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

24.06.2008 — 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) $k = (304)_7$, $n = 10$

b) $k = (73)_{10}$, $n = 2$

c) $k = (\mathrm{C3})_{16}$, $n = 2$

d) $k = (231)_8$, $n = 2$

e) $k = (420)_5$, $n = 2$

f) $k = (1101110)_2$, $n = 16$

Soluzione

a) $(304)_7 = 3{\cdot}7^2+0{\cdot}7^1+4{\cdot}7^0 = 3{\cdot}49+0{\cdot}7+4{\cdot}1 = 147 + 0 + 4 = 151$

$(304)_7 = (151)_{10}$

b)

quoziente	resto
73	
36	1
18	0
9	0
4	1
2	0
1	0
0	1

$(73)_{10} = (1001001)_2$

c)

base 16	C	3
base 2	1100	0011

$(\mathrm{C3})_{16} = (11000011)_2$

d)

base 8	2	3	1
base 2	010	011	001

$(231)_8 = (10011001)_2$

e) $(420)_5 = 4{\cdot}5^2+2{\cdot}5^1+0{\cdot}5^0 = 4{\cdot}25+2{\cdot}5+0{\cdot}1 = 100 + 10 + 0 = 110$

quoziente	resto
110	
55	0
27	1
13	1
6	1
3	0
1	1
0	1

$(420)_5 = (1101110)_2$

f)

base 2	0110	1110
base 16	6	E

$(1101110)_2 = (6\mathrm{E})_{16}$

Esercizio 2

Dati $a = -17$, $b = 3$ 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.

$2^n + b = 2^5 + 3 = 35$. 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 01111 e 00011, troncata a 5 bit è: $s_a + s_b = 10010$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 10010, 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	+	$-s_b$
01111	=	s_a
101100		si devono considerare solo gli ultimi 5 bit
01100		$s_a - s_b$

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

Esercizio 3

Una azienda tessile produce camicie con le seguenti caratteristiche:

- taglia: *extra small*, *small*, *medium*, *large*, *extra large*;
- tessuto: cotone, lino, seta;
- colletto: lungo, corto.

Tali camicie vengono vendute singolarmente o in offerta speciale in confezioni da cinque camicie della stessa taglia.

Si calcoli:

a) il numero di bit necessari per codificare le caratteristiche (taglia, tessuto, colletto);

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

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

Soluzione

a)
- 5 taglie: $\lceil \log_2 5 \rceil = 3$ bit;
- 3 tessuti: $\lceil \log_2 3 \rceil = 2$ bit;
- 2 colletti: $\lceil \log_2 2 \rceil = 1$ bit.

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

c) Ogni offerta speciale è composta da 5 camicie della stessa taglia. Data la natura dei beni e dell'offerta, pare ragionevole che siano ammesse le ripetizioni (uno potrebbe essere interessato ad avere anche tutte e cinque le camicie uguali) e che l'ordine non sia importante. Per ogni taglia, il numero di offerte speciali differenti è quindi dato dalle combinazioni con ripetizione di 6 elementi (le possibili camicie della stessa taglia) su 5 posti (il numero di camicie dell'offerta speciale):

$$\begin{aligned} C_r(6,\,5) &= C(10,5) = \frac{10!}{5!\cdot 5!} = \\ &\frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{5\cdot 4\cdot 3\cdot 2} = 2^2\cdot 7\cdot 9 = \\ &2^2\cdot 63 \end{aligned}$$

Essendoci 5 taglie, il numero totale di offerte speciali differenti è $5 \times 2^2 \cdot 63 = 2^2 \cdot 315$. Poiché la prima potenza di 2 che supera 315 è 2^9, per codificare le offerte speciali serviranno $\lceil \log_2(2^2 \cdot 315) \rceil = \lceil \log_2 2^2 + \log_2 315 \rceil = \lceil 2 + \log_2 315 \rceil = 2 + \lceil \log_2 315 \rceil = 2 + 9 = 11$ bit.

Esercizio 4

Sia data la seguente formula, F:

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

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 preleva, versi, e viceversa):

a) quando Alice versa, Bice e Carlo prelevano;

b) Carlo non preleva, Bice e Alice sì;

c) sia Carlo, sia Bice prelevano;

d) Alice preleva se e solo se Bice o Carlo versano;

e) Alice preleva solo se preleva anche Carlo.

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

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

Soluzione

Dati i seguenti simboli proposizionali:

a	Alice preleva
$\neg a$	Alice versa
b	Bice preleva
$\neg b$	Bice versa
c	Carlo preleva
$\neg c$	Carlo versa

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

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

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

c) $c \wedge b$

d) $a \leftrightarrow (\neg b \vee \neg c)$

e) $a \to c$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

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

b)

(1)	$(a \to b) \leftrightarrow c$	Ip1
(2)	$((a \to b) \to c) \wedge (c \to (a \to b))$	Def. biimpl. (1)
(3)	$(a \to b) \to c$	Elim. cong. (2)
(4)	$\neg c$	Ip2
(5)	$\neg(a \to b)$	M.T. (3) e (4)
(6)	$\neg(\neg a \vee b)$	Def. impl. (5)
(7)	$a \wedge \neg b$	De Morgan (6)
(8)	a	Elim. cong. (7)

c)

(1)	$\neg c$	Ip2
(2)	$\neg c \vee b$	Introd. disgiunzione (1)
(3)	$c \to b$	Def. implicazione (2)
(4)	$(c \to b) \to a$	Ip1
(5)	a	Modus ponens (3) e (4)