

**Fondamenti di informatica per la sicurezza**

anno accademico 2004–2005

docente: Stefano FERRARI

Esempio — Prima parte — versione Avalutazioni **1** (4) _____ **2** (5) _____ **3** (5) _____ **4** (5) _____ **5** (4) _____ **6** (9) _____

Cognome _____

Nome _____

Matricola _____ Firma _____

Esercizio 1

Effettuare i seguenti cambi di base:

- a) $(237)_8 = (???)_{10}$
- b) $(258)_{10} = (???)_2$
- c) $(1C)_{16} = (???)_2$
- d) $(702)_8 = (???)_2$
- e) $(53)_7 = (???)_2$

Esercizio 2Dati $a = 13$, $b = -3$ e $n = 4$:

- a) calcolare la rappresentazione in complemento a 2 a n bit di a e b (indicate nel seguito con s_a e s_b), specificando se si verifica un overflow;
- b) calcolare la somma (in complemento a 2) delle stringhe binarie s_a e s_b , specificando se si verifica un overflow;
- c) calcolare la differenza (in complemento a 2) delle stringhe binarie s_a e s_b , specificando se si verifica un overflow.

Esercizio 3

Una azienda tessile produce lenzuola con le seguenti caratteristiche:

- colore: bianco, giallo, blu, verde, rosa, grigio, azzurro;
- larghezza: 80, 100, 120, 150 e 180 cm;
- lunghezza: 180, 190 e 200 cm;
- rifinitura: con elastici angolari e senza.

Inoltre, l'azienda propone un'offerta speciale per chi acquista 5 lenzuoli aventi la stessa misure.

Si calcoli:

- a) il numero di bit necessari per codificare ciascuna caratteristica (colore, larghezza, lunghezza, rifinitura);
- b) il numero di bit necessari per codificare un modello di lenzuolo;
- c) il numero di bit necessari per codificare le possibili offerte speciali.

Esercizio 4Dimostrare, tramite tavola di verità, **se** la seguente formula è una tautologia:

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

Esercizio 5

Formalizzare le seguenti proposizioni:

- a) Aldo ride e Bruno o Carlo balla;
- b) se Aldo ride, Bruno balla;
- c) Bruno balla;
- d) Carlo non balla e Aldo ride;
- e) Bruno non balla, Carlo sì.

Esercizio 6

Dimostrare, che le seguenti inferenze sono valide:

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

Tautologie

- $(a \wedge b) \rightarrow a$ (Eliminazione di congiunzione)
- $a \rightarrow (a \vee b)$ (Introduzione di disgiunzione)
- $\neg(a \leftrightarrow b) \leftrightarrow (\neg a \leftrightarrow b)$ (Negazione della biimplicazione)
- $(a \vee b) \wedge \neg b \rightarrow a$ (Sillogismo disgiuntivo)
- $\neg a \rightarrow (a \rightarrow b)$ (*Ex falso sequitur quodlibet*)
- $a \rightarrow (b \rightarrow a)$ (*Verum sequitur a quodlibet*)
- $a \vee \neg a$ (Terzo escluso)
- $\neg(a \wedge \neg a)$ (Non contraddizione)
- $((a \rightarrow b) \wedge (\neg a \rightarrow b)) \rightarrow b$ (Dimostrazione per casi)
- $(\neg b \rightarrow a \wedge \neg a) \rightarrow b$ (Dimostrazione per assurdo)
- (De Morgan)
 - $\neg(a \wedge b) \leftrightarrow (\neg a \vee \neg b)$
 - $\neg(a \vee b) \leftrightarrow (\neg a \wedge \neg b)$
- (Sillogismo ipotetico)
 - $((a \rightarrow b) \wedge (b \rightarrow c)) \rightarrow (a \rightarrow c)$
 - $(a \rightarrow b) \rightarrow ((b \rightarrow c) \rightarrow (a \rightarrow c))$
- $(a \rightarrow (b \wedge c)) \leftrightarrow ((a \rightarrow b) \wedge (a \rightarrow c))$ (Transitività dell'implicazione)
- $a \rightarrow b \leftrightarrow \neg b \rightarrow \neg a$ (Contrapposizione)
- $a \rightarrow (b \wedge c) \leftrightarrow (a \rightarrow b) \wedge (a \rightarrow c)$ (Distributività delle conseguenze)
- $(a \wedge b) \rightarrow c \leftrightarrow a \rightarrow (b \rightarrow c)$ (Esportazione/importazione delle premesse)
- $\neg\neg a \leftrightarrow a$ (Doppia negazione)
- $a \rightarrow (a \vee b)$ (Disgiunzione con vero)