T-79.231 **Autumn 2002**
Parallel and distributed digital systems
Answers to Tutorial 7
Nov 4th, 2002

1. Let us create the incidence matrix of the net (the columns indicate the changes in the place markings by transitions are)

$$C = \begin{pmatrix} -1 & 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

The vector representation of the column ι is an invariant iff $C^T \cdot \iota = 0$, where 0 is a [column] vector.

a) Our task is to prove the following with invariants: $M(p_4) \leq 2$.
Let us make the guess that one of the invariants is $\iota = M(p_2) + M(p_4)$. Hence, we obtain the ι vector, where the multipliers for both places are 1. Let us check that our vector really is an invariant:

$$C^T \cdot \iota = \begin{pmatrix} -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 1 & 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

So $\iota = M(p_2) + M(p_4)$ really is an invariant. Then we will compute, using the initial marking M_0, the value of the invariant.

$$\iota^T \cdot M_0 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 2$$

The result was $M(p_2) + M(p_4) = 2 \Rightarrow M(p_4) \leq 2$, which means that at most 2 processors can access the memory concurrently.

b) First we will prove that $\iota = M(p_1) + M(p_3) + M(p_4) + M(p_5)$ is an invariant. Let us check it:

$$C^T \cdot \iota = \begin{pmatrix} -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 1 & 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

As the next step we will compute the value of the invariant, again basing on the initial marking:

$$\iota^T \cdot M_0 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 5$$

Hence we have proved the following formula to be the invariant: $M(p_1) + M(p_3) + M(p_4) + M(p_5) = 5$.

2. A Maria description of the TicketME algorithm:

```
typedef unsigned (0..2) owner_t;
typedef owner_t (1..) client_t;
typedef struct {
  client_t next;
  client_t granted;
} turn_t;
typedef struct {
  client_t client;
  owner_t owner;
} ticket_t;
place idle (0..#client_t) client_t: client_t client: client;
place pending (0..#client_t) client_t;
place testing (0..#client_t) client_t;
place critical (0..1) client_t;
place turn (1) turn_t: <turn_t;
place tickets (#client_t) ticket_t: client_t client: { client, 0 };

trans try
in { place idle: client; }
out { place pending: client; };

trans enter
in {
  place pending: client;
  place turn: { next, granted };
  place tickets: { client, t };
}
out {
  place testing: (next != granted)#client;
  place critical: (next == granted)#client;
  place turn: { +next, granted };
  place tickets: { client, next };
};

trans test
in {
  place testing: client;
  place turn: { next, granted };
  place tickets: { client, t };
}
out {
  place testing: (t == 0 || is client_t t != granted)#client;
  place critical: (t > 0 && is client_t t == granted)#client;
  place turn: { next, granted };
  place tickets: { client, t };
};

trans exit
in {
  place critical: client;
  place turn: { next, granted };
  place tickets: { client, t };
}
out {
  place idle: client;
  place turn: { next, +granted };
  place tickets: { client, 0 };
};
```

(a) Let the above Maria description be in the file `ticket.pn`. Let us present:

- The property as an LTL formula,
- The property as a Maria LTL formula,
- Is the property valid?
- An example of a model checking run.

- Two processes are never in the critical section concurrently:

$$\Box\neg(\text{critical}(1) \wedge \text{critical}(2))$$

```
reject (client_t c && (c subset place critical)) && fatal;
```

The property holds.

```
state 1 /lhome/jhonkola $tail -1 ticket.pn
reject (client_t c && (c subset place critical)) && fatal;
state 2 /lhome/jhonkola $maria -b ticket.pn
"ticket.pn": 32 states (3..3 bytes), 64 arcs
@0$exit$
```

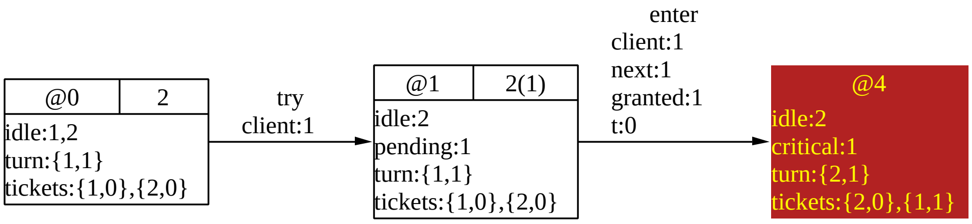
- The process 1 never makes it to the critical section:

$$\Box\neg\text{critical}(1)$$

```
reject (1 subset place critical) && fatal;
```

The property does not hold.

```
state 1 /lhome/jhonkola $tail -1 ticket.pn
reject (1 subset place critical) && fatal;
state 2 /lhome/jhonkola $maria -b ticket.pn
fatally rejected state @4
"ticket.pn": 5 states (3..3 bytes), 4 arcs
@0$visual path @4 @0$
```

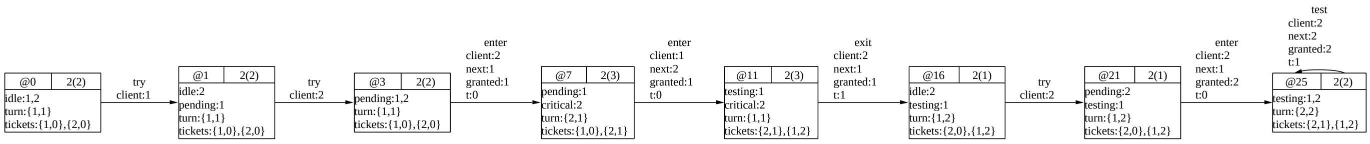


- If the process 1 wants access to the critical section, it will eventually make it there:

$$\Box(\text{pending}(1) \implies \Diamond\text{critical}(1))$$

```
[]((1 subset place pending) => <> (1 subset place critical))
```

The property does not hold in the model. Maria gives a counter example where the process 2 is continuously firing the transition `test` and the process 1 cannot make any progress.

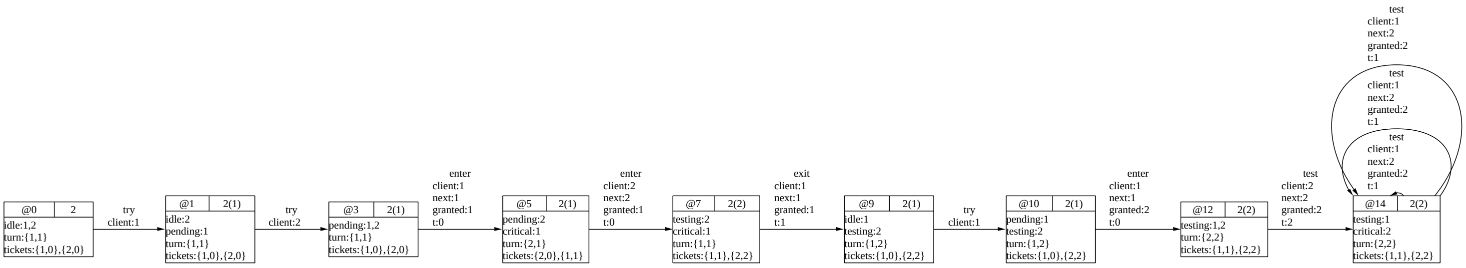


- If the process 2 is in the critical section, it will eventually leave the critical section:

$$\neg(\Diamond\Box\text{critical}(2))$$

```
!(<>[](2 subset place critical))
```

The property does not hold. Maria gives a counter example where the process 2 is in the critical section and the process 1 is continuously firing the transition `test`.



Next we will add the fairness assumptions to the model. The necessary fairness sets will be the following:

- One weak fairness set for all the instances of transition `exit`
- One weak fairness set for each possible value of variable `client` in transitions `enter` or `test`.

The fairness sets can be defined as follows:

```
weakly_fair trans exit;
weakly_fair client_t c: (trans enter: c == is client_t client)
  || (trans test: c == is client_t client);
```

Now we will be able to do the model checking of our formulas w.r.t. the fairness assumption:

- If the process 1 wants access to the critical section , it will eventually make it there:

$$\Box(\text{pending}(1) \implies \Diamond\text{critical}(1))$$

```
[]((1 subset place pending) => <> (1 subset place critical))
```

The property holds with the fairness assumptions:

```
state 1 /lhome/jhonkola $maria/maria -m ticket.pn
@0$translator "lbt/lbt-1.2.1/lbt"
@0$visual []((1 subset place pending) => <> (1 subset place critical))
(command line):2:property holds
"ticket.pn": 32 states (3..3 bytes), 64 arcs
@0$exit
state 2 /lhome/jhonkola $
```