Verified Train Controllers for the Federal Railroad Administration Train Kinematics Model: Balancing Competing Brake and Track Forces

Aditi Kabra  Stefan Mitsch  André Platzer

Computer Science Department, Carnegie Mellon University

INTERNATIONAL CONFERENCE ON EMBEDDED SOFTWARE 2022
Train Control: Complicated

End of movement authority: the train must stop by this point
End of movement authority: the train must stop by this point.
Train Control: Complicated

End of movement authority: the train must stop by this point

Gravity

uphill
Train Control: Complicated

End of movement authority: the train must stop by this point

Gravity decreases uphill

Acceleration
End of movement authority: the train must stop by this point.

- Gravity decreases uphill.
- Acceleration decreases.
- Resistance decreases.
Train Control: Complicated

End of movement authority: the train must stop by this point

Gravity: decreases uphill

Acceleration: decreases

Resistance: increases
Train Control: Complicated

End of movement authority: the train must stop by this point

Gravity

- decreases uphill

Acceleration

- changes
- decreases

Resistance

- increases
Train Control: Complicated

- End of movement authority: the train must stop by this point

- Gravity decreases uphill

- Acceleration changes

- Resistance decreases, Resistance increases

- Air brake acceleration

- Time since brake application
Train Control: Complicated

End of movement authority: the train must stop by this point

Gravity decreases uphill

Acceleration changes

Resistance decreases

Air brake acceleration increases

Time since brake application
Formal Verification

Formal Verification

Formal Model

Proving in KeYmaera X Theorem Prover

Complete FRA Model[1]

2545 lines of proof tactic

Formal Verification

Complete FRA Model[1]

Proof: ✔ All goals closed

2545 lines of proof tactic

Infinitely many possibilities checked once and for all

Formal Verification

Formal Model

Infinitely many possibilities checked once and for all

Proving in KeYmaera X Theorem Prover

2545 lines of proof tactic

Complete FRA Model[1]

Proof: ✔ All goals closed

FRA Model

Complete


Generalizable
Approach: Impact

Approach: Impact

Approach: Impact

Overview

- Introduction
- Techniques
- Evaluation
- Summary
Background: Dynamics

\[ p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b \]

with \( a_l \in [-b_{\text{max}}, a_{\text{max}}] \), \( a_a = \max(a_b, a_{b_{\text{max}}}) \)
Background: Dynamics

\[ p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b \]

with \( a_l \in [-b_{\text{max}}, a_{\text{max}}], a_a = \max(a_b, a_{b_{\text{max}}}) \)

Rate of change of train position is velocity
Rate of change of train position is velocity

Rate of change of train velocity is acceleration

\[ p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b \]

with \( a_l \in [-b_{\text{max}}, a_{\text{max}}], a_a = \max(a_b, a_{b_{\text{max}}}) \)
Background: Dynamics

Rate of change of train velocity is acceleration

\[ p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b \]

with \( a_l \in [-b_{\text{max}}, a_{\text{max}}], a_a = \max(a_b, a_{b\text{max}}) \)

Rate of change of train position is velocity

Air brakes ramp up
Background: Dynamics

Rate of change of train position is velocity

Rate of change of train velocity is acceleration

Air brakes ramp up

\[ p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b \]

with \( a_l \in [-b_{\text{max}}, a_{\text{max}}], a_a = \text{max}(a_b, a_{b_{\text{max}}}) \)
Unknown functions: slope, curve

\[ p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b \]
Unknown functions: slope, curve

\[ p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b \]
Unknown functions: slope, curve

\[ p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b \]
Unknown functions: slope, curve

Use worst case value ... 

\[ p' = v, \quad v' = a_l + a_a + a_s(p) + a_r(v) + a_b(p), \quad a'_b = m_b \]

Unknown function: replace with worst case value \( m_s \)

Unknown function: replace with worst case value 0
Unknown functions: slope, curve

... with improving estimates.

\[ a_s(p) \leq \bar{a}_s(p_0) = \min(m_s, a_s(p_0) + u \cdot h_{\text{max}} \cdot T) \]
Unknown functions: slope, curve

... with improving estimates.

\[ a_s(p) \leq \bar{a}_s(p_0) = \min(m_s, a_s(p_0) + u \cdot h_{\text{max}} \cdot T) \]
Other Techniques

Circular Dependencies

**Problem:** Circular dependence while estimating worst case values.

**Solution:** Bootstrap cycle with naive values, then iterate.

Taylor Polynomial

**Problem:** Davis resistance integrates poorly.

\[
\left( \sqrt[4]{(a_i + m_s)a_2 - a_i^2} \right) \cdot \tan \left( \frac{t \sqrt[4]{(a_i + m_s)a_2 - a_i^2}}{2} + \tan^{-1} \left( \frac{a_1 + 2a_2\gamma_0}{\sqrt[4]{(a_i + m_s)a_2 - a_i^2}} \right) \right) - a_1
\]

**Solution:** Taylor polynomial approximation.

Ghost Trains

**Problem:** Intermediate reasoning steps transcendental.

**Solution:** Reason about as ODE (here represents dynamics of a “ghost” train).

\[
geq
\]
Overview

- Introduction
- Techniques
- Evaluation
- Summary
Limiting Undershoot while Maintaining Safety

Limiting Undershoot while Maintaining Safety

Limiting Undershoot while Maintaining Safety

Start braking

Train stops

End of movement authority

Summary

Verified controller for full FRA model dynamics. KeYmaera X proofs available online.

Generalizable Techniques
- Dealing with unknown functions
- Circular dependencies
- Taylor polynomials
- Ghost dynamics

Verified Model Generalizability
- Abstraction of physical details
- Nondeterministic controller

Experiments
Controller limits undershoot while maintaining safety