HW0

Problem 1

A

Yes, Q is an inductive invariant of A.

The definition of inductive invariant is: If $Q_0 \subseteq I$ and $Post(I) \subseteq I$ then I is an invariant, i.e., $Reach_A \subseteq I$. Such invariants are called inductive invariants.

$Q_0 \subseteq Q$ and $Post(Q) \subseteq Q$ are true, so Q is an inductive invariant of A.

B

For I to be an inductive invariant of A, $Q_0 \subseteq I$ and $Post(I) \subseteq I$ must be true.

To help prove safety, I should not intersect with the unsafe set U.

Problem 1

Yes, $0 \leq v_1(t) \leq v_0$ is an invariant of A.

The vehicle starts with a speed of v_0 and can only decelerate or maintain its speed. Thus, the speed of the vehicle will always be between 0 and v_0.

Problem 2

Yes, $timer(t) \leq v_0/a_b$ is an invariant of A.

The $timer(t)$ represents how long the vehicle has been braking. So, we have $timer(t) = (v_0 - v_1(t))/a_b$. According to the invariant $0 \leq v_1(t) \leq v_0$ and induction, we have $timer(t) \leq (v_0 - 0)/a_b = v_0/a_b$.

Problem 3

```
SimpleCar(Dsense, v0, x10, x20, ab), x20 > x10
Initially: x1(0) = x10, x2(0) = x20, v1(0) = v0, v2(0) = 0
s(0) = 0, timer(0) = 0, timer2(0) = 0, aware(0) = 0
d(t) = x2(t) - x1(t)
if d(t)   Dsense
    s(t + 1) = 1
    aware(t + 1) = aware(t) + 1
    if aware(t + 1) >= Treact
        if v1(t)   ab
            v1(t + 1) = v1(t) - ab
            timer(t + 1) = timer(t) + 1
            timer2(t + 1) = timer2(t)
```

```
        else
            v1(t + 1) = 0
            timer(t + 1) = timer(t)
            timer2(t + 1) = timer2(t)
    else
        v1(t + 1) = v1(t) + as
        timer(t + 1) = timer(t)
        timer2(t + 1) = timer2(t) + 1
else
    s(t + 1) = 0
    v1(t + 1) = v1(t) + as
    timer(t + 1) = timer(t)
    timer2(t + 1) = timer2(t) + 1
x1(t + 1) = x1(t) + v1(t + 1)
```

Problem 4