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

20.04.2006 — 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) $k = (34)_9$, $n = 10$

b) $k = (71)_{10}$, $n = 2$

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

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

e) $k = (143)_5$, $n = 2$

f) $k = (11100111)_2$, $n = 16$

Soluzione

a) $(34)_9 = 3 \cdot 9^1 + 4 \cdot 9^0 = 3 \cdot 9 + 4 \cdot 1 = 27 + 4 = 31$

$(34)_9 = (31)_{10}$

b)

quoziente	resto
71	
35	1
17	1
8	1
4	0
2	0
1	0
0	1

$(71)_{10} = (1000111)_2$

c)

base 16	8	B
base 2	1000	1011

$(8\mathrm{B})_{16} = (10001011)_2$

d)

base 8	1	2	6
base 2	001	010	110

$(126)_8 = (1010110)_2$

$(143)_5 = 1 \cdot 5^2 + 4 \cdot 5^1 + 3 \cdot 5^0 = 1 \cdot 25 + 4 \cdot 5 + 3 \cdot 1 = 25 + 20 + 3 = 48$

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

$(143)_5 = (110000)_2$

e)

base 2	1110	0111
base 16	E	7

$(11100111)_2 = (\mathrm{E}7)_{16}$

Esercizio 2

Dati $a = 12$, $b = -7$ 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.

$2^n + b = 2^4 - 7 = 9$. Codificando 9 in binario e troncando tale codifica a 4 bit si ottiene: $s_b = 1001$.

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

2. La somma binaria di 1100 e 1001, troncata a 4 bit è: $s_a + s_b = 0101$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 0101, si è verificato un overflow.

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

1001		sottraendo, s_b
0110	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
0111	+	$-s_b$
1100	=	s_a
10011		si devono considerare solo gli ultimi 4 bit
0011		$s_a - s_b$

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

Esercizio 3

Una azienda di ristorazione confeziona panini con le seguenti caratteristiche:

- tipo: semola, integrale, rustico;
- farcitura: prosciutto, formaggio, verdure, salame;
- dimensione: piccolo, grande.

I panini vengono venduti confezionati in un scatola che ne contiene 3, tutti della stessa dimensione, ma con almeno una delle altre caratteristiche diversa. Al fine di prolungare la durata del prodotto, la scatola ha un'apertura tale da consentire l'estrazione di un panino per volta (in ordine inverso a quello di inserimento).

Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (tipo, farcitura, dimensione);

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

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

Soluzione

a)
- 3 tipi: $\lceil \log_2 3 \rceil = 2$ bit;
- 4 farciture: $\lceil \log_2 4 \rceil = 2$ bit;
- 2 dimensioni: $\lceil \log_2 2 \rceil = 1$ bit.

b) Ci sono $3 \times 4 \times 2 = 24$ varianti di panino, quindi servono $\lceil \log_2 24 \rceil = 5$ bit.

c) Le confezioni sono sono composte da 3 palloncini della stessa dimensione. Le ripetizioni non sono ammesse in quanto tutte le altre caratteristiche (tipo e farcitura) devono essere diverse. Vi sono specifiche esplicite riguardo all'ordine con cui i panini compaiono nella confezione, e ciò lascia pensare che l'ordine sia da tenere in considerazione. Quindi, per ogni dimensione, si potranno avere un numero di confezioni pari al numero di disposizioni semplici di 12 oggetti (3 tipi $\times$ 4 farciture) su 3 posti.

$$\begin{aligned} D(12, 3) &= \frac{12!}{(12-3)!} = 12 \cdot 11 \cdot 10 = \\ &= 2^3 \cdot 3 \cdot 5 \cdot 11 = 2^3 \cdot 165 \end{aligned}$$

Poiché si hanno 2 differenti dimensioni, in totale si avranno quindi $2 \cdot 2^3 \cdot 165 = 2^4 \cdot 165$ possibili confezioni. Poiché la prima potenza di 2 che supera 165 è 2^8, per codificare le possibili confezioni serviranno $\lceil \log_2(2^4 \cdot 165) \rceil = \lceil \log_2 2^4 + \log_2 165 \rceil = \lceil 4 + \log_2 165 \rceil = 4 + \lceil \log_2 165 \rceil = 4 + 8 = 12$ bit.

Esercizio 4

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

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

Soluzione

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

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non disegna, scriva, e viceversa):

a) Carlo disegna solo se anche Bice fa lo stesso;

b) Carlo non scrive, Bice e Antonio sì;

c) Bice disegna se e solo se Carlo scrive;

d) Antonio o Bice disegnano;

e) se Carlo scrive, Bice e Antonio disegnano;

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

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

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio disegna
$\neg a$	Antonio scrive
b	Bice disegna
$\neg b$	Bice scrive
c	Carlo disegna
$\neg c$	Carlo scrive

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

a) $c \to b$

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

c) $b \leftrightarrow \neg c$

d) $a \vee b$

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

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	a	Ip1
(2)	$a \vee c$	Introd. disgiunzione (1)
(3)	$(a \wedge b) \vee \neg(a \vee c)$	Ip2
(4)	$\neg(a \vee c) \vee (a \wedge b)$	Commutatività (3)
(5)	$(a \vee c) \to (a \wedge b)$	Def. implicazione (4)
(6)	$a \wedge b$	Modus Ponens (2) e (5)
(7)	b	Elim. congiunzione (6)

b)

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

c)

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