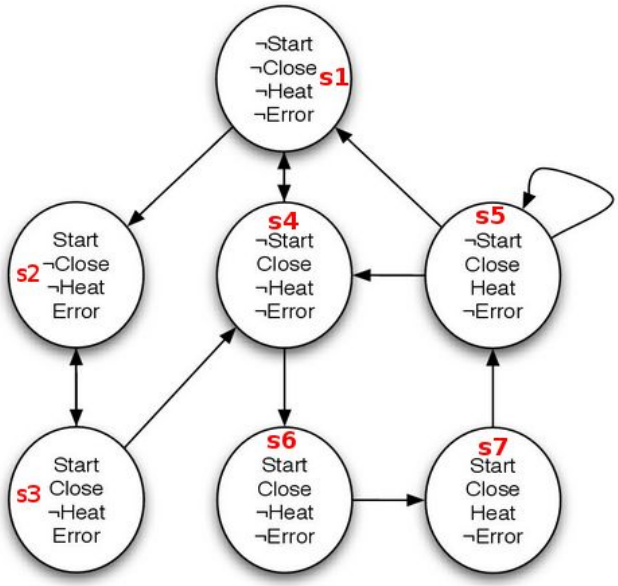
SSC5793 - Especificação formal de software
Trabalho 01

Instrutor: Prof. Dr. Adenilso Simão (adenilso@icmc.usp.br)

Alunos: Carlos Damasceno (damascenodiego@usp.br) / Stevão Andrade (stevao@icmc.usp.br)

Data: 10 Outubro 2015

Para o Trabalho 01 foi solicitado que fosse verificado se um conjunto de propriedades em CTL é verdadeiro dada uma máquina de transição de estados para um microondas. Se alguma propriedades for falsa, sugerir uma **modificação** na máquina de estados que mantenha a ideia da máquina, mas que ao mesmo tempo faça a propriedade ser verdadeira. Além disso, também foi solicitada uma descrição em linguagem natural para cada propriedade fornecida. A seguir podem ser vistas a máquina de estados para um microondas e as propriedades.



- AG(Start => AF Heat)
- A[!Heat U Close]
- AG(Error => AF !Error)

Figura 1: Máquina de Estados para um microondas e propriedades a serem verificadas

Para testar as propriedades CTL, foi criado um modelo[1] em NuSMV correspondente à representação da maquina de estados do microondas apresentado a seguir. O plugin para Eclipse NuSeen[2] foi usado para auxiliar o desenvolvimento do modelo e a versão NuSMV-zchaff-2.5.4 para linux x86_64.

```
1 MODULE main
2 VAR
3     state : {s1, s2, s3, s4, s5,s6,s7};
4 ASSIGN
5
6     next(state) :=
7
8         case
9
10            state = s1 : {s2, s4};
11            state = s2 : s3;
12            state = s3 : {s2, s4};
13            state = s4 : {s1, s6};
14            state = s5 : {s1, s4, s5};
15            state = s6 : s7;
16            state = s7 : s5;
17
18        esac;
19
20 DEFINE
21
22 start  := (state = s2) | (state = s3) | (state = s6) | (state = s7);
23 closed := (state = s3) | (state = s4) | (state = s5) | (state = s6) |
   (state = s7);
24 heat   := (state = s5) | (state = s7);
25 error  := (state = s2) | (state = s3);
```

Figura 2: Modelo CTL para a ferramenta NuSMV do trabalho 1

[1] Os artefatos gerados nesse trabalho encontram-se disponíveis em https://github.com/damascenodiego/formalSpecification_usp_2015/tree/master/efs_trabalho01_nuSMV
[2] NuSeen: an eclipse-based environment for the NuSMV model checker: https://marketplace.eclipse.org/content/nuseen

Verificação das Propriedades CTL

Para cada propriedade CTL definida, foram obtidas a seguinte saida:

Propriedade 1: `AG( Start => AF Heat )`

- Descrição em LN:
  - SEMPRE QUE A PROPRIEDADE 'START' DO MICROONDAS FOR VALIDA, EM ALGUM MOMENTO NO FUTURO ELE PODERÁ AQUECER (HEAT).
- Propriedade convertida:
  - `!EF !( !start | ! EG !heat)`
- Saida NuSMV: **FALSE**

Propriedade 2: `A[!Heat U Close]`

- Descrição em LN:
  - O MICROONDAS SEMPRE NÃO AQUECERÁ (! HEAT) ATÉ QUE ESTEJA FECHADO (CLOSE).
- Propriedade convertida:
  - `!(E [(!closed) U (!(!heat | closed))] | (EG (!closed)))`
- Saida NuSMV: **TRUE**

Propriedade 3: `AG( Error => AF !Error )`

- Descrição em LN:
  - SEMPRE QUE HOUVER UM ERRO (ERROR), ENTÃO EM ALGUM MOMENTO NO FUTURO O ERRO DEIXARÁ DE EXISTIR (! ERROR)
- Propriedade convertida:
  - `!EF !(!error | !EG(error))`
- Saida NuSMV: **FALSE**

Sugerindo correções para as Propriedades 1 e 3.

Após verificar as propriedades utilizando NuSMV, notou-se que a **Propriedade 1** e **Propriedade 3** eram falsas. Conforme pedido no trabalho, foram então propostas modificações na maquina de estados do microondas para que as propriedades se torna-sem verdadeiras. A nova maquina de estados correspondente ao microondas pode ser visualizada na figura a seguir:

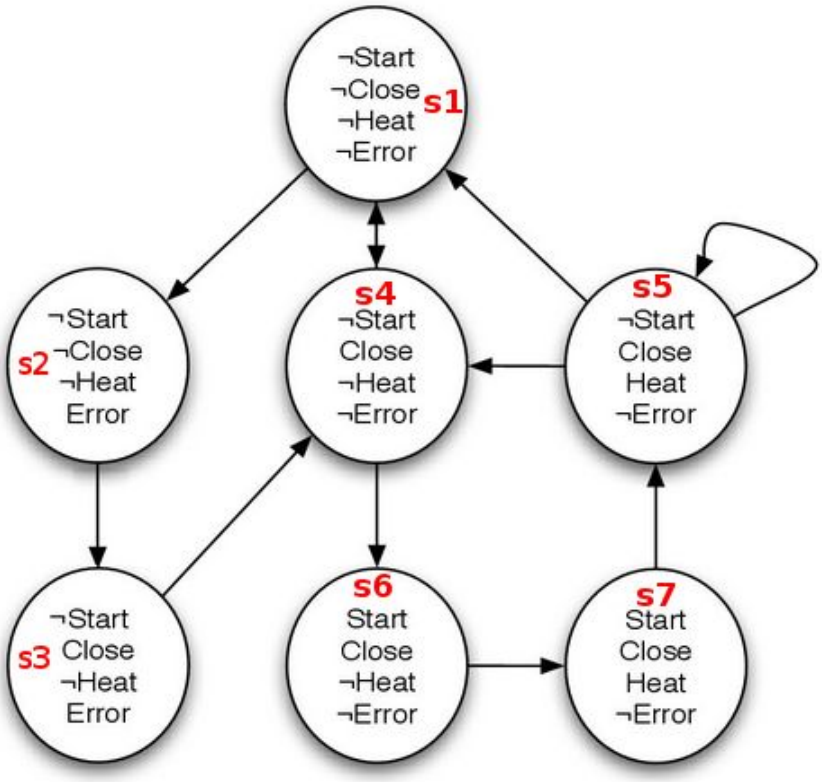


Figura 3: Máquina de Estados para um microondas (Versão modificada)

Para solucionar o problema das propriedades foram tomadas as seguintes medidas:

Propriedade 1: `AG( Start => AF Heat )`

Remover a transição do estado S3 -> S2 corrige o problema da **Propriedade 1**.

Propriedade 3: `AG( Error => AF !Error )`

Remover a propriedade START dos estados S2 e S3 resolve o problema da **Propriedade 3**.

Estas alterações fazem com que a maquina se torne consistente para as 3 propriedades que foram propostas. No fim, temos então a nova implementação em NuSVM:

```
 1 MODULE main
 2 VAR
 3     state : {s1, s2, s3, s4, s5,s6,s7};
 4 ASSIGN
 5
 6     next(state) :=
 7
 8         case
 9
10             state = s1 : {s2, s4};
11             state = s2 : s3;
12             state = s3 : {s4};
13             state = s4 : {s1, s6};
14             state = s5 : {s1, s4, s5};
15             state = s6 : s7;
16             state = s7 : s5;
17
18         esac;
19
20 DEFINE
21
22 start  := (state = s6) | (state = s7);
23 closed := (state = s3) | (state = s4) | (state = s5) | (state = s6) |
   (state = s7);
24 heat   := (state = s5) | (state = s7);
25 error  := (state = s2) | (state = s3);
```

Figura 4: Modelo CTL para a ferramenta NuSMV do trabalho 1 (Versão modificada)

Sugerindo novas Propriedades CTL

Foram solicitadas três novas propriedades que pudessem ser testadas no modelo, expressadas em CTL, além da sua correspondente tradução para linguagem natural.

Propriedade 1: `!AG(start & closed & heat & error)`

- Descrição em LN:
    - Não existe um caminho global em que as propriedades start, closed, heat e error sejam validas
- Saida NuSMV: **TRUE**

Propriedade 2: `EF(E[error U (closed & heat)])`

- Descrição em LN:
    - No futuro existe um caminho que a propriedade error será valida até que as propriedades closed e heat sejam validas.
- Saida NuSMV: **TRUE**

Propriedade 3: `AG(heat -> EF!heat)`

- Descrição em LN:
    - Para todos os caminhos, se o microondas esquenta (heat), então existe um caminho no futuro em que ele não irá esquentar (!heat)
- Saida NuSMV: **TRUE**