

Homework 2

Tarek Abdel Sater – tga15

Problem: Fixing the mutex liveness model.

The objective is to fix the model in such a way that it satisfies both **liveness**, and **safety**.

Safety means that no two processes are in the critical section simultaneously.

This is represented by the formula: $AG(\neg (C1 \ \& \ C2))$.

Liveness means that, at any time a process tries to go into the critical section, it will eventually enter it.

This is represented by the formula: $(AG(T1 \Rightarrow (AF(C1)))) \ \& \ (AG(T2 \Rightarrow (AF(C2))))$.

And the additional condition $(EG(N1) \ \& \ EG(N2))$.

To satisfy safety, we simply make sure that there exists no state where C1 and C2 both hold.

To satisfy liveness, we need to repair the model in such a way that C1 will eventually occur in all paths from states where T1 holds. The same goes for C2 and T2.

Problems arise whenever we have a state where only both T1 and T2 hold. In that case, it is difficult to satisfy liveness without the use of “black” transitions, i.e. illegal transitions where both processes transition to a single state at the same time.

To solve this, we use the F1 and F2 values to control the transitions in such a way that we ‘synchronize’ the two processes. For example, whenever F1 and T1 holds, check if T2 holds. If no, proceed to C1. If yes, concede the execution path to C2.

To satisfy $EG(N1) \ \& \ EG(N2)$, we simply make sure that all paths lead back to the neutral (start) state.