0
0	1

$(33)_{10} = (100001)_2$

c)

base 16	A	3
base 2	1010	0011

$(\mathrm{A3})_{16} = (10100011)_2$

d)

base 8	4	1	3
base 2	100	001	011

$(413)_8 = (100001011)_2$

e) $(124)_5 = 1 \cdot 5^2 + 2 \cdot 5^1 + 4 \cdot 5^0 = 1 \cdot 25 + 2 \cdot 5 + 4 \cdot 1 = 25 + 10 + 4 = 39$

quoziente	resto
39	
19	1
9	1
4	1
2	0
1	0
0	1

$(124)_5 = (100111)_2$

f)

base 2	1011	1000
base 16	B	8

$(10111000)_2 = (\mathrm{B8})_{16}$

Esercizio 2

Dati $a = 12$, $b = -5$ e $n = 4$, 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 4 bit possono essere rappresentati tutti i numeri interi compresi fra -2^{4-1} e $2^{4-1} - 1$. Possono pertanto essere rappresentati senza causare overflow tutti e soli i numeri x che rispettano la condizione $-8 \leq x \leq 7$.

1. $2^n + a = 2^4 + 12 = 28$. Codificando 28 in binario e troncando tale codifica a 4 bit si ottiene: $s_a = 1100$.

   Poiché $a = 12 > 7$, si è verificato un overflow.

$2^n + b = 2^4 - 5 = 11$. Codificando 11 in binario e troncando tale codifica a 4 bit si ottiene: $s_b = 1011$.

Poiché $-8 \leq -5 \leq 7$, non si è verificato un overflow.

2. La somma binaria di 1100 e 1011, troncata a 4 bit è: $s_a + s_b = 0111$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 0111, si è verificato un overflow.

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

1011		sottraendo, s_b
0100	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
0101	+	$-s_b$
1100	=	s_a
10001		si devono considerare solo gli ultimi 4 bit
0001		$s_a - s_b$

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

Esercizio 3

Una azienda specializzata in prodotti per la casa esibisce nel proprio catalogo i seguenti prodotti:

- posate: modelli *Baroque*, *Romantic* e *Modern*;
- piatti: modelli *Classico*, *Colorato*, *TuttiGiorni*, *Raffinato* e *Ondulato*;
- bicchieri: modelli *Zaphir* e *Cristal*.

L'azienda commercializza i prodotti in due kit:

- kit *Base*: una confezione composta da un servizio da 6 di posate, un servizio da 6 di piatti e un servizio da 6 di bicchieri;
- kit *Family*: una confezione composta da due servizi da 6 di posate, tre servizi da 6 di piatti e un servizio da 6 di bicchieri.

Si calcoli:

a) il numero di bit necessari per codificare ciascun tipo di prodotto (posate, piatti, bicchieri);

b) il numero di bit necessari per codificare i possibili kit *Base*;

c) il numero di bit necessari per codificare i possibili kit *Family*.

I servizi da 6 sono composti da 6 unità identiche.

Soluzione

a)
- 3 modelli di posate: $\lceil \log_2 3 \rceil = 2$ bit;
- 5 modelli di piatti: $\lceil \log_2 5 \rceil = 3$ bit;
- 2 modelli di bicchieri: $\lceil \log_2 2 \rceil = 1$ bit.

b) Per la regola moltiplicativa, ci sono $3 \times 5 \times 2 = 30$ possibili kit *Base*, quindi servono $\lceil \log_2 30 \rceil = 5$ bit.

c) Nei kit *Family* sono presenti due servizi di posate (scelti su 3 modelli), tre servizi di piatti (scelti fra 5 modelli) e un servizio di bicchieri (scelto fra 2 modelli). Sembra ragionevole pensare che gli elementi dei kit possano essere ripetuti e che l'ordine non abbia importanza. Quindi, per ogni elemento il numero di configurazioni che possono essere trovate in un kit *Family* è dato dalle combinazioni con ripetizione:

- per le posate:

$$C_r(3,\,2) = C(3+2-1,\,2) = \frac{4!}{(4-2)!(2)!} = \frac{4 \cdot 3}{2!} = 2 \cdot 3$$

- per i piatti:

$$C_r(5,\,3) = C(5+3-1,\,3) = \frac{7!}{(7-3)!(3)!} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 5 \cdot 7$$

- per i bicchieri:

$$C_r(2,\,1) = C(2+1-1,\,1) = \frac{2!}{(2-1)!(1)!} = 2$$

Per la regola moltiplicativa, si potranno avere un numero di differenti kit pari al prodotto delle configurazioni di ciascun elemento. Pertanto si potranno avere $2 \cdot 3 \cdot 5 \cdot 7 \cdot 2 = 2^2 \cdot 105$ possibili kit. Poiché la prima potenza di 2 che supera 105 è 2^7, per codificare i possibili kit serviranno $\lceil \log_2(2^2 \cdot 105) \rceil = \lceil \log_2 2^2 + \log_2 105 \rceil = \lceil 2 + \log_2 105 \rceil = 2 + \lceil \log_2 105 \rceil = 2 + 7 = 9$ bit.

Esercizio 4

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

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

Soluzione

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

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

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

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non taglia, incolli, e viceversa):

a) Carlo non taglia, Bice e Anna sì;

b) Carlo incolla solo se anche Anna fa lo stesso;

c) se Carlo incolla, Bice e Anna tagliano;

d) Bice taglia se e solo se Carlo incolla;

e) Anna o Bice incollano;

Soluzione

Dati i seguenti simboli proposizionali:

a	Anna taglia
$\neg a$	Anna incolla
b	Bice taglia
$\neg b$	Bice incolla
c	Carlo taglia
$\neg c$	Carlo incolla

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

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

b) $\neg c \to \neg a$

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

d) $b \leftrightarrow \neg c$

e) $\neg a \vee \neg b$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$a \vee b$	Ip1
(2)	$\neg a \to b$	Def. implicazione (1)
(3)	$a \to (b \wedge c)$	Ip2
(4)	$(a \to b) \wedge (a \to c)$	Distrib. delle cons. (3)
(5)	$a \to b$	Elim. di cong. (4)
(6)	b	Dim. per casi (2) e (4)
(7)	$c \to b$	Verum sequitur (6)

b)

(1)	$a \vee (a \wedge b)$	Ip1
(2)	$(a \vee a) \wedge (a \vee b)$	Distrib. (1)
(3)	$a \vee a$	Elim. di cong. (2)
(4)	a	Idempotenza (3)
(5)	$a \to (\neg a \vee c)$	Ip2
(6)	$\neg a \vee c$	M. Ponens (4) e (5)
(7)	$a \to c$	Def. di implicazione (6)
(8)	c	M. Ponens (4) e (7)
(9)	$\neg c \to c$	Verum sequitur (8)

c)

(1)	$(b \vee c) \vee a$	Ip1
(2)	$\neg(b \vee c) \to a$	Def. di implicazione (1)
(3)	$\neg a \vee c$	Ip2
(4)	$a \to c$	Def. di implicazione (3)
(5)	$\neg(b \vee c) \to c$	Sillogismo ipotetico (2) e (4)
(6)	$(b \vee c) \vee c$	Def. di implicazione (5)
(7)	$b \vee c \vee c$	Associatività (6)
(8)	$b \vee c$	Idempotenza (7)
(9)	$\neg b \to c$	Def. di implicazione (8)