Fondamenti di informatica per la sicurezza

Università degli Studi di Milano

anno accademico 2007–2008 docente: Stefano Ferrari

05.11.2007 — Soluzione del primo compitino — versione B

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) $k = (82)_{10}$, $n = 2$

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

d) $k = (740)_8$, $n = 2$

e) $k = (231)_5$, $n = 2$

f) $k = (1011101)_2$, $n = 16$

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
82	
41	0
20	1
10	0
5	0
2	1
1	0
0	1

$(82)_{10} = (1010010)_2$

c)

base 16	2	C
base 2	0010	1100

$(2C)_{16} = (101100)_2$

d)

base 8	7	4	0
base 2	111	100	000

$(740)_8 = (111100000)_2$

e) $(231)_5 = 2{\cdot}5^2+3{\cdot}5^1+1{\cdot}5^0 = 2{\cdot}25+3{\cdot}5+1{\cdot}1 = 50 + 15 + 1 = 66$

quoziente	resto
66	
33	0
16	1
8	0
4	0
2	0
1	0
0	1

$(231)_5 = (1000010)_2$

f)

base 2	0101	1101
base 16	5	D

$(1011101)_2 = (5D)_{16}$

Esercizio 2

Dati $a = -17$, $b = 1$ e $n = 5$, calcolare in complemento a 2 a n bit, specificando sempre 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. $2^n+a = 2^5-17 = 15$. Codificando 15 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 01111$.

Poiché $a = -17 < -16$, si è verificato un overflow.

$2^n + b = 2^5 + 1 = 33$. Codificando 33 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 00001$.

Poiché $-16 \leq 1 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 01111 e 00001, 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 $-s_b$.

00001		sottraendo, s_b
11110	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
011111		si devono considerare solo gli ultimi 5 bit
11111	+	$-s_b$
01111	=	s_a
101110		si devono considerare solo gli ultimi 5 bit
01110		$s_a - s_b$

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

Esercizio 3

Una azienda produce pietanze utilizzando i seguenti ingredienti:

- carne: manzo, pollo, struzzo, maiale, coniglio;
- verdura: peperone, cipolla;
- spezie: aglio, origano, zenzero, rosmarino.

Ogni pietanza viene confezionata utilizzando un ingrediente di ogni categoria.

Inoltre, vengono prodotti spiedini con 8 pezzi di carne.

Si calcoli:

a) il numero di bit necessari per codificare le caratteristiche degli ingredienti (carne, verdura, spezie);

b) il numero di bit necessari per codificare le possibili pietanze;

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

Soluzione

a)
- 5 carni: $\lceil \log_2 5 \rceil = 3$ bit;
- 2 verdure: $\lceil \log_2 2 \rceil = 1$ bit;
- 4 spezie: $\lceil \log_2 4 \rceil = 2$ bit.

b) Per la regola moltiplicativa, ci sono $5 \times 2 \times 4 = 40$ possibili pietanze, quindi servono $\lceil \log_2 40 \rceil = 6$ bit.

c) Ogni spiedino è composto da otto pezzi di carne. Poiché i tipi di carne sono solo cinque, appare evidente che le ripetizioni siano possibili. Due interpretazioni sono invece possibili per l'importanza dell'ordine: se anche l'apperenza visiva viene tenuta in considerazione, l'ordine è importante, mentre se si considera solo il gusto, l'ordine può non essere considerato. Per esempio, uno spiedino formato da manzo, coniglio e pollo apparirà differente da uno spiedino formato da coniglio, manzo e pollo, mentre non vi sarà differenza dal punto di vista della degustazione (lo spiedino permette di accedere ad un qualsiasi pezzo). Pertanto, non considerando l'ordine, il numero di configurazioni che possono essere assunte da uno spiedino è dato dalle combinazioni con ripetizione di 5 elementi (le carni) su 8 posti (gli elementi dello spiedino):

$$
\begin{aligned}
C_r(5,\, 8) = C(12,\, 8) &= \frac{12!}{8!\,4!} \\
&= \frac{12 \cdot 11 \cdot 10 \cdot 9}{4 \cdot 3 \cdot 2} = 11 \cdot 5 \cdot 9 \\
&= 495
\end{aligned}
$$

Poiché la prima potenza di 2 che supera 495 è 2^9, per codificare i possibili gelati multistrato serviranno $\lceil \log_2 495 \rceil = 9$ bit.

Se invece si fosse considerato importante l'ordine, il numero di configurazioni possibili di uno spiedino sarebbe stato dato dalle disposizioni con ripetizione di 5 elementi (le carni) su 8 posti (gli elementi dello spiedino):

$$D_r(5,\, 8) = 5^8 = 390625$$

Poiché la prima potenza di 2 che supera 390625 è 2^{19}, per codificare i possibili spiedini sarebbero serviti $\lceil \log_2 390625 \rceil = 19$ bit.

Esercizio 4

Sia data la seguente formula, F:

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

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.

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

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

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non osserva, ignori, e viceversa):

a) sia Carlo, sia Bice ignorano;

b) Bice osserva se e solo se Antonio e Carlo ignorano;

c) Carlo non osserva, Bice o Antonio sì;

d) Antonio osserva solo se osserva anche Bice;

e) quando Antonio osserva, Bice e Carlo ignorano.

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio osserva
$\neg a$	Antonio ignora
b	Bice osserva
$\neg b$	Bice ignora
c	Carlo osserva
$\neg c$	Carlo ignora

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

a) $\neg c \land \neg b$

b) $b \leftrightarrow (\neg a \land \neg c)$

c) $\neg c \land (b \lor a)$

d) $a \to b$

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

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

a) **Ip1** a
Ip2 $b \lor (\neg a \land c)$
Tesi b

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

c) **Ip1** $\neg((c \leftrightarrow a) \lor (b \land \neg a))$
Ip2 c
Tesi $\neg b$

Soluzione

a)

(1)	$b \lor (\neg a \land c)$	Ip2
(2)	$(b \lor \neg a) \land (b \lor c)$	Distributività (1)
(3)	$b \lor \neg a$	Elim. congiunzione (2)
(4)	$\neg b \to \neg a$	Def. implicazione (3)
(5)	a	Ip1
(6)	$\neg\neg b$	Modus tollens (4) e (5)
(7)	b	Doppia negazione (6)

b)

(1)	$\neg(c \to (b \land \neg a))$	Ip1
(2)	$\neg(\neg c \lor (b \land \neg a))$	Def. implicazione (1)
(3)	$c \land \neg(b \land \neg a)$	Legge di De Morgan (2)
(4)	$\neg(b \land \neg a)$	Elim. congiunzione (3)
(5)	$\neg b \lor a$	Legge di De Morgan (4)
(6)	$b \to a$	Def. implicazione (5)
(7)	$\neg a$	Ip2
(8)	$\neg b$	Modus tollens (6) e (7)

c)

(1)	$\neg((c \leftrightarrow a) \lor (b \land \neg a))$	Ip1
(2)	$\neg(c \leftrightarrow a) \land \neg(b \land \neg a))$	De Morgan (1)
(3)	$\neg(c \leftrightarrow a)$	Elim. cong. (2)
(4)	$\neg c \leftrightarrow a$	Neg. di biimpl. (3)
(5)	$(\neg c \to a) \land (a \to \neg c)$	Def. biimpl. (4)
(6)	$a \to \neg c$	Elim. cong. (5)
(7)	c	Ip2
(8)	$\neg a$	M. tollens (6) e (7)
(9)	$\neg(b \land \neg a)$	Elim. cong. (2)
(10)	$\neg b \lor a$	De Morgan (9)
(11)	$\neg b$	Sill. disg. (8) e (10)