Università degli Studi di Milano

Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2007–2008 docente: Stefano Ferrari

05.11.2007 — Soluzione del primo compitino — versione D

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) $k = (601)_7$, $n = 10$

b) $k = (39)_{10}$, $n = 2$

c) $k = (5\text{F})_{16}$, $n = 2$

d) $k = (370)_8$, $n = 2$

e) $k = (410)_5$, $n = 2$

f) $k = (1011110)_2$, $n = 16$

Soluzione

a) $(601)_7 = 6 \cdot 7^2 + 0 \cdot 7^1 + 1 \cdot 7^0 = 6 \cdot 49 + 0 \cdot 7 + 1 \cdot 1 = 294 + 0 + 1 = 295$

$(601)_7 = (295)_{10}$

b)

quoziente	resto
39	
19	1
9	1
4	1
2	0
1	0
0	1

$(39)_{10} = (100111)_2$

c)

base 16	5	F
base 2	0101	1111

$(5\text{F})_{16} = (1011111)_2$

d)

base 8	3	7	0
base 2	011	111	000

$(370)_8 = (11111000)_2$

e) $(410)_5 = 4 \cdot 5^2 + 1 \cdot 5^1 + 0 \cdot 5^0 = 4 \cdot 25 + 1 \cdot 5 + 0 \cdot 1 = 100 + 5 + 0 = 105$

quoziente	resto
105	
52	1
26	0
13	0
6	1
3	0
1	1
0	1

$(410)_5 = (1101001)_2$

f)

base 2	0101	1110
base 16	5	E

$(1011110)_2 = (5\text{E})_{16}$

Esercizio 2

Dati $a = -7$, $b = 16$ 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

Dati $a = -7$, $b = 16$ 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.

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. $2^n+a = 2^5-7 = 25$. Codificando 25 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 11001$.

   Poiché $-16 \leq -7 \leq 15$, non si è verificato un overflow.

   $2^n+b = 2^5+16 = 48$. Codificando 48 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 10000$.

   Poiché $b = 16 > 15$, si è verificato un overflow.

2. La somma binaria di 11001 e 10000, troncata a 5 bit è: $s_a + s_b = 01001$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 01001, 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		$-s_b$
		s_b e $-s_b$ hanno lo stesso segno: si è verificato un overflow
10000	+	$-s_b$
11001	=	s_a
101001		si devono considerare solo gli ultimi 5 bit
01001		$s_a - s_b$

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

Esercizio 3

Una agenzia viaggi propone viaggi con le seguenti caratteristiche:

- tipologia: relax, trekking, viaggio di nozze, viaggio di cultura, crociera;
- durata: 3 giorni, una settimana, 2 settimane, un mese, 6 mesi;
- classe: 2 stelle, 3 stelle, 4 stelle, super lusso.

Ogni viaggio è ovviamente caratterizzato da una caratteristica per ogni categoria.

Inoltre, viene proposta un forte sconto per chi acquisti tre viaggi.

Si calcoli:

a) il numero di bit necessari per codificare le caratteristiche (tipologia, durata, classe);

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

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

Soluzione

a)
- 5 tipologie: $\lceil \log_2 5 \rceil = 3$ bit;
- 5 durate: $\lceil \log_2 5 \rceil = 3$ bit;
- 4 classi: $\lceil \log_2 4 \rceil = 2$ bit.

b) Per la regola moltiplicativa, ci sono $5 \times 5 \times 4 = 100$ possibili viaggi, quindi servono $\lceil \log_2 100 \rceil = 7$ bit.

c) Ogni offerta speciale è composta da tre viaggi. Poiché appare ragionevole pensare che l'ordine non abbia importanza (i viaggi non devono essere necessariamente fruiti dalla stessa persona) e non sono esplicitamente vietate le ripetizioni (un viaggio per tre persone può essere realizzato acquistando tre viaggi con le medesime caratteristiche), il numero di configurazioni che possono essere assunte da una offerta speciale è dato dalle combinazioni con ripetizione di 100 elementi (i viaggi possibili) su 3 posti (il numero di viaggi dell'offerta):

$$C_r(100,\,3) = C(102,\,3) = \frac{102!}{99!\,3!} = \\ \frac{102 \cdot 101 \cdot 100}{3 \cdot 2} = 34 \cdot 101 \cdot 50 = \\ 2^2 \cdot 17 \cdot 25 \cdot 101 = 2^2 \cdot 42925$$

Poiché la prima potenza di 2 che supera 42925 è 2^{16}, per codificare le possibili offerte speciali serviranno $\lceil \log_2(2^2 \cdot 42925) \rceil = \lceil \log_2 2^2 + \log_2 42925 \rceil = \lceil 2 + \log_2 42925 \rceil = 2 + \lceil \log_2 42925 \rceil = 2 + 16 = 18$ bit.

Se invece si intendono le specifiche in maniera restrittiva e si impone che le località visitate siano differenti, il numero di possibili offerte speciali è dato dalle combinazioni semplici di 100 elementi (i viaggi possibili) su 3 posti (il numero di viaggi dell'offerta):

$$C(100,\,3) = \frac{100!}{97!\,3!} = \\ \frac{100 \cdot 99 \cdot 98}{3 \cdot 2} = 50 \cdot 33 \cdot 98 = \\ 2^2 \cdot 25 \cdot 33 \cdot 49 = 2^2 \cdot 40425$$

Poiché la prima potenza di 2 che supera 40425 è 2^{16}, per codificare le possibili offerte speciali serviranno anche in questo caso $\lceil \log_2(2^2 \cdot 40425) \rceil = \lceil \log_2 2^2 + \log_2 40425 \rceil = \lceil 2 + \log_2 40425 \rceil = 2 + \lceil \log_2 40425 \rceil = 2 + 16 = 18$ bit.

Esercizio 4

Sia data la seguente formula, F:

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

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:

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

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 lucida, smerigli, e viceversa):

a) sia Carlo, sia Bice lucidano;

b) Bice smeriglia se e solo se Antonio e Carlo lucidano;

c) Carlo non smeriglia, Bice o Antonio sì;

d) quando Antonio smeriglia, Bice e Carlo lucidano;

e) Antonio smeriglia solo se smeriglia anche Bice.

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio lucida
$\neg a$	Antonio smeriglia
b	Bice lucida
$\neg b$	Bice smeriglia
c	Carlo lucida
$\neg c$	Carlo smeriglia

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

a) $c \wedge b$

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

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

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

e) $\neg a \rightarrow \neg b$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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

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

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

Soluzione

a)

(1)	$\neg(b \rightarrow \neg a)$	Ip1
(2)	$\neg(\neg b \vee \neg a)$	Def. implicazione (1)
(3)	$b \wedge a$	Legge di De Morgan (2)
(4)	b	Elim. congiunzione (3)
(5)	$b \rightarrow c$	Ip2
(6)	c	Modus ponens (4) e (5)

b)

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

c)

(1)	$(a \rightarrow b) \leftrightarrow c$	Ip1
(2)	$((a \rightarrow b) \rightarrow c) \wedge (c \rightarrow (a \rightarrow b))$	Def. biimpl. (1)
(3)	$(a \rightarrow b) \rightarrow c$	Elim. cong. (2)
(4)	$\neg c$	Ip2
(5)	$\neg(a \rightarrow b)$	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)