Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

Università degli Studi di Milano

anno accademico 2007–2008 docente: Stefano Ferrari

01.12.2007 — 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) $k = (621)_7$, $n = 10$

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

c) $k = (3\text{A})_{16}$, $n = 2$

d) $k = (706)_8$, $n = 2$

e) $k = (104)_5$, $n = 2$

f) $k = (1010101)_2$, $n = 16$

Soluzione

a) $(621)_7 = 6\cdot7^2+2\cdot7^1+1\cdot7^0 = 6\cdot49+2\cdot7+1\cdot1 = 294 + 14 + 1 = 309$

$(621)_7 = (309)_{10}$

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	3	A
base 2	0011	1010

$(3\text{A})_{16} = (111010)_2$

d)

base 8	7	0	6
base 2	111	000	110

$(706)_8 = (111000110)_2$

e) $(104)_5 = 1\cdot5^2+0\cdot5^1+4\cdot5^0 = 1\cdot24+0\cdot5+4\cdot1 = 24 + 0 + 4 = 29$

quoziente	resto
29	
14	1
7	0
3	1
1	1
0	1

$(104)_5 = (11101)_2$

f)

base 2	0101	0101
base 16	5	5

$(1010101)_2 = (55)_{16}$

Esercizio 2

Dati $a = 8$, $b = -16$ 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. $2^n + a = 2^5 + 8 = 40$. Codificando 40 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 01000$.

   Poiché $-16 \leq 8 \leq 15$, non si è verificato un overflow.

$2^n + b = 2^5 - 16 = 16$. Codificando 16 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 10000$.

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

2. La somma binaria di 01000 e 10000, troncata a 5 bit è: $s_a + s_b = 11000$.

   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 $-s_b$.

10000		sottraendo, s_b
01111	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
10000	+	$-s_b$
01000	=	s_a
11000		$s_a - s_b$

   Poiché s_a e s_b hanno il primo bit diverso, e il primo bit della loro differenza, 11000, non è uguale al primo bit di s_a, si è verificato un overflow.

Esercizio 3

Una bar prepara panini utilizzando i seguenti ingredienti:

- tipo: baguette, integrale, arabo, segale;
- farcitura: prosciutto, tonno, mozzarella, pancetta, fontina, speck, pecorino;
- salsa: tonnata, rosa, maionese.

Ogni panino viene confezionato utilizzando un ingrediente di ogni categoria.

Inoltre, vengono proposti anche panini *super* che contengono tre farciture differenti.

Si calcoli:

a) il numero di bit necessari per codificare le caratteristiche degli ingredienti (tipo di pane, facitura, salsa);

b) il numero di bit necessari per codificare i possibili panini;

c) il numero di bit necessari per codificare i possibili panini *super*.

Soluzione

a)
- 4 tipi: $\lceil \log_2 4 \rceil = 2$ bit;
- 7 farciture: $\lceil \log_2 7 \rceil = 3$ bit;
- 3 salse: $\lceil \log_2 3 \rceil = 2$ bit.

b) Per la regola moltiplicativa, ci sono $4 \times 7 \times 3 = 84$ possibili panini, quindi servono $\lceil \log_2 84 \rceil = 7$ bit.

c) Ogni panino *super* è composto da un pane, una salsa e tre farciture. Poiché appare ragionevole pensare che l'ordine con cui le farciture vengono disposte nel panino non abbia importanza e sono esplicitamente vietate le ripetizioni, il numero di configurazioni che possono essere assunte dalle farciture di un panino *super* è dato dalle combinazioni semplici di 7 elementi (le farciture disponibili) su 3 posti (il numero di farciture presenti nel panino *super*):

$$C(7,\,3) = \frac{7!}{4!\,3!} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 35$$

Quindi, per la regola moltiplicativa, il numero di panini *super* possibili sarà $4 \times 35 \times 3 = 2^2 \cdot 105$. Poiché la prima potenza di 2 che supera 105 è 2^7, per codificare le possibili offerte speciali 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

Sia data la seguente formula, F:

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

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.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non scrive, cancelli, e viceversa):

a) sia Carlo, sia Bice scrivono;

b) Antonio cancella solo se cancella anche Bice;

c) Bice cancella se e solo se Antonio e Carlo scrivono;

d) Carlo non scrive, Bice o Antonio sì;

e) quando Antonio scrive, Bice e Carlo cancellano.

Soluzione

Dati i seguenti simboli proposizionali:

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

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

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

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

a) $c \land b$

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

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

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

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

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$b \to (c \lor \neg a)$	Ip2
(2)	$\neg b \lor (c \lor \neg a)$	Def. implicazione (1)
(3)	$\neg b \lor c \lor \neg a$	Associatività (2)
(4)	$\neg b \lor \neg a \lor c$	Commutatività (3)
(5)	$\neg(\neg b \lor \neg a) \to c$	Def. implicazione (4)
(6)	$(b \land a) \to c$	De Morgan (5)
(7)	$c \lor (b \land a)$	Ip1
(8)	$(b \land a) \lor c$	Commutatività (7)
(9)	$\neg(b \land a) \to c$	Def. Implicazione (8)
(10)	c	Dim. per casi (6) e (9)

b)

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

c)

(1)	$b \lor c$	Ip2
(2)	$b \lor c \lor \neg a$	Intr. disg. (1)
(3)	$\neg a \lor c \lor b$	Commutatività (2)
(4)	$(a \to c) \lor b$	Def. implicazione (3)
(5)	$\neg(a \to c)$	Ip1
(6)	b	Sill. disgiuntivo (4) e (5)