Justin Mang 556002335 – Mutual Exclusion - Assignment 3 - CMPT 477 Summer 2018

Assumptions About the Environment:

1. A waitlist must empty before taking on a new process.
2. Waitlist 1 empties when its process can enter its critical state.
3. Waitlisted processes can only move up, via FIFO stack.
4. An empty waitlist can remain empty if no process is in a trying state.
5. A process will not remain in its critical section infinitely.
6. A process will attempt to enter its critical state.

Modelling Decisions:

A process that is trying will eventually become critical

```
SPEC

AG (pr1.st = t) -> AF(pr1.st = c)

SPEC

AG (pr2.st = t) -> AF(pr2.st = c)

SPEC

AG (pr3.st = t) -> AF(pr3.st = c)
```

A process that is in non-critical will eventually try

```
SPEC

AG ((pr1.st = n) -> EX(pr1.st = t))

SPEC

AG ((pr2.st = n) -> EX(pr2.st = t))

SPEC

AG ((pr3.st = n) -> EX(pr3.st = t))
```

Only one process can be in its critical section at a time

```
SPEC

AG !((pr1.st = c) & AF(pr2.st = c))

SPEC

AG !((pr1.st = c) & AF(pr3.st = c))

SPEC

AG !((pr2.st = c) & AF(pr3.st = c))
```

A process will eventually try

```
SPEC

EF (pr1.st=t)

SPEC

EF (pr2.st=t)

SPEC

EF (pr3.st=t)
```

A process will eventually become critical

```
SPEC

EF (pr1.st=c)

SPEC

EF (pr2.st=c)

SPEC

EF (pr3.st=c)
```

Additional Properties:

A waitlist cannot hold identical processes

```
SPEC

AG ((Wait_List1 = Wait_List2) | (Wait_List1 = Wait_List3)) -> (Wait_List1 = 0)

SPEC

AG ((Wait_List2 = Wait_List1) | (Wait_List2 = Wait_List3)) -> (Wait_List2 = 0)

SPEC

AG ((Wait_List3 = Wait_List1) | (Wait_List3 = Wait_List2)) -> (Wait_List3 = 0)
```

Verification Time for Properties:

< 0.5 seconds