Università degli Studi di Roma "La Sapienza"
Facoltà di Ingegneria – Corso di Laurea Specialistica in Ingegneria Informatica
Corso di Metodi Formali nell'Ingegneria del Software
Prof. Toni Mancini

Esercizio **E.III.20060718**

versione del 4 luglio 2007

Si considerino i seguenti requisiti:

> Uno pneumatico gonfio si può sgonfiare; se è sgonfio si può gonfiare. Quando si fora emette un sibilo e rimane forato.

1. Rappresentare i requisiti mediante un opportuno diagramma UML.
2. Rappresentare i requisiti in un linguaggio formale fra quelli considerati durante il corso.
3. Considerando la rappresentazione formale, quali deduzioni interessanti possono essere effettuate?
4. Quale strumento software fra quelli utilizzati nel corso utilizzereste per dimostrare tali deduzioni?
5. Per lo strumento software scelto, fornire il file di input e l'output atteso.

Una possibile soluzione è riportata nelle pagine seguenti.

Soluzione

1. UML: cfr. figura 1 (diagramma degli stati e delle transizioni).

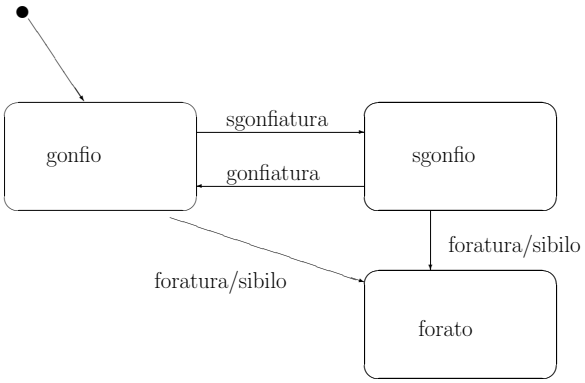

Figura 1: Diagramma UML per la domanda 1

2. Rappresentiamo i requisiti in logica temporale lineare (LTL):

$$
\begin{aligned}
& \text{// Uno pneumatico gonfio si può sgonfiare} \\
G \quad & ((stato = gonfio \ \wedge \ evento = sgonfiatura) \ \rightarrow \ X stato = sgonfio) \qquad (1) \\
& \text{// Se è sgonfio si può gonfiare} \\
G \quad & ((stato = sgonfio \ \wedge \ evento = gonfiatura) \ \rightarrow \ X stato = gonfio) \qquad (2) \\
& \text{// Quando si fora emette un sibilo} \\
& evento \ \neq \ foratura \, WX \ azione \ = \ sibilo \qquad (3) \\
& \text{// Quando si fora rimane forato} \\
& evento \ \neq \ foratura \, WXG \ stato \ = \ forato \qquad (4)
\end{aligned}
$$

3. Possiamo dimostrare che il diagramma UML degli stati e delle transizioni (punto 1) è coerente con la sua specifica formale (punto 2).

   Formalmente, detta Φ la congiunzione delle formule LTL di cui al punto 2 e $\mathcal{M}$ il sistema di transizioni ottenuto traducendo il diagramma del punto 1, vale la seguente relazione:

$$\mathcal{M} \models \Phi. \qquad (5)$$

4. Per dimostrare la deduzione di cui al punto 3 possiamo usare NUSMV, chiedendo che dimostri la relazione (5).

5. Il file nuSMV è il seguente:

```
-- Time-stamp: "2006-06-23 22:10:32 cadoli"
-- File: pneumatico.smv
-- Descrizione: diagramma UML S&T compito MFIS 06-07-18

MODULE pneumatico
-- rappresenta un diagramma degli stati e delle transizioni
VAR
-- descrive gli stati, gli eventi e le azioni
  stato : {gonfio, sgonfio, forato};
  evento: {gonfiatura, sgonfiatura, foratura, null};
  azione: {sibilo, null};
TRANS
-- descrive le transizioni
  case
    stato = gonfio & evento = sgonfiatura:
            next(stato) = sgonfio & next(azione) = null;
    stato = gonfio & evento = foratura:
            next(stato) = forato & next(azione) = sibilo;
    stato = sgonfio & evento = gonfiatura:
            next(stato) = gonfio & next(azione) = null;
    stato = sgonfio & evento = foratura:
            next(stato) = forato & next(azione) = sibilo;
-- per tutti i casi non contemplati dal diagramma S&T
    1:      next(stato) = stato & next(azione) = null;
  esac
-- fine MODULE pneumatico

MODULE main
VAR
-- un cliente dell'oggetto "pneumatico"
  p: pneumatico;
ASSIGN
-- assegna lo stato iniziale a p
  init(p.stato) := gonfio;
-- fine MODULE main

LTLSPEC
-- Uno pneumatico gonfio si può sgonfiare
--    G((p.stato = gonfio & p.evento = sgonfiatura) -> X p.stato = sgonfio)
-- Se è sgonfio si può gonfiare
--    G((p.stato = sgonfio & p.evento = gonfiatura) -> X p.stato = gonfio)
-- Quando si fora emette un sibilo
--    (p.evento != foratura U X p.azione = sibilo) | G p.evento != foratura
```

```
-- Quando si fora rimane forato
    (p.evento != foratura U X G p.stato = forato) | G p.evento != foratura
```

Ci si aspetta che nuSMV dimostri la verità delle formule LTL.

Infatti, l'output di nuSMV (ad esempio, per la (4)) comprende:

```
-- specification
((p.evento != foratura U  X  G p.stato = forato) |  G p.evento != foratura)
   is true
```