LFCPS Exercise Class 4
Differential Invariants

Exercise 1. Prove the following formulas using differential invariants, differential cuts, and differential weakening as required:

1. \( \omega \geq 0 \land x = 0 \land y = 3 \rightarrow \{x' = y, y' = -\omega^2 x - 2\omega y\}\omega^2 x^2 + y^2 \leq 9 \)
2. \( xy^2 + x \geq 7 \rightarrow \{x' = -2xy, y' = 1 + y^2\}\)xy^2 + x \geq 7
3. \( x \geq 2 \land y = 1 \rightarrow \{x' = x^2 y + x^4, y' = 1 + y^2\}\)x^2 + y \geq 1
4. \( x \geq 2 \land y \geq 2 \land z = 1 \rightarrow \{x' = x^2 z + x^4, y' = y^2 + y^4 z, z' = z^2 + 1\}\)x^2 + y \geq 1 \land y \geq 1
5. \( x^2 + y^2 = 0 \rightarrow \{x' = 4y^3, y' = -4x^3\}\)x^2 + y^2 = 0

Exercise 2. Simplify the following formulas using the rules for the differential operator:

1. \( (v^2 + w^2 < r^2 \land v \leq 0) \lor v = 0 \)’
2. \( (x^2 + 2x < 0 \lor (x \neq 0 \land x > 1)) \)’

Exercise 3. Prove that the following dL formula is a sound axiom:

\[ [x' = f(x)](e) = 0 \rightarrow ([x' = f(x)]e = 0 \leftrightarrow e = 0). \]

Exercise 4. Prove or disprove the following proof rule:

\[
\frac{F \land Q \vdash [x' := f(x)](F)' \quad F \vdash [x' = f(x) \& Q][F]'}{F \vdash [x' = f(x) \& Q][F]'}
\]

Exercise 5. Is the following dL formula a sound axiom?

\[ (Q \rightarrow [x' = f(x) \& Q](e = 0))' \rightarrow ([x' = f(x) \& Q]e = 0 \leftrightarrow e = 0) \]

Note: In this exercise class, I wrongly claimed that

\[ (1 = 0 \rightarrow [x' = 0 \& 1 = 0](1 = 0))' \rightarrow ([x' = 0 \& 1 = 0](1 = 0) \leftrightarrow 0 = 0) \]

is a counter example to show that the dL formula in exercise 5 is not an axiom. However, recall the following definition of the box modality:

“A box modal formula \([\alpha]P\) is true in state \(\omega\) iff its postcondition \(P\) is true in all states \(\nu\) that are reachable by running \(\alpha\) from \(\omega\). (p.144, Logical Foundations of Cyber-Physical Systems)”

Note that the constraint \(1 = 0\) is false in all states and we have \([x' = 0 \& 1 = 0] = \emptyset\). By the definition of the box modality the formula \([x' = 0 \& 1 = 0](0 = 0)\) evaluates to \(true\), because there are no runs of the program. Therefore, the right-hand side of the formula evaluates to \(true \leftrightarrow true\), which is true in all states.

The following is a correct counter example

\[ (1 = 0 \rightarrow [x' = 0 \& 1 = 0](1 = 0))' \rightarrow ([x' = 0 \& 1 = 0](1 = 0) \leftrightarrow 1 = 0)). \]