Verification of Cyber-Physical System
Fall 2017

Exercice Sheet 4

Author : Sylvain Julmy

Professor : Ultes-Nitsche Ulrich
Assistant : Prisca Dotti

Exercice 1

Using the *spin* command line interface, we can automatically create a never claim from the *LTL* formula $\Diamond\Box q$. Because it is a never claim and we have to check that q satisfies the system behavior, we have to create the never claim with $\neg(\Diamond\Box q)$:

`spin -f '!(<>[]q)'`

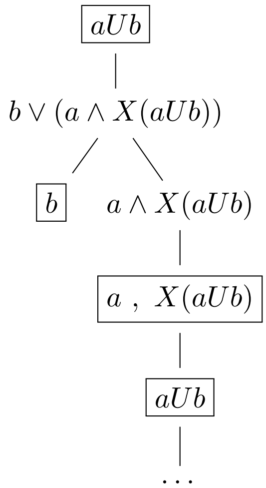
which give us the following never claim :

```
never {    /* !(<>[]q) */
T0_init:
  do
  :: (! ((q))) -> goto accept_S9
  :: (1) -> goto T0_init
  od;
accept_S9:
  do
  :: (1) -> goto T0_init
  od;
}
```

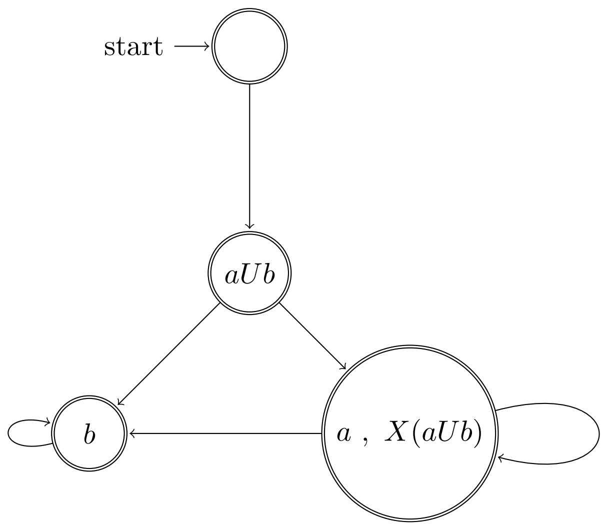
Exercice 2

(1)

Algorithmic sugar :



Automaton construction :



(2)

First, we transform

$$\Box\Diamond a$$

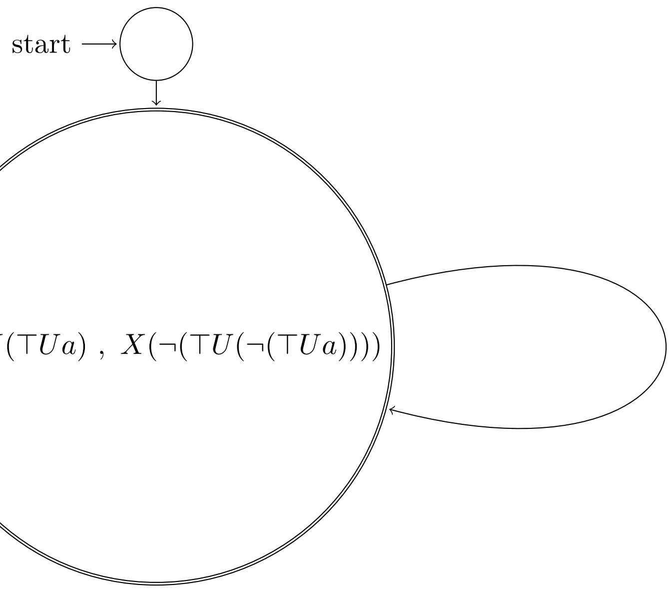
into

$$\begin{aligned}\Box\Diamond a &\equiv \neg\Diamond\neg(\Diamond a)\\ &\equiv \neg(\top U(\neg(\Diamond a)))\\ &\equiv \neg(\top U(\neg(\top U a)))\end{aligned}$$

Algorithmic sugar (note : we simplify formulae like $\top \wedge a \equiv a$ and $\bot \vee a \equiv a$) :

$$\neg(\top U(\neg(\top U a)))$$
$$|$$
$$\neg(\neg\top U a) \wedge (\neg\top \vee \neg X(\top U(\neg(\top U a))))$$
$$|$$
$$\neg(\neg\top U a)\ ,\ (\neg\top \vee \neg X(\top U(\neg(\top U a))))$$
$$|$$
$$\top U a\ ,\ \bot \vee \neg X(\top U(\neg(\top U a)))$$
$$|$$
$$a \wedge (\top \wedge X(\top U a))\ ,\ \bot \vee \neg X(\top U(\neg(\top U a)))$$
$$|$$
$$a\ ,\ X(\top U a)\ ,\ \neg X(\top U(\neg(\top U a)))$$
$$|$$
$$\boxed{a\ ,\ X(\top U a)\ ,\ X(\neg(\top U(\neg(\top U a))))}$$
$$|$$
$$\top U a\ ,\ \neg(\top U(\neg(\top U a)))$$
$$|$$
$$\ldots$$

Automaton construction :



Exercice 3

We denote (ϕ, λ) a moment in the timeline where ϕ represent p and λ represent q (for example, $s_i = (\top, \bot)$ means that p is true and q is false at moment i), where $S = (s_0, s_1, \cdots, s_n, \cdots)$

(1)

$\Box p \vee q \not\leftrightarrow \Box(p \vee q)$, because of the following timeline :

$$((\top, \bot), (\bot, \top), (\top, \bot), \cdots, (\top, \bot), (\bot, \top), (\top, \bot), (\bot, \top), \cdots)$$

$\Box p \vee q$ is false at s_0 and $\Box(p \vee q)$ is always true.

(2)

$\Diamond p \vee \Diamond q \leftrightarrow \Diamond(p \vee q)$ because it is just the distributivity law of $\Diamond$: $\Diamond(p \vee q) \equiv \Diamond p \vee \Diamond q$.

(3)

$\Diamond(pUq) \leftrightarrow \Diamond q$, because we don't care about p, if $\Diamond(pUq)$ holds at a certain moment, it means that q will holds at a certain moment, which is $\Diamond q$.