Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006

docente: Stefano Ferrari

02.12.2005 — Soluzione del primo compitino — versione C

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) $k = (451)_7$, $n = 10$

b) $k = (83)_{10}$, $n = 2$

c) $k = (\mathrm{F1})_{16}$, $n = 2$

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

e) $k = (430)_5$, $n = 2$

f) $k = (1011010)_2$, $n = 16$

Soluzione

a) $(451)_7 = 4 \cdot 7^2 + 5 \cdot 7^1 + 1 \cdot 7^0 = 4 \cdot 49 + 5 \cdot 7 + 1 \cdot 1 = 196 + 35 + 1 = 232$

$(451)_7 = (232)_{10}$

b)

quoziente	resto
83	
41	1
20	1
10	0
5	0
2	1
1	0
0	1

$(83)_{10} = (1010011)_2$

c)

base 16	F	1
base 2	1111	0001

$(\mathrm{F1})_{16} = (11110001)_2$

d)

base 8	7	0	6
base 2	111	000	110

$(706)_8 = (111000110)_2$

e) $(430)_5 = 4 \cdot 5^2 + 3 \cdot 5^1 + 0 \cdot 5^0 = 4 \cdot 25 + 3 \cdot 5 + 0 \cdot 1 = 100 + 15 + 0 = 115$

quoziente	resto
115	
57	1
28	1
14	0
7	0
3	1
1	1
0	1

$(430)_5 = (1110011)_2$

f)

base 2	0101	1010
base 16	5	A

$(1011010)_2 = (5\mathrm{A})_{16}$

Esercizio 2

Dati $a = 2$, $b = 21$ e $n = 5$, 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 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. $2^n + a = 2^5 + 2 = 34$. Codificando 34 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 00010$.

Poiché $-16 \leq 2 \leq 15$, non si è verificato un overflow.

$2^n + b = 2^5 + 21 = 53$. Codificando 53 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 10101$.

Poiché $b = 21 > 15$, si è verificato un overflow.

2. La somma binaria di 00010 e 10101, troncata a 5 bit è: $s_a + s_b = 10111$.

   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 $-s_b$.

10101		sottraendo, s_b
01010	+	negazione delle cifre di s_b, $\overline{s_b}$
1	=	
01011	+	$-s_b$
00010	=	s_a
01101		$s_a - s_b$

   Poiché s_a e s_b hanno il primo bit diverso, e il primo bit della loro differenza, 01101, è uguale al primo bit di s_a, non si è verificato un overflow.

Esercizio 3

Una azienda produce penne biro con le seguenti caratteristiche:

- inchiostro: rosso, blu, nero, verde, viola;
- apertura: a scatto, a torsione;
- impugnatura: liscia, zigrinata, in gomma.

L'azienda commercializza le penne in confezioni da 20, tutte con lo stesso inchiostro.
Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (inchiostro, apertura, impugnatura);

b) il numero di bit necessari per codificare una penna;

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

Soluzione

a)
- 5 colori di inchiostro: $\lceil \log_2 5 \rceil = 3$ bit;
- 2 tipi di apertura: $\lceil \log_2 2 \rceil = 1$ bit;
- 3 tipi di impugnatura: $\lceil \log_2 3 \rceil = 2$ bit.

b) Ci sono $5 \times 2 \times 3 = 30$ varianti di biro, quindi servono $\lceil \log_2 30 \rceil = 5$ bit.

c) Le confezioni sono sono composte da 20 biro, tutte con lo stesso inchiostro. Sembra ragionevole ammettere le ripetizioni, ma non considerare l'ordine delle biro nella confezione. Quindi, per ogni colore di inchiostro, si potranno avere un numero di confezioni pari al numero di combinazioni con ripetizione di 6 oggetti (2 tipi di apertura $\times$ 3 tipi di impugnatura) su 20 posti.

$$\begin{aligned} C_r(6,\,20) &= C(6+20-1,\,20) = C(25,\,20) = \\ &= \binom{25}{20} = \frac{25!}{5! \cdot 20!} = \\ &= \frac{25 \cdot 24 \cdot 23 \cdot 22 \cdot 21}{5 \cdot 4 \cdot 3 \cdot 2} = \\ &= 5 \cdot 23 \cdot 2 \cdot 11 \cdot 21 = 2 \cdot 26565 \end{aligned}$$

Poiché si hanno 5 colori di inchiostro, in totale si avranno quindi $5 \cdot 2 \cdot 26565 = 2 \cdot 132825$ possibili confezioni. Poiché la prima potenza di 2 che supera 132825 è 2^{18}, per codificare le possibili confezioni serviranno $\lceil \log_2(2 \cdot 132825) \rceil = \lceil \log_2 2 + \log_2 132825 \rceil = \lceil 1 + \log_2 132825 \rceil = 1 + \lceil \log_2 132825 \rceil = 1 + 18 = 19$ bit.

Esercizio 4

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

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

Soluzione

La tabella di verità è riportata in figura 1. Poiché tutte le interpretazioni rendono vera la proposizione data, essa è una tautologia.

Esercizio 5

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

a) se Antonia cuce, Berto e Chiara tagliano;

b) Chiara non taglia, Berto o Antonia sì;

c) Chiara o Berto cuciono;

d) Antonia cuce solo se anche Berto fa lo stesso;

e) Berto taglia se e solo se Antonia cuce;

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonia cuce
$\neg a$	Antonia taglia
b	Berto cuce
$\neg b$	Berto taglia
c	Chiara cuce
$\neg c$	Chiara taglia

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

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

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

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

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

c) $c \vee b$

d) $a \rightarrow b$

e) $\neg b \leftrightarrow a$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$b \rightarrow (\neg b \wedge a)$	Ip2
(2)	$(b \rightarrow \neg b) \wedge (b \rightarrow a)$	Distr. delle cons. (1)
(3)	$b \rightarrow \neg b$	Elim. di cong. (2)
(4)	$\neg b \vee \neg b$	Def. implicazione (3)
(5)	$\neg b$	Idempotenza (4)
(6)	$\neg(c \wedge \neg b)$	Ip1
(7)	$\neg c \vee b$	Leggi di De Morgan (6)
(8)	$b \vee \neg c$	Commutatività (7)
(9)	$\neg b \rightarrow \neg c$	Def. implicazione (8)
(10)	$\neg c$	M. Ponens da (5) e (9)

b)

(1)	$\neg(a \wedge b)$	Ip2
(2)	$\neg a \vee \neg b$	Leggi di De Morgan (1)
(3)	$a \rightarrow \neg b$	Def. Implicazione (2)
(4)	$\neg b \vee (a \wedge c)$	Ip1
(5)	$(\neg b \vee a) \wedge (\neg b \vee c)$	Distributività (4)
(6)	$\neg b \vee a$	Elim. di cong. (5)
(7)	$a \vee \neg b$	Commutatività (6)
(8)	$\neg a \rightarrow \neg b$	Def. implicazione (7)
(9)	$\neg b$	Dim. per casi da (3) e (8)

c)

(1)	$a \wedge (a \vee (a \rightarrow a))$	Ip2
(2)	a	Elim. di cong. (1)
(3)	$a \rightarrow (c \wedge (a \vee a))$	Ip1
(4)	$(a \rightarrow c) \wedge (a \rightarrow (a \vee a))$	Distr. delle cons. (3)
(5)	$a \rightarrow c$	Elim. di cong. (4)
(6)	c	M. Ponens da (2) e (5)