
Vérification en XTL du système SCSI-2

Radu Mateescu

INRIA Rhône-Alpes / VASY



Plan

- Description du système d'entrées-sorties SCSI-2
- Présentation (succincte) du langage XTL
- Vérification des propriétés de sûreté du SCSI-2
- Vérification des propriétés de vivacité du SCSI-2

Le langage XTL

Formules sur actions

$$\alpha ::= G O_1 \dots O_n \text{ [where } E]$$
$$| \text{ true } | \text{ false } | \neg \alpha | \alpha \wedge \alpha | \alpha \vee \alpha$$

Exemple :

(RECV ?m:Msg ?c:Nat where c = checksum (m))

or

(RECV ?m:Msg !no_checksum)

Le langage XTL (suite)

Expressions régulières

$$R ::= \alpha$$
$$| \text{nil} \mid R.R \mid R|R \mid R^* \mid R^+$$

Exemple :

```
(REQUEST ?s:Addr) .  
  i* .  
  (INDICATION !s) .  
    i* .  
    (RESPONSE ?d:Addr) .  
      i* .  
      (CONFIRM !d)
```

Le langage XTL (suite)

Formules sur états

$\varphi ::= E$

| true | false | $\neg\varphi$ | $\varphi \wedge \varphi$ | $\varphi \vee \varphi$

| $\langle R \rangle \varphi$ | $[R] \varphi$

| $\mu Y(x:T:=E).\varphi$ | $\nu Y(x:T:=E).\varphi$ | $Y(E)$

| exists $x:T . \varphi$ | forall $x:T . \varphi$

| let...endlet

| if...endif

| case...endcase

Notations

Constantes :

N_{min} : numéro minimal de périphérique

N_{max} : numéro maximal de périphérique

NC : numéro du contrôleur

Prédicats sur actions :

$NARB$: action ARB !**false**...!**false** (personne ne demande le bus)

$ARB(i)$: action ARB ...!**true**!**false**...!**false** (le périphérique i gagne le bus)

Propriétés de sûreté

“rien de mal n’arrivera”

Propriétés de sûreté du SCSI-2 :

- absence d’actions indésirables
- accès des périphériques au bus
- précedence des actions par des accès au bus
- séquençement des commandes et des reconnections
- séquençement des accès au bus
- répétitions bornées des actions

Propriétés de sûreté (suite)

Absence d'actions indésirables

S.1. *le contrôleur ne peut pas envoyer des messages CMD !NC et les disques ne peuvent pas envoyer des messages REC !NC :*

$[\text{true}^* \cdot (\text{CMD !NC or REC !NC})] \text{ false}$

Accès des périphériques au bus

S.2. *après un message CMD ou REC, il est impossible d'atteindre un autre CMD ou REC sans faire un ARB entre temps :*

$[\text{true}^* \cdot (\text{CMD any or REC any}) \cdot (\text{not ARB any})^* \cdot (\text{CMD any or REC any})] \text{ false}$

Propriétés de sûreté (suite)

Précédence des actions par des accès au bus

S.4. *chaque message* **CMD !i** doit être précédé par une action **ARB !NC** :

$[(\mathbf{nil} \mid (\mathbf{true}^* \cdot \mathbf{CMD} \mathbf{any})) \cdot (\mathbf{not} \mathbf{ARB} \mathbf{!NC})^* \cdot \mathbf{CMD} \mathbf{any}] \mathbf{false}$

S.5. *chaque message* **REC !i** doit être précédé par une action **ARB !i** :

forall $i < N_{max}$.

$[(\mathbf{nil} \mid (\mathbf{true}^* \cdot \mathbf{REC} \mathbf{any})) \cdot (\mathbf{not} \mathbf{ARB} \mathbf{!i})^* \cdot \mathbf{REC} \mathbf{!i}] \mathbf{false}$

Propriétés de sûreté (suite)

Séquence des commandes et des reconnections

S.3. *après chaque CMD !j, il est impossible d'atteindre un REC !i avec i < j avant d'effectuer REC !j :*

$$[\text{true}^* \cdot \text{CMD } ?j \cdot (\text{not REC } !j)^* \cdot (\text{REC } ?i \text{ where } i < j)] \text{ false}$$

S.7. *après chaque séquence CMD !i, CMD !j avec j < i, il est impossible qu'un REC !j soit émis avant un REC !i :*

$$[\text{true}^* \cdot \text{CMD } ?i \cdot (\text{not REC } !i)^* \cdot (\text{CMD } ?j \text{ where } j < i) \cdot (\text{not REC } !i)^* \cdot \text{REC } !j] \text{ false}$$

Propriétés de sûreté (suite)

Séquence des accès au bus

S.6. *si deux ARB se succèdent immédiatement, alors le premier est forcément un NARB :*

$[\text{true}^* \cdot (\text{not NARB}) \cdot (\text{not (CMD any or REC any)})^* \cdot \text{ARB any}] \text{ false}$

S.8. *après chaque REC i avec $i < NC$, il est impossible d'effectuer un ARB(i) avant le prochain CMD i :*

$[\text{true}^* \cdot \text{REC } ?i \text{ where } i < NC \cdot (\text{not CMD } !i)^* \cdot \text{ARB } !i \cdot (\text{not CMD } !i)^* \cdot \text{CMD } !i] \text{ false}$

Propriétés de sûreté (suite)

Répétitions bornées des actions

S.9. *sur chaque chemin et pour tout $i \neq NC$,*

$$0 \leq \#ARB(i) - \#REC \ !i \leq 1 :$$

forall $i \neq NC$.

nu $X(d:=0)$.

if $d \geq 0$ **and** $d \leq 1$ **then**

$[ARB(i)] X(d+1)$ **and**

$[REC \ !i] X(d-1)$ **and**

$[not (ARB(i) or REC \ !i)] X(d)$

else

false

endif

Propriétés de sûreté (suite)

Répétitions bornées des actions (suite)

S.10. *sur chaque chemin et pour tout $i \neq NC$,*

$$0 \leq \#ARB(NC) - \#CMD \ !i \leq 1 :$$

forall $i \neq NC$.

nu $X(d:=0)$.

if $d \geq 0$ **and** $d \leq 1$ **then**

$[ARB(NC)] X(d+1)$ **and**

$[CMD \ !i] X(d-1)$ **and**

$[not (ARB(NC) or CMD \ !i)] X(d)$

else

false

endif

Propriétés de sûreté (suite)

Répétitions bornées des actions (suite)

S.11. *sur chaque chemin et pour tout i , $0 \leq \# \text{CMD } !i - \# \text{REC } !i \leq 8$ (= la taille des files d'attente) :*

```
forall  $i$  .  
  nu  $X(d:=0)$  .  
    if  $d \geq 0$  and  $d \leq 8$  then  
      [CMD  $!i$ ]  $X(d+1)$  and  
      [REC  $!i$ ]  $X(d-1)$  and  
      [not (CMD  $!i$  or REC  $!i$ )]  $X(d)$   
    else  
      false  
    endif
```

Propriétés de vivacité

“quelque chose de bien arrivera”

Propriétés de vivacité du SCSI-2 :

- absence de blocage
- accès des périphériques au bus
- réponses aux actions
- séquençement des actions au démarrage du système

Propriétés de vivacité (suite)

Absence de blocage (L.1.)

$\text{nu } X . (\langle \text{true} \rangle \text{ true and } [\text{true}] X)$

Accès des périphériques au bus

L.2. *après chaque message $\text{CMD } !i$ avec $i > N_{min}$, il y aura inévitablement un $\text{ARB}(i)$:*

$[\text{true}^* . \text{CMD } !i \text{ where } i > N_{min}]$

$\text{mu } X . (\langle \text{true} \rangle \text{ true and } [\text{not } \text{ARB}(i)] X)$

Propriétés de vivacité (suite)

Accès des périphériques au bus (suite)

L.3. *si* $NC > N_{min}$, *après chaque* $CMD !N_{min}$, *le disque* N_{min} *est menacé de famine :*

```
if  $NC > N_{min}$  then
  [true* .  $CMD !N_{min}$ ] nu  $X$  .  $\langle$ not  $ARB(N_{min})$  $\rangle X$ 
else
  false
endif
```

L.4. *chaque périphérique* i *accède équitabement au bus par une action* $ARB(i)$:

```
forall  $i$  . [true* . (not  $ARB(i)$ )*]  $\langle$ (not  $ARB(i)$ )* .  $ARB(i)$  $\rangle$  true
```

Propriétés de vivacité (suite)

Réponses aux actions

L.5. *chaque* $ARB(NC)$ est immédiatement suivi par un CMD :

$$[true^* . ARB(NC)] \langle CMD \text{ any} \rangle true$$

L.6. *chaque* $ARB(i)$ est immédiatement suivi par un $REC !i$:

$$forall\ i . [true^* . ARB(i)] \langle REC !i \rangle true$$

L.7. *chaque* $NARB$ est suivi par un ARB sans qu'un CMD ou REC soit émis entre temps :

$$[true^* . NARB]$$
$$mu\ X . (\langle true \rangle true \text{ and } [CMD \text{ any or } REC \text{ any}] false \text{ and } [not\ ARB \text{ any}] X)$$

Propriétés de vivacité (suite)

Séquencement des actions au démarrage du système

L.8. *initialement, un ARB(NC) est toujours équitablement atteint avant aucun CMD ou REC :*

$$\begin{aligned} & [(\text{not } (\text{ARB}(NC) \text{ or } \text{CMD any or REC any}))^*] \\ & \langle (\text{not } (\text{ARB}(NC) \text{ or } \text{CMD any or REC any}))^* \cdot \text{ARB}(NC) \rangle \text{ true} \end{aligned}$$